Министерство образования и науки Российской Федерации
Федеральное агентство по образованию

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

НАУЧНАЯ СЕССИЯ ТУСУР–2009

**Материалы докладов
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
12–15 мая 2009 г.**

В пяти частях

Часть 3

Тематический выпуск
«СИСТЕМНАЯ ИНТЕГРАЦИЯ И БЕЗОПАСНОСТЬ»

В-Спектр
Томск–2009

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

Н-34 Научная сессия ТУСУР–2009: Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. 12–15 мая 2009 г.: В пяти частях. – Ч. 3. Тематический выпуск «Системная интеграция и безопасность». – Томск: В-Спектр, 2009. – 392 с.

ISBN 978-5-91191-103-4
ISBN 978-5-91191-106-5 (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-измерительных приборов и устройств, распределенных информационных технологий, вычислительного интеллекта, автоматизации технологических процессов, в частности, в системах управления и проектирования, информационной безопасности и защите информации. Представлены материалы по математическому моделированию в технике, экономике и менеджменте, антикризисному управлению, автоматизации управления в технике и образование, также касающиеся социокультурных проблем современности, экологии, мониторинга окружающей среды и безопасности жизнедеятельности.

Для студентов, аспирантов, технических работников.

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

ISBN 978-5-91191-103-4
ISBN 978-5-91191-106-5 (Ч. 3)

© Том. гос. ун-т систем управления
и радиоэлектроники, 2009

Вступительное слово

Прошел год с момента создания Института системной интеграции и безопасности ТУСУРа (ИСИБ), который состоит из Центра технологий безопасности, Удостоверяющего центра Сибири, Центра по обработке конфиденциальной информации, Центра подготовки и переподготовки кадров, Филиала ТУСУР в г. Сургуте, кафедры Комплексной информационной безопасности электронно-вычислительных систем, научно-производственных лабораторий: речевых технологий, безопасных биомедицинских технологий, систем безопасности. За этот период становления нашим коллективом сделано немало. Практически начал работать Центр подготовки и переподготовки кадров, успешно продолжается работа других центров Института. Разворачиваются работы по созданию Центра «Антитеррор». За прошедший год объем внебюджетных средств, привлеченный Институтом, составил около 60 млн. рублей. Безусловно, для многих это сумма может показаться мизерной. Однако, учитывая сложности становления, отсутствие централизованного финансирования для развития, мы считаем это неплохим результатом. Институтом проведена X Всероссийская конференция «Безопасность государства, общества, личности», в которой приняли участие представители 52-х университетов России, Министерства образования и науки, федерального Агентства информационных технологий, ФСБ, ФСТЭК, ряда коммерческих фирм, специализирующихся на проблемах безопасности. При финансовой и научно-методической поддержке Института проведен III Пленум Сибирского отделения учебно-методического объединения по образованию в области информационной безопасности. Продолжен выпуск специалистов по защите информации, инженеров по проектированию ЭВС, в 2008 г. количество выпускников составило 124 человека.

По итогам 2008 г. кафедра КИБЭВС стала лучшей в ТУСУРе, заняв первое место по учебно-методической работе, второе – по информатизации, третье место – по научной работе. За прошедший год Институтом подготовлено и выпушено 3 сборника научных и методических работ, более 150 научных публикаций в различных сборниках трудов и журналах, в том числе из Перечня ВАК, получено 4 свидетельства ОФАП, проведен VIII Всероссийский конкурс студентов и аспирантов по информационной безопасности. Это лишь первые, но весьма уверенные шаги нашего Института.

Ставший традиционным тематический сборник «Системная интеграция и безопасность» включает в себя результаты современных научных исследований в области автоматизации и информационной безопасности. В условиях общемирового финансового кризиса, стано-

вятся еще более актуальными задачи повышения эффективности работы различных систем, являющихся составной частью российской экономики, и защита этих систем от внешних и внутренних угроз. 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. В этом году сборник включает 130 работ, и, следует отметить, что в его наполнении приняли участие также молодые ученые со всех уголков нашей страны: от самой западной (г. Калининград), до самой восточной (г. Владивосток) границ России. Эти факты бесспорно подтверждают нашу уверенность в том, что научные исследования по важнейшим направлениям развития современного общества будут успешно продолжаться. Спасибо всем авторам за готовность поделится с научным и профессиональным сообществом своими результатами!

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

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., к.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 секции – Еханин Сергей Георгиевич, д.ф.-м.н., профессор КУДР

Секция 5. Конструирование и технологии радиоэлектронных средств. Председатель секции – Лощилов Антон Геннадьевич, м.н.с. каф. ТОР, к.т.н.; зам. председателя – Бомбизов Александр Александрович, инженер НИИ ЭТОСС

Секция 6. Интегрированные информационно-управляющие системы. Председатель секции – Катаев Михаил Юрьевич, д.т.н., проф. 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. СВЧ и КР, 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., профессор

Секция 9. Распределенные информационные технологии и системы. Председатель секции – Ехлаков Юрий Поликарпович, проректор по информатизации 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., проф. 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 каф. КИБЭВС; 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, первый проректор 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, 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 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, аспирант 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, зав. каф. КИБЭВС, д.т.н., профессор; зам. председателя – Мещеряков Роман Валерьевич, к.т.н., доц. каф. КИБЭВС

Секция 15. Информационно-измерительные приборы и устройства. Председатель секции – Светлаков Анатолий Антонович, д.т.н., профессор каф. ЭСАУ; зам. председателя – Шидловский Виктор Станиславович, к.т.н., доцент каф. ИИТ

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, 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, 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-методического 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 – Шостак Аркадий Степанович, д.т.н., профессор каф. КИПР; зам. председателя – Озеркин Денис Витальевич, 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: eak@main.tusur.ru

Материалы научных докладов,

представленные на конференцию, опубликованы в сборнике

«НАУЧНАЯ СЕССИЯ ТУСУР–2009»

в пяти частях

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

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

3-я часть – доклады 11-й и 14-й секций;

4-я часть – доклады 13-й, 15–17-й секций;

5-я часть – доклады 18–26-й секций.

СЕКЦИЯ 11

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

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

ТРЕХМЕРНОЕ МОДЕЛИРОВАНИЕ ЛИЦА ЧЕЛОВЕКА

М.С. Агапов, студент 5-го курса, каф. КИБЭВС,
Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-407-74-73, ams@sibmail.com

При современном развитии информационных технологий в области трехмерного моделирования изображений, искусственного интеллекта и вычислительной мощи персональных компьютеров становится возможным создание системы визуализации процесса произношения текста, как это делал бы человек.

В первую очередь, задача анимации речи является одной из задач, формирующих идеологию «дружественного» интерфейса с компьютером. Совмещение данной системы с программами, синтезирующими речевой сигнал, будет существенно способствовать более легкому восприятию информации. Сюда же можно отнести и вещание с Интернет-сайтов – так называемых виртуальных ведущих.

Первым и основополагающим этапом разработки системы анимации речи по печатному тексту является построение трехмерной графической модели. Для реализации такой модели удобно воспользоваться графическим 3D редактором, что позволит значительно упростить работу и сократить время на выполнение этапа. В качестве графического 3D редактора был выбран 3DS MAX 2009 как мощное, удобное и хорошо зарекомендовавшее себя средство 3D моделирования.

Существует множество подходов к моделированию человеческого лица. Большинство этих методов преследуют весьма специфические цели, такие, как лучшая передача черт лица, лучшая анимация мимики, упрощение нанесения текстуры и т.д. Лишь немногие приемы позволяют достигнуть всех этих целей одновременно, что требуется для создания реалистичной модели и анимации лица, а также выражения человеческих эмоций на модели [3].

Для выполнения поставленной задачи по построению графической модели был выбран метод сплайнов. Данный метод является одним из наиболее удобных для моделирования сложных реальных объектов, таких как лицо человека. Применение данной технологии подразумевает использование эскизов будущей графической модели.

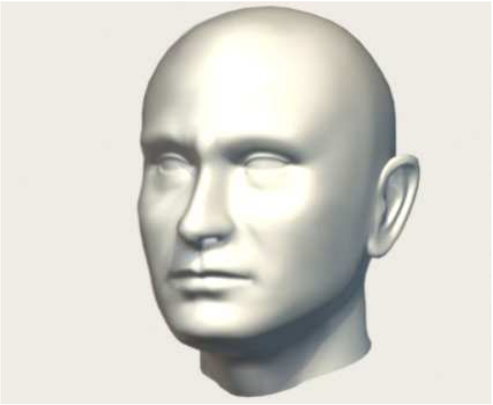
В данном случае в качестве эскизов использовались фотографии человека, в фас и профиль. При этом оба вида должны соответствовать друг другу в плане размеров и пропорций. Задача облегчается еще и тем, что работа ведется с симметричной моделью, то есть достаточно построить только одну ее половину, а затем зеркально отобразить готовую часть.

Эскизы загружаются в 3DS MAX, в соответствующие поля, фронтальный вид и вид слева, после чего создается так называемая виртуальная студия. В данном случае поскольку работа ведется с двумя эскизами, то для создания виртуальной студии можно использовать простое пересечение двух плоскостей.

Сплайны строятся таким образом, чтобы повторять основные черты эскиза модели. После выделения сплайнами основных горизонтальных линий на эскизе, необходимо соединить вершины поперечными сплайнами. Таким образом, получается сплайновая сетка графической модели.

После этого, с помощью модификатора Surface, примененного к полученной сплайновой сетке, можно получить поверхность трехмерной графической модели. А затем аналогичным образом, при помощи сплайнов, моделируются отверстия носа и ушная раковина.

Таким образом, была построена трехмерная графическая модель лица человека, представленная на рисунке.



Трехмерная графическая модель лица человека

Следует отметить, что представленная на рисунке графическая модель является промежуточным вариантом. На нее не были нанесены текстуры, а также отсутствует модель ротовой полости.

В дальнейшем планируется завершить графическую модель, добавить модель ротовой полости и текстуры, а также выделить управляющие точки на модели и определить траектории их движений при синтезе речевого сигнала. Затем разработать и реализовать программное приложение, которое будет управлять данной графической моделью, создавая эффект проговаривания текста, как это делал бы человек.

ЛИТЕРАТУРА

1. Шаммс Мортье. 3DS MAX 8 для «чайников»: Пер. с англ. М.: Издательский дом «Вильямс», 2006. 368 с.

2. Верстак В.А. 3DS MAX 8. Секреты мастерства. СПб.: Питер, 2006. 672 с.

3. http://www.3dtotal.ru/forum/showthread.php?t=6048 – Уроки по 3DS MAX. Моделирование головы.

СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ДЛЯ РАБОТЫ С БАЗОЙ ДАННЫХ

Р.Ф. Акчурин, студент 3-го курса, каф. КИБЭВС,
Н.А. Новгородова, ассистент каф. КИБЭВС
г. Томск, ТУСУР, nurka12@rambler.ru

С развитием компьютерной индустрии ЭВМ все глубже и глубже проникают в различные сферы человеческой деятельности, особенно где требуется обработка больших объемов информации.

Современная экономика немыслима без эффективного управления.

Успех управления во многом определяется эффективностью принятия интегрированных решений, которые учитывают самые разносторонние факторы и тенденции динамики развития ЭВМ.

Таким образом, главной целью автоматизированной системы являются быстрые и удобные процессы поиска, сбора, хранения, обработки, представления и распространения информации, реализованные с помощью ЭВМ и человека. Повышение эффективности работы компании, учреждения или какой-либо организации – основная задача автоматизированной системы обработки данных.

Для того чтобы создать какую-либо автоматизированную информационную систему, необходимо четко определиться с предметной областью, знать, какие сведения будут накапливаться и подвергаться обработке, а также что именно должна эта система автоматизировать. Определение предметной области является начальным этапом при проектировании. На этом этапе выявляются все потребности и все

пользователи, которые будут составлять содержание будущей системы, определяются объекты, представляющие интерес, их свойства и отношения [1].

Для наглядности проводят моделирование особенностей предметной области, например, используя технологии IDEF (Integration Definition for Function Modeling) – технологии структурного анализа, базирующиеся на хорошо известных методологиях, позволяющих анализировать процессы с трех ключевых точек зрения одновременно – IDEF0, IDEF3 и DFD.

Для функционального моделирования используется технология IDEF0. Согласно этой технологии анализируемый процесс представляется в виде совокупности множества взаимосвязанных действий, работ, которые взаимодействуют между собой на основе определенных правил, с учетом потребляемых информационных, человеческих и производственных ресурсов. Она хороша тем, что описывает систему в целом как множество взаимозависимых действий, или функций.

IDEF3 – технология сбора данных, необходима для проведения структурного анализа системы, дополняющая технологию IDEF0. Технология IDEF3 также может быть использована как метод проектирования бизнес-процессов.

Для структурного анализа потока данных используется технология DFD (Data Flow Diagrams). Диаграммы DFD позволяют описать процесс обмена информацией между элементами изучаемой системы. Данные диаграммы обеспечивают удобный способ описания передаваемой информации как между частями моделируемой системы, так и между системой и внешним миром.

Далее начинается проектирование базы данных, которая будет систематизировать все необходимые данные выбранной предметной области, поддерживать накопление и хранение информации об основных компонентах предметной области, автоматизировать выполнение бизнес-процессов. Необходимо спроектировать схему структуры базы данных таким образом, чтобы она была доступна для анализа и при ее модификации не возникали противоречия. Объекты подвергаются классификации и фиксируются совокупность их свойств, посредством которых будет описаны в базе данных типы объектов. Определяются бизнес-правила, представляющие собой механизмы управления БД и предназначенные для поддержания БД в целостном состоянии. Бизнес-правила можно реализовывать как на физическом, так и на программном уровнях.

Концептуальная модель данных строится с использованием методологии информационного моделирования IDEF1X (Integrated DEFinitions 1 eXpanded). При этом выделяют три уровня: уровень «сущность – связь», «уровень ключей» и уровень атрибутов. После

этого преобразовываются универсальные отношения, сформированные на уровне «сущность – связь», в систему отношений, удовлетворяющих определенным формальным отношениям [2].

Для хранения информации об объектах предметной области наиболее часто используется реляционная база данных, которая представляет собой множество взаимосвязанных двумерных таблиц – реляционных таблиц. Каждая таблица содержит информацию о субъектах (предметах) определенного типа. Для перевода концептуальной модели данных в реляционную необходимо каждой сущности предметной области поставить в соответствие таблицу базы данных, определить первичные и внешние ключи, а также нормализовать каждую из таблиц так, чтобы ликвидировать избыточность данных и противоречивость при работе с данными.

Завершив проектирование базы данных, необходимо выбрать среду для разработки будущей базы данных. Среда должна быть достаточно функциональной, удобной для использования, обеспечивать высокую скорость и удобство доступа к данным, чтобы обеспечить высокую скорость разработки приложений.

Проектирование автоматизированной системы начинается после выбора среды разработки RAD (Rapid Application Development). Разработка программы производится на основании технического задания. Для подключения к базе данных могут быть использованы различные технологии, например: ADO (ActiveX Data Object), ODBC (Open DataBase Connectivity) и др. Автоматизированная система должна позволять через удобный интерфейс заносить данные в таблицы базы данных, редактировать, удалять, просматривать уже занесенные данные, предоставлять пользователю возможности поиска необходимых данных, их сортировки, фильтрации и пр. Желательно предусмотреть вывод отчетных форм на экран и на печать.

Особо следует отметить необходимость организации защиты информации в базе данных, которая приобретает исключительно важное значение, поскольку информация представляет собой чрезвычайно ценный ресурс. Защита информации должна осуществляться в процессе ее сбора, хранения и обработки. Под защитой информации понимается совокупность мероприятий, методов и средств, обеспечивающих целостности информации, исключение несанкционированного доступа к ресурсам, а также исключение несанкционированного использования хранящихся данных.

ЛИТЕРАТУРА

1. Давыдова Е.М., Новгородова Н.А. Базы данных: учеб. пособие. Томск: Том. гос. ун-та систем управления и радиоэлектроники, 2005. 127 с.

2. Черемных С.В. Моделирование и анализ систем. IDEF-технологии: практикум. М.: Финансы и статистика, 2002. 192 с.

АВТОМАТИЗАЦИЯ РАБОТЫ ТОРГОВОГО ПРЕДПРИЯТИЯ С ПОМОЩЬЮ ТЕХНОЛОГИИ IDEF

Р.Ф. Акчурин, студент 3-го курса, каф. КИБЭВС
г. Томск, ТУСУР, nurka12@rambler.ru

В настоящее время все большую популярность приобретают инженерные методы реорганизации предприятий на основе современных информационных технологий. Расширяется спектр компьютеризованных инструментальных методов анализа экономических, а также бизнес-процессов. Поэтому сейчас невозможно представить ни одно из направлений бизнеса или производства без использования ЭВМ, компьютерного моделирования и прочих средств, помогающих отобразить, проанализировать экономические и бизнес-процессы.

Уже с давних пор в каждой стране, городе, и уже даже на улице появились различные предприятия торговли – от маленьких павильонов, до крупных торговых гипермаркетов. С каждым днем их становится все больше и больше. И для успешного менеджмента и работы магазинов необходим хороший структурный анализ бизнес-процессов.

IDEF (Integration Definition for Function Modeling) – технологии структурного анализа, базирующиеся на хорошо известных специалистам методологиях, позволяющих анализировать процессы (в том числе и бизнес-процессы) с трех ключевых точек зрения одновременно – IDEF0, IDEF3 и DFD [1].

IDEF0 – технология структурного анализа и проектирования, описывает систему в целом как множества взаимозависимых действий, или функций. IDEF0-функции системы исследуются независимо от объектов, которые обеспечивают их выполнение. Действие, обычно в IDEF0 называемое функцией, обрабатывает или переводит входные параметры (сырье, информацию и т.п.) в выходные.

На рис. 1 показаны основные производственные функции торгового предприятия.

Данная модель отличается тем, что она не конкретизирует область детальности торгового предприятия, а лишь показывает основные его функциональные составляющие, что является положительным в том смысле, что полученные диаграммы декомпозиций могут использоваться любым торговым предприятием, осуществляющим деятельность по купле-продаже.

Для проведения структурного анализа системы можно воспользоваться технологией сбора данных IDEF3, дополняющей технологию IDEF0. С помощью нее изучается возможность уточнить картину процесса, привлекая внимание аналитика к очередности выполнения функций и бизнес-процессов в целом.

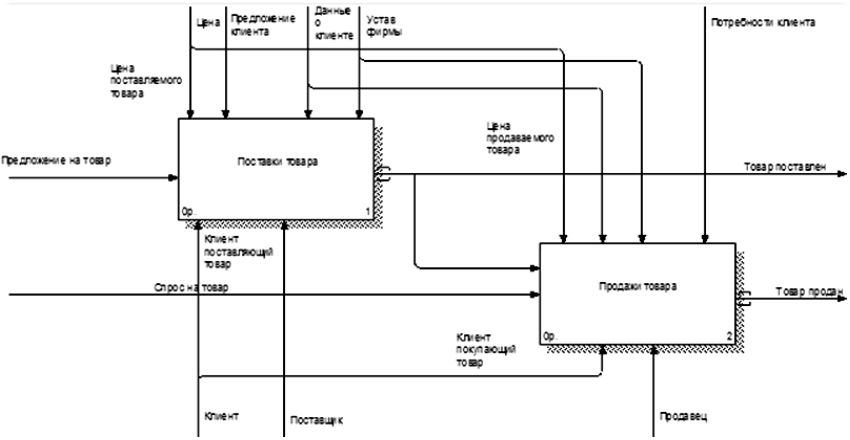


Рис. 1. Диаграмма декомпозиции деятельности (развернутая) по методологии IDEF0

На рис. 2 показана диаграмма декомпозиции поставки товара по методологии IDEF3.

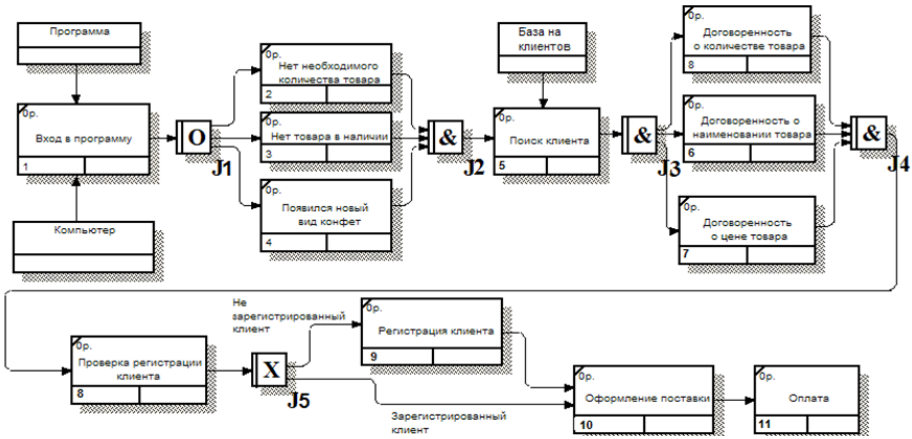


Рис. 2. Диаграмма декомпозиции поставки товара по методологии IDEF3

Данная модель хороша для описания процессов. В данном случае были описаны последовательность шагов, которые необходимо провести для того, чтобы осуществить поставку товаров в магазин.

DFD (*Data Flow Diagrams*) – структурный анализ потоков данных. Диаграммы DFD позволяют описать процесс обмена информацией между элементами изучаемой системы [1].

Диаграммы потоков данных обеспечивают удобный способ описания передаваемой информации, как между частями моделируемой системы, так и между системой и внешним миром. Они используются для создания моделей информационного обмена организации.

На рис. 3 приведена диаграмма декомпозиции поставки товара по методологии DFD.

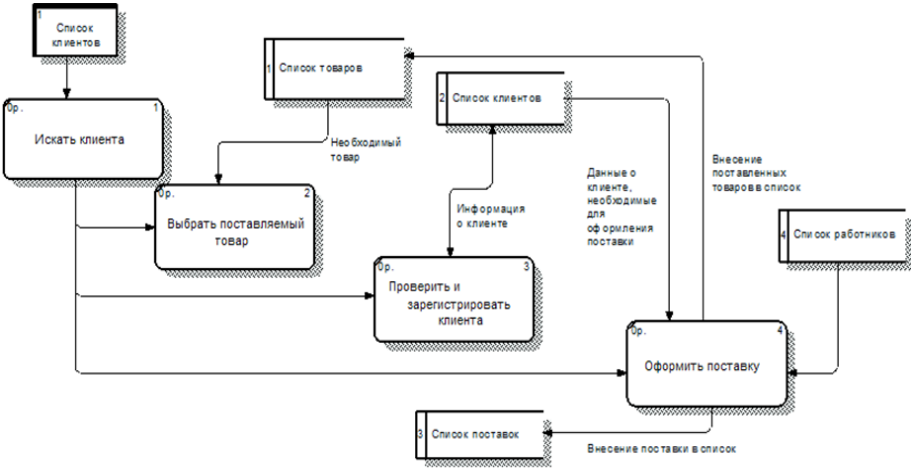


Рис. 3. Диаграмма декомпозиции поставки товара по методологии DFD

Таким образом, проводится структурный и функциональный анализ деятельности торгового предприятия, осуществляющего ведение бизнеса в области торговли, а именно купли-продажи какого-либо товара с использованием технологий IDEF0, IDEF3 и DFD.

ЛИТЕРАТУРА

1. Черемных С.В. Моделирование и анализ систем. IDEF-технологии: практикум. М.: Финансы и статистика, 2002. 192 с.

СИСТЕМА КЛАССИФИКАЦИИ ДАННЫХ

Р.Ф. Акчурин, В.А. Трошин, студенты 3-го курса, каф. КИБЭВС
г. Томск, ТУСУР, nurka12@rambler.ru

Еще во II в. до нашей эры в «Письме ученому соседу» Демокрит писал: «Если тебе, дорогой друг, нужно разобраться в сложном нагромождении фактов или вещей, ты сначала разложи их на небольшое число куч по похожести. Картина прояснится, и ты поймешь природу этих вещей» [1].

Группировка объектов по похожести их свойств упрощает решение многих практических задач анализа данных. Теория классификации и систематизации сложноорганизованных областей действительности, имеющих обычно иерархическое строение, решает эту задачу. Швейцарский ботаник О. Декандоль в 1813 г. назвал данную теорию таксономией (от греч. taxis – расположение, строй, порядок и nomos – закон [2]).

В 60–70-х гг. XX в. возникла тенденция определять таксономию как раздел систематики, как учение о системе таксономических категорий, обозначающих соподчиненные группы объектов – таксоны.

В настоящее время найти программу, реализующую классификацию объектов, достаточно сложно. Поэтому было решено создать такую классифицирующую систему, которой мог бы воспользоваться любой желающий, вне зависимости от своей предметной области.

Система должна обеспечивать внесение данных (вручную или импортированных с файла) о характеристиках назначенных объектов, анализ исходных данных и дальнейшую классификацию объектов по одному из четырех алгоритмов (с возможностью визуального просмотра результатов). Пользователю будет предоставлен выбор метода классификации (алгоритма таксономии).

Человек одно и то же множество m-объектов может разбить на k-таксонов различным образом, руководствуясь каким-то критерием F, который позволяет отличать хорошие группировки от плохих и выбирать наилучший вариант таксономии. Самый известный критерий F состоит в том, что в один таксон должны собираться объекты, похожие, близкие по своим характеристикам.

В разрабатываемой программе будут обрабатываться объекты, признаки которых измерены в сильных шкалах, что позволяет оценивать похожесть через евклидово расстояние между точками в многомерном пространстве. Если координаты центра j-го таксона обозначить символом C_j, то сумма расстояния $\rho(C_j, a_i)$ между центром и всеми m_j точками a_i этого таксона, где $i = 1 \div m$, а сумма таких внутренних расстояний для всех k таксонов $F = \sum \rho_j$, $j = 1 \div k$. Смысл критерия похожести на центр состоит в том, что нужно найти такое разбиение m объектов на k таксонов, чтобы величина F была минимальной [1]. Выполнение этого условия можно достичь с помощью алгоритма FOREL – одного из алгоритмов, который будет реализован в программе.

Таксоны, получаемые этим алгоритмом, имеют сферическую форму. Количество таксонов зависит от радиуса сфер: чем меньше радиус,

тем больше получается таксонов. Вначале признаки объектов нормируются так, чтобы значения всех признаков находились в диапазоне от нуля до единицы. Затем строится гиперсфера минимального радиуса R_0, которая охватывает все m точек. Начальная сфера с радиусом R_0 является главным таксоном. Для получения большего количества таксонов необходимо уменьшать радиус, при этом перемещая центр сферы в любую из имеющихся точек. После этого находится центр тяжести точек, попавших в данную сферу. Центр сферы перемещается в полученную точку и снова находится центр тяжести нового множества «внутренних точек». Такая процедура определения внутренних точек и переноса центра сферы продолжается до тех пор, пока сфера не остановится, т.е. пока на очередном шаге не обнаружится, что состав «внутренних точек», а следовательно, и их центр тяжести, не меняется. Это означает, что сфера остановилась в области локального максимума плотности точек в признаковом пространстве.

Точки, оказавшиеся внутри остановившейся сферы, объявляются принадлежащими первому таксону и исключаются из дальнейшего рассмотрения. Для оставшихся точек процедура повторяется [3].

Данный алгоритм является базовым.

Методы таксономии используется в различных областях науки. Примером решения задачи таксономии является анализ психологических характеристик студентов университета, анализ погодных таксонов, полученных на массиве метеорологических наблюдений, классификация типов почв и т.д.

Таким образом, разрабатываемую систему будет возможно применять в различных сферах деятельности человека для решения практических задач, с которыми справиться, без применения вычислительной техники достаточно сложно.

ЛИТЕРАТУРА

1. Загоруйко Н.Г. Прикладные методы анализа данных и знаний. Новосибирск: ИМ СО РАН, 1999. 264 с.

2. http://www.entomologija.ru/page.php?id=294

3. Елкина В.Н., Загоруйко Н.Г., Темиркаев В.С. Алгоритмы направленного таксономического поиска информативных подсистем признаков (НТПП). Новосибирск: 1974. 238 с.

МЕДИЦИНСКАЯ СИСТЕМА ВОССТАНОВЛЕНИЯ ГОЛОСОВОЙ ФУНКЦИИ

А.А. Авдеев, студент 5-го курса, КИБЭВС
г. Томск, ТУСУР, aaa0406@mail.ru

Возможности применения современных технологий в медицине в настоящее время достаточно обширны. При помощи информационных систем, ставших своего рода опорой современной медицины, врач может получить доступ к данным о больном, при этом значительно повышается быстрота их получения. При этом все виды применяемых технологий делятся на два направления, служащих обеспечению процесса:

1) обработка данных о пациенте: персональные данные (ПД), врачебная тайна;

2) излечение пациента.

Практически всегда для снижения стоимости сложные медицинские системы строятся на базе персональных компьютеров общего назначения с дополнениями в виде датчиков и устройствами отображения информации. В результате простейшей возможностью по улучшению системы является замена используемого программного обеспечения.

Данная система будет участвовать в процессе реабилитации онкологических больных, перенесших хирургические операции на гортани (полное удаление или частичную резекцию) [1]. Таким образом, по приведенной выше классификации система сочетает в себе оба направления, что особым образом должно отобразиться в ее структурной схеме. В настоящее время проблема защиты персональных данных стала остра как никогда ранее. Предпосылками к этому стали:

- достаточное распространение информационных систем персональных данных (ИСПДн);
- отсутствие в открытом доступе нормативных документов;
- сложность переработки имеющихся ИСПДн.

При этом в медицинских автоматизированных системах заведомо циркулирует информация, связанная с врачебной тайной, в результате чего система автоматически включается в класс специальных ИСПДн.

27 июля 2006 г. был принят Федеральный закон «О персональных данных» [2]. Приведем выдержку из статьи 19 этого нормативного акта: «…оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распро-

странения персональных данных, а также от иных неправомерных действий».

Из всего вышеперечисленного следует что медицинским учреждениям (да и всем остальным организациям) необходимо в срок до 1 января 2010 г. привести свои ИСПДн в соответствие с законодательством Российской Федерации. Предлагается схема взаимодействия медицинской системы с сервером баз данных (БД) по защищенному каналу связи посредством криптографии с открытым ключом (рис. 1). При этом идентификация и аутентификация пользователей могут проходить на основе сертификатов открытых ключей стандарта X.509.

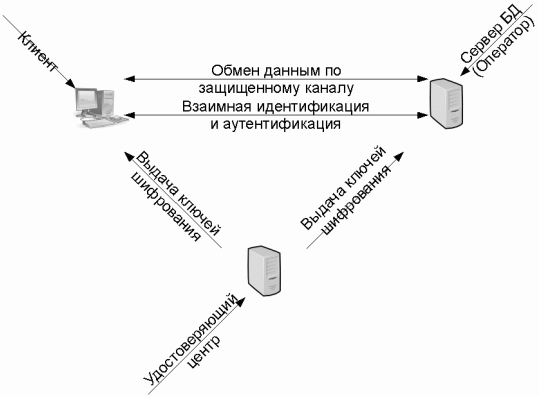


Рис. 1. Схема взаимодействия медицинской системы с сервером баз данных

ЛИТЕРАТУРА

1. Чойнзонов Е.Л., Балацкая Л.Н., Кицманюк З.Д. и др. Реабилитация больных опухолями головы и шеи. Томск: НТЛ, 2003. 296 с.

2. Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных». М., 2006.

МОДУЛЬ ОПОВЕЩЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ РАСПРЕДЕЛЕННЫМ ЛИФТОВЫМ ХОЗЯЙСТВОМ

А.И. Балашов, студент 3-го курса, каф. КИБЭВС,
М.И. Мельников, аспирант каф. КИБЭВС
г. Томск, ТУСУР, mmi@keva.tusur.ru

В мире, наполненном информационными технологиями, некоторые процессы до сих пор имеют слабую автоматизацию. Так, управле-

ние лифтами происходит в полуавтоматическим режиме, что вносит дополнительные факторы риска (такие, как человеческий фактор) и проблемы (такие, как несвоевременная диагностика и предупреждение аварийных ситуаций). Система, разрабатываемая нашим коллективом, должна минимизировать участие человека в процессе управления лифтовым хозяйством, а также сократить время реакции на нештатные ситуации, или же в некоторых случаях предупреждать эти ситуации. Как любой сложной системе с продуманной архитектурой, системе управления лифтовым хозяйством требуется специальный модуль, значительно расширяющий ее функционал, а именно модуль оповещения.

Подробная схема системы, для которой разрабатывается модуль [1] оповещения, представлена на рис. 1.

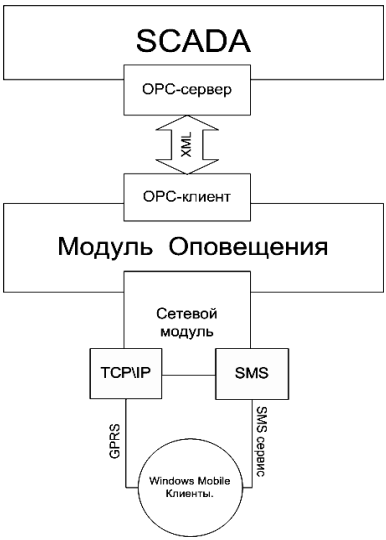


Рис. 1. Схема системы

Отдельного пояснения требуют связи между SCADA [3] системой и модулем оповещения, реализованные через OPC XML-DA (XML-Data Access) [2], протокол и связь windows mobile клиентов с сетевым модулем. Так как одним из критериев разработки системы выступает ее расширяемость, было решено использовать протокол OPC XML-DA [2], который в качестве формата передачи данных использует XML [4] – текстовый формат, предназначенный для хранения структурированных данных. Модуль оповещения сопряжен с клиентами через сетевой модуль, который позволяет организовать передачу данных через две различных среды Интернет (TCP/IP) и через сотовую связь (sms). Это необходимо для того, чтобы иметь возможность гибкой настройки системы под конкретного клиента и его потребности.

Таким образом, можно заключить, что разрабатываемая система будет высоко востребована, а также в последующем очень гибка, расширяема и легко поддерживаема.

Модуль оповещения – служит для связи SCADA системы с мобильным телефоном, установленным на нем программным обеспечением. Связь может осуществляться с помощью gsm шлюза и/или по

протоколу TCP/IP. На рис. 3 представлена структурная схема взаимодействия программы с OPC сервером и мобильным телефоном.

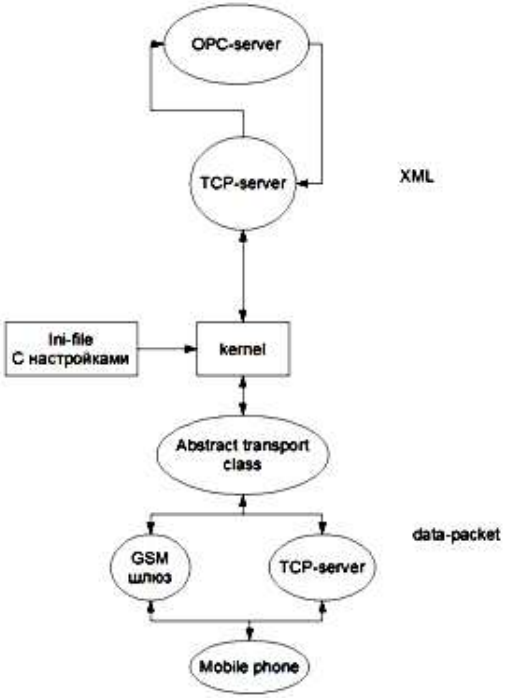


Рис. 3. Схема взаимодействия

Модуль оповещения будет взаимодействовать с OPC-сервером посредством TCP-сокета [1], ожидающего входящие соединения, открытого на 2009 порту. Формат передачи данных – XML.

В последующем возможно его расширение и дополнение для обеспечения дополнительного функционала.

Для взаимодействия с телефоном посредством gsm-шлюза или tcp-сервера будет использоваться data-packet, на данном этапе разработки модуля еще обсуждается вопрос формата пакета, но были предложены следующие варианты.

1. Использовать сериализованную структуру packet_t.
2. Использовать сообщение формата XML по аналогии с предложенной выше.

На данном этапе планируется закончить разработку и тестовую эксплуатацию модуля оповещения и приступить к разработке интерфейса управления.

ЛИТЕРАТУРА

1. Страуструп Б. Язык программирования C++. М.: Бином, 2005. 1104 с.
2. OPC Foundation, OPC Specifications: http://www.opcfoundation.org/Downloads.aspx?CM=1&CN=KEY&CI=283
3. Supervisory Control And Data Acquisition http://ru.wikipedia.org/wiki/SCADA
4. eXtensible Markup Language http://ru.wikipedia.org/wiki/XML

ФУНКЦИОНАЛЬНАЯ СХЕМА ДЛЯ ПРОЕКТА «ИССЛЕДОВАТЕЛЬСКИЙ РОБОТ»

С.П. Берляков, Д.С. Бронников, Е.О. Воронина, Т.Р. Муксунов, студенты 3-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-411-60-02, katehok@sibmail.com

Идея построения электронной «начинки» робота заключается в разделении двух основных функций: 1) формирования слова управления по информации, полученной от датчиков, и по результату построения математической модели окружения; 2) управления системой электроприводов, осуществление синхронизации их работы.

Введение раздельного управления продиктовано невыгодностью совмещения в одном кристалле требуемых для выполнения обеих задач функций [2]. Так, например, МК, заточенный под управление двигателями, имеет все необходимые для этого порты ввода-вывода и вложенные в него аппаратные решения для организации их синхронной работы. Но в то же время его ресурсов не хватит для сложных математических расчетов, которые загружают процессор при создании модели окружения в реальном времени. Для этих функций предназначен другой класс МК: сигнальные процессоры, «не боящиеся» громоздкой математики.

Сигнальные процессоры работают на частотах около 1 ГГц и имеют обширную библиотеку математических функций [1]. В его задачи будут входить вычисление таблицы расстояний до окружающих предметов по изображению полученной бинокулярной системой, аппроксимация, анализ полученной поверхности, вычисление максимумов и минимумов (для «карабкающегося» движения по поверхностям большого наклона) и выбор оптимальной траектории движения, разведенного для каждого сегмента ножек. Вычисленная траектория движения сегментов преобразуется в «слово управления», которое содержит инструкцию для исполнительного МК: адрес соответствующего привода, длительность и частота управляющей импульсной последовательности и общий порядок выполнения. Моделирование происходит в реальном времени с заданной частотой обновления. Следующее «слово управления» начнет формироваться после приема соответствующего сигнала от исполнительного МК, информирующего об окончании своей работы [3].

Для соединения двух плат возможно использовать PC104 формат расширения. Этот интерфейс удобен с конструкторской точки зрения. В то же время обмен между математическим и функциональным модулем не накладывает критических требований по скорости обмена информацией, что позволяет использовать 8-битную шину [1].

Для управления системой шаговых приводов можно использовать медленные (1–16 МГц), но компактные и не требовательные к питанию промышленные контроллеры, в то же время обладающие рядом нужных особенностей. Логика этих процессоров 8- или 16-битная, что вполне достаточно. Любые свои операции процессор будет тем не менее выполнять за доли секунды, что меньше скорости выполнения механической операции. Будем исходить из того, что одновременно МК будет поддерживать исполнение не более 3х4 механических операций по числу активных ног и числу сочленений в каждой ножке. Это должно быть учтено при формировании «слова управления» от СП (рис. 1).

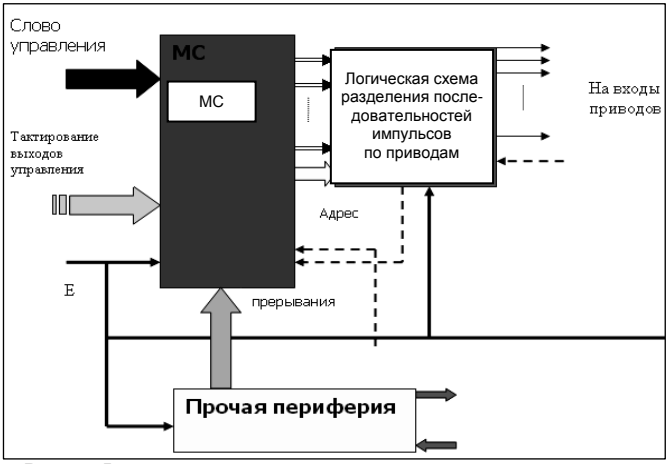


Рис. 1. Функциональная схема платы управления приводами

При движении по сложной наклонной поверхности в случае механического сбоя следует продумать систему отката предыдущих действий и попытки повторить последовательность, а в случае повторения ошибки процесс исполнения текущего «слова» должен быть временно или полностью прерван и ошибка должна быть отправлена СП на обработку и формирование аварийного «слова».

Таким образом, на данном этапе мы имеем следующие технические задачи по проектированию:

1. Выбор типа приводов.
2. Выбор МК для их управления.
3. Создание характеристической, а потом и принципиальной схемы управления.

Схемотехника функционального модуля сильно зависит как от типа привода, так и от МК, на базе которого она проектируется. Для уменьшения требований по количеству выводов требуется аппаратно

реализовать логику выбора привода по генерируемому адресу и т.д. Одним из решений является подведение питания по каналу данных, что позволит уменьшить количество проводников, однако уменьшит скорость обмена.

ЛИТЕРАТУРА

1. **Ошибка! Недопустимый объект гиперссылки.**

2. Мехатроника: Пер. с яп. Т. Исии, И. Симояма, Х. Иноуэ. М: Мир, 1988. 318 с.

3. Осипов Ю.М. Основы мехатроники. Томск: ТУСУР, 2007. 162 с.

БАЗА ДАННЫХ ПО ИНВЕНТАРИЗАЦИИ КОМПЬЮТЕРНОЙ ТЕХНИКИ ОРГАНИЗАЦИИ

А.О. Битюцкая, студентка 3-го курса, каф. КИБЭВС

г. Томск, ТУСУР, bao_89@mail.ru

В рамках проекта «Инженерия баз данных», проводимого на кафедре КИБЭВС, было принято решение все данные по инвентаризации компьютерной техники организовать в виде централизованной базы данных.

Цель проекта: проектирование и создание базы данных для регистрации и учета компьютерной техники и программного обеспечения, а также разработка приложения для работы с базой данных.

Задача разработанной базы данных – ведение сведений об аппаратуре, периферийных устройствах и программном обеспечении.

В процессе работы проводилось исследование предметной области с целью выявления наиболее значимых сущностей и их атрибутов, нормализация базы данных.

Достигнутые результаты: определены все наиболее значимые сущности предметной области и их атрибуты, создана база данных для регистрации и учета компьютерной техники и программного обеспечения.

База данных должна обеспечивать:

1. Учет сведений об аппаратуре, принадлежащей кафедре КИБЭВС.
2. Учет сведений о периферийных устройствах.
3. Учет сведений о программном обеспечении.
4. Учет сведений о пользователях системы.
5. Архивацию.

Основные бизнес-процессы:

1. Учет данных о компьютерах.
2. Учет сведений о пользователях.

3. Контроль смены аппаратуры, периферийных устройств и программного обеспечения.

4. Архивация данных.

Эти процессы выполняются полуавтоматически с минимальным участием пользователей системы.

Бизнес-правила:

1. Место нахождения аппаратуры и периферийных устройств (ПУ) совпадает с местом нахождения компьютера.

2. Место приобретения аппаратуры и ПУ по умолчанию совпадает с местом приобретения компьютера, если аппаратура или ПУ были куплены отдельно, то это учитывается.

3. Ответственный за компьютер, программное обеспечение (ПО), аппаратуру и ПУ администратор.

4. У компьютера может быть несколько видов аппаратур.

5. Один и тот же тип аппаратуры может стоять на многих компьютерах.

6. Для одного и того же типа аппаратуры может быть несколько драйверов (версий).

7. На одном и том же компьютере может стоять только один драйвер из нескольких возможных для данной аппаратуры.

8. На один и тот же компьютер можно поставить несколько ПО.

9. Одно и то же ПО стоит на многих компьютерах.

10. В одном и том же месте может находиться много компьютеров.

11. В одном и том же месте может быть приобретено много компьютеров.

Концептуальная модель данных строится с использованием методологии информационного моделирования IDEF1X (Integrated DEFinitions 1 eXpanded), имеющей в настоящее время статус федерального стандарта США. В IDEF1X различают три уровня графического представления информации.

Уровень «сущность – связь» (Entity-Relationship, ER-level). Это уровень наименее детального представления информации, где сущности и связи представлены только именами.

Уровень ключей (Key-Based, KB level). На этом уровне в диаграммах отражаются имена первичных и внешних ключей сущностей и связей.

Уровень атрибутов (Fully attributed, FA level). Диаграмма FA-уровня показывает имена всех атрибутов сущностей и связей и полностью определяет структуру и взаимосвязи данных.

Ниже представлена диаграмма уровня «сущность – связь» (рис. 1).

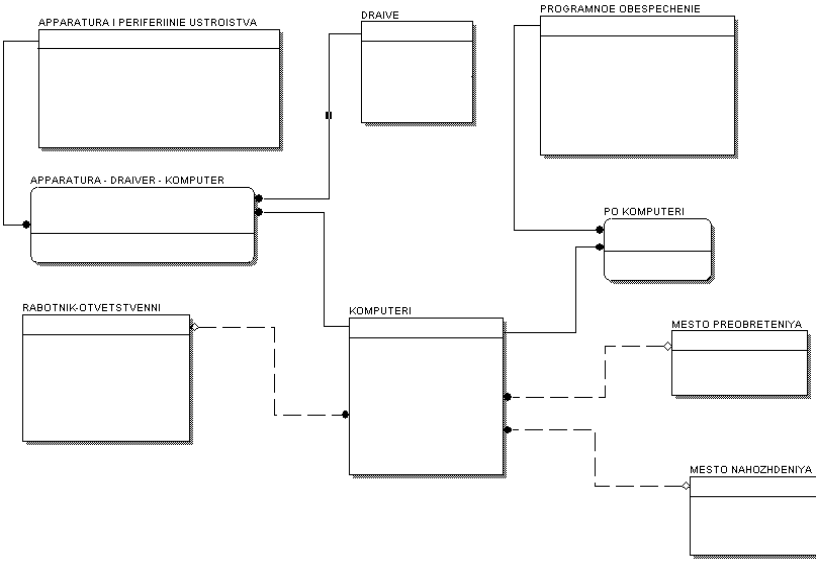


Рис. 1. Уровень «сущность – связь» (ER-уровень)

ЛИТЕРАТУРА

1. Бори Х. Firebird: руководство разработчика баз данных. СПб.: БХВ-Петербург, 2006. 1104 с.

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

СТРУКТУРНЫЙ АНАЛИЗ СИСТЕМЫ УЧЕТА КОМПЬЮТЕРНОЙ ТЕХНИКИ

А.О. Битюцкая, студентка 3-го курса, каф. КИБЭВС

г. Томск, ТУСУР, bao_89@mail.ru

В последние годы все интенсивнее развивается компьютерная индустрия. В большинстве сфер человеческой жизни обработка информации уже невозможна без ЭВМ, особенно если обрабатываются большие объемы информации.

Вопрос об инвентаризации имущества в наше время очень актуален, так как компьютерная техника и программное обеспечение требуют высоких материальных затрат. Также в наше время ужесточился контроль за лицензионным программным обеспечением. Все это ведет к обязательному контролю компьютерной техники и программного

обеспечения. Учет компьютерной техники в организациях может стать проще с помощью автоматизированной системы сбора и обработки данных.

В процессе работы проводилось исследование предметной области с целью выявления наиболее значимых сущностей и их атрибутов. Также были выявлены бизнес-процессы и бизнес-правила.

Основные бизнес-процессы:

– учет данных о компьютерах;

– учет сведений о пользователях;

– контроль смены аппаратуры, периферийных устройств и программного обеспечения;

– архивация данных.

Эти процессы выполняются полуавтоматически с минимальным участием пользователей системы.

Проводится функциональное моделирование по методологии IDEF0 (рис. 1).

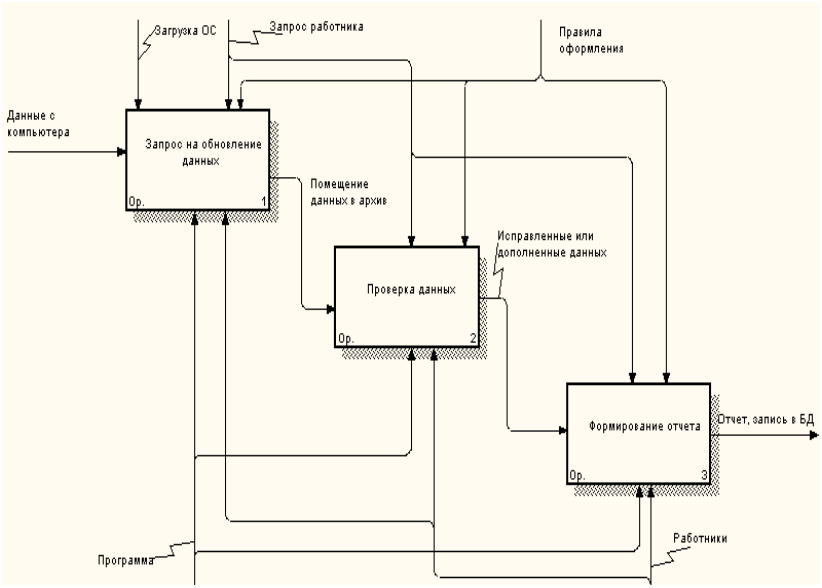


Рис. 1. Диаграмма декомпозиции деятельности системы (развернутая) по методологии IDEF0

Бизнес-правила:

– место нахождения аппаратуры и периферийных устройств (ПУ) совпадает с местом нахождения компьютера;

– место приобретения аппаратуры и ПУ по умолчанию совпадает с местом приобретения компьютера, если аппаратура или ПУ были куплены отдельно, то это учитывается;

– ответственный за компьютер, программное обеспечение (ПО), аппаратуру и ПУ администратор;

– у компьютера может быть несколько видов аппаратур;

– один и тот же тип аппаратуры может стоять на многих компьютерах;

– для одного и того же типа аппаратуры может быть несколько драйверов (версий);

– на одном и том же компьютере может стоять только один драйвер из нескольких возможных для данной аппаратуры;

– на один и тот же компьютер можно поставить несколько ПО;

– одно и то же ПО стоит на многих компьютерах;

– в одном и том же месте может находиться много компьютеров;

– в одном и том же месте может быть приобретено много компьютеров.

ЛИТЕРАТУРА

1. Давыдова Е.М., Новгородова Н.А. Базы данных: учеб. пособие. Томск: Томс. гос. ун-та систем управления и радиоэлектроники, 2005. 127 с.

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

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПОИСКА, АНАЛИЗА И ПРИНЯТИЯ РЕШЕНИЙ В СЕТИ ИНТЕРНЕТ (ПУАРО)

А.С. Бондаренко, студент 4-го курса, каф. КИБЭВС,
А.И. Гуляев, А.С. Яценко, студенты 3-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-913-112-91-08, boalse@yandex.ru

Современные поисковые системы позволяют достаточно точно найти желаемую информацию, но почти немногие из них могут помочь пользователю принять решение. Программы такого вида, а именно системы поддержки принятия решений, уже существуют и используются в целях проектирования программного обеспечения. На протяжении нескольких десятилетий стоит задача поиска повторяемого, предсказуемого процесса или методологии, которые бы улучшили продуктивность и качество создаваемого программного обеспечения. Такая программа нужна для четкого управления процессами.

В нашем случае система принятия решений, подключенная к поиску информации, поможет пользователю получить ответ на его во-

прос, сделать выводы о найденной информации. В данной работе предложен один из вариантов общего построения такой системы (рис. 1).

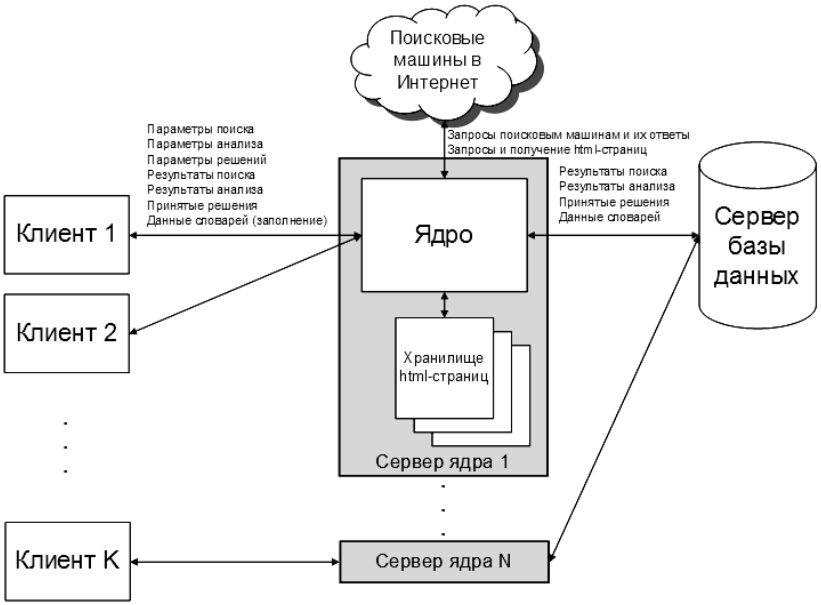


Рис. 1. Концептуальная схема системы ПУАРО

Описание клиентской программы (далее клиент).

Клиент взаимодействует с ядром через открытый на сервере ядра порт клиента. Клиент посылает ядру параметры поиска, анализа, решений, данные словарей (для заполнения словарей), получает от ядра результаты поиска, анализа, принятых решений, данные словарей (для просмотра словарей). Потенциально возможна также посылка других запросов ядру и получение от него соответствующих ответов, необходимость в этом может появиться при дальнейшей разработке.

Клиент не предназначен для сложных вычислений и обработке больших объемов данных, он нужен лишь для формирования запросов пользователем, посылки этих запросов ядру и визуального отображения результатов запросов пользователю.

Клиентов может быть неограниченное количество *K*, каждый из которых может взаимодействовать только с одним из *N* ядер и только с ним.

Если клиенту требуется получить данные от сервера базы данных, он должен делать это через ядро.

Клиент должен предоставлять пользователю удобный и интуитивно-понятный визуальный интерфейс.

Описание сервера ядра.

Ядро физически находится на той же ЭВМ, что и хранилище html-страниц (далее – хранилище) для более быстрой и эффективной обработки этих страниц, представляющих в совокупности большой объем данных. Описанная в данном пункте ЭВМ далее называется «сервер ядра».

Серверов ядра может быть неопределенное количество *N*, каждый сервер ядра взаимодействует с одним общим сервером базы данных.

Ядро взаимодействует с клиентом по правилам, описанным ранее.

Получая от клиента запрос на поиск и параметры поиска, ядро посылает запрос в Интернет поисковым машинам по переданным клиентам параметрам. От поисковых машин приходят страницы со ссылками на найденные ресурсы (далее – ссылки) и краткое описание о найденных ресурсах (далее – краткое описание). Из ссылок формируется список ссылок.

В зависимости от параметров запроса, переданных от клиента, ядро может удалить из общего списка ссылок, полученного в предыдущем пункте, ненужные ссылки, проанализировав краткое описание по определенным алгоритмам анализа.

По каждой ссылке из списка ссылок ядро запрашивает в Интернет страницу, получает ее и записывает в хранилище в виде отдельного файла с уникальным именем. Информация о том, какая страница в хранилище была получена по конкретной ссылке, передается на сервер базы данных и сохраняется там. Процесс связывания страницы с ее ссылкой в Интернет назовем индексацией хранилища.

Получая от клиента запрос на анализ и параметры анализа, ядро запрашивает у сервера базы данных список страниц хранилища, удовлетворяющих параметрам запроса. Каждая страница анализируется ядром по определенным алгоритмам анализа. Результаты анализа передаются клиенту и серверу базы данных для их долговременного хранения.

В ядро должна быть заложена потенциальная возможность выполнять другие запросы клиента, необходимость в которых может появиться при дальнейшей разработке. Также необходимо предусмотреть потенциальную возможность пересылки и получения другой информации в сервер базы данных, пока не рассматриваемой в данном документе.

Для гибкости системы ядро должно быть кроссплатформенным, в связи с чем для его реализации была выбрана библиотека «QT».

Сервер базы данных (сервер БД).

Сервер БД реализован на СУБД MySQL, взаимодействие ядра с сервером БД происходит через порт, который открывает MySQL-сервер для доступа к нему. Сервер БД в системе является единственным, напрямую с ним взаимодействуют только ядра.

Описание модели системы не является полным, в данной статье представлена лишь общая концепция ее построения. Такая структура системы достаточно гибкая, ее можно целиком реализовать как на одной локальной ЭВМ, так и развернуть в вычислительной сети, причем принцип кроссплатформенности позволит ей работать на машинах с различными операционными системами.

ЛИТЕРАТУРА

1. Черноруцкий И.Г. Методы принятия решений. СПб.: БХВ-«Петербург», 2005. 410 с.

ОПТИМАЛЬНОЕ РАЗМЕЩЕНИЕ МОДУЛЕЙ ВТОРОГО УРОВНЯ В ПЕРФОРИРОВАННОМ БЛОКЕ ЭЛЕКТРОННОГО СРЕДСТВА

С.А. Чебатков, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-913-877-36-84, stanislav@27cards.ru

Обеспечение нормального теплового режима является одним из основных факторов, определяющих надежность аппаратуры различного целевого назначения.

Большинство радиотехнических устройств, потребляя от источников питания мощность, измеряемую десятками, а иногда и сотнями ватт, отдают полезной нагрузке от десятых долей до единиц ватт. Остальная электрическая энергия, подводимая к элементу, превращаясь в тепловую, выделяется внутри корпуса. Температура корпуса оказывается выше температуры окружающей среды, в результате чего происходит процесс отдачи теплоты в окружающее пространство. Этот процесс идет тем интенсивнее, чем больше разность температур корпуса и окружающей среды.

Известно, что надежность элементов радиоэлектронной аппаратуры сильно зависит от температуры окружающей среды. Для каждого типа элемента в технических условиях указывается предельная температура, при превышении которой элемент нельзя эксплуатировать. Поэтому одной из важнейших задач при проектировании является задача обеспечения нормального теплового режима для каждого модуля ЭВС.

Проблема обеспечения одинаковых условий (по температурным воздействиям) для всех модулей аппаратуры стоит достаточно остро. Эта проблема может быть разрешена полностью или частично еще на ранних стадиях проектирования аппаратуры за счет правильной компоновки и размещения модулей различного уровня конструктивной иерархии: электрорадиоэлементов и интегральных микросхем на печатной плате, типовых элементов замены (ТЭЗ), ячеек и др. в блоках и блоков в рамах (стойках).

Наибольший интерес представляют надежностно-тепловые показатели.

Суммарная интенсивность (опасность) отказов λ_Σ модулей определяется выражением

$$\min \lambda_\Sigma = \min \sum_{i=1}^{n} \lambda_i(t_i),$$

где n – количество модулей; t_i – среднеповерхностная температура i-й группы модулей.

В общем случае зависимости $\lambda_i(t_i)$ аппроксимируются многочленами вида

$$\lambda_i(t_i) = B_{1i} + B_{2i}t_i + B_{3i}t_i^2 + B_{4i}t_i^3 + \ldots$$

где $B_{1i}, B_{2i}, B_{3i}, B_{4i}, \ldots$ – коэффициенты аппроксимации.

Поэтому для оценки интенсивности (опасности) отказов $\lambda_i(t_i)$ модулей необходимо знание среднеповерхностной температуры i-й группы модулей t_i.

В ходе работы было спроектировано программное обеспечение, позволяющие найти температуры каждой платы для двух моделей расчета: платы развернуты в одну сторону и платы развернуты в противоположные стороны. Для каждой модели типовые элементы замены возможно разметить вручную, методом «min-max» (чередование плат с максимальными и минимальными температурами) и методом «седло» (на краях блока располагаются платы с максимальными температурам, а к центру – с наименьшими).

Используя вычисленные температуры, программа позволяет рассчитать коэффициенты аппроксимации B_{2i}, которые вносят наибольший вклад в величину $\lambda_i(t_i)$ (около 20%). Затем для каждой платы вычисляется значение интенсивности отказов.

Также программа снабжена базой данных, позволяющей добавлять необходимые элементы, компоновать их в платы и собирать в блоки, а затем моделировать размещение.

АНАЛИЗ ПРОГРАММ ПО УЧЕТУ КОМПЬЮТЕРНОЙ ТЕХНИКИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

М.П. Чеплакова, студентка 3-го курса, каф. КИБЭВС
г. Томск, ТУСУР, milstar@inbox.ru

На кафедре КИБЭВС ведется разработка проекта, целью которого является проектирование и создание базы данных для регистрации и учета компьютерной техники и программного обеспечения. Немаловажную роль играет разработка непосредственно самого приложения для работы с базой данных.

Был проведен анализ рынка программ-аналогов данного направления, в частности внимание акцентировалось на бесплатные (PS Wizard, System Info for Windows) и условно-бесплатные (SiSoftware Sandra Lite) программы. Был сделан вывод, что проект актуален, так как позволяет наиболее удобно собирать и обрабатывать данные и упростить задачу инвентаризации на любом предприятии, в сравнении с другими программами-аналогами.

Результаты анализа были реализованы в виде таблицы. В качестве критериев были выбраны:

– информация о периферийных устройствах;
– информация о памяти;
– информация о дисках;
– информация о драйверах;
– информация о материнской плате, чипсете;
– наличие мастера создания отчетов;
– другие.

Результат анализа программ-аналогов приведен в таблице.

Результат анализа программ-аналогов

Программы-аналоги	SiSoftware Sandra Lite XII.SP1 (Win32 x86) (2008.1.13.12) Rus	PC Wizard	SIW (System Info for Windows)	DB-KEVA
Информация о материнской плате/чипсете	+	+	+	+
Информация о процессоре	+	+	+	+
Информация о видеокарте	+	+	+	+
Информация о принтере	+	+	+	+
– Информация о клавиатуре – Информация о мыши – Информация о звуковой карте	+	+	–	+
– Информация о памяти Windows – Информация о Windows	+	+	+	+

Продолжение таблицы

– Информация о модеме/ISDN TA – Информация о сети	+	+	+	+
– Информация о дисках (съемные жесткие диски, CD-ROM/DVD, RamDrives, и т.д.) – Информация о портах (последовательный, параллельный)	+	+	+	+
– Информация о драйверах	+	–	+	+
– Ключевые приложения* (веб-браузер, e-mail, новости, антивирус, брандмауэр и т.д.) – Установленные приложения* – Установленные программы*	+	+	–	+
– Мастер создания отчетов (сохранение, печать, отправка по факсу или e-mail в форматах CIM (SMS/DMI), HTML, XML, RPT или TEXT)	+	+	+	–
– Обширный файл помощи, содержащий более 500 подсказок	+	–	–	–
Лицензия (платная, бесплатная, условно-бесплатная)	У/б	Б	Б	Б
Архив	–	–	–	+
Ответственный работник	–	–	–	+
Периодическая сверка в автоматическом режиме информации	–	–	–	+
Централизованное хранение и обработка данных в базе данных	–	–	–	+

В результате анализа была поставлена задача разработать свой программный продукт, в котором выделены инновационные составляющие, такие как:

– архив;

– ответственный работник;

– периодическая сверка информации в автоматическом режиме;

– централизованное хранение и обработка данных в базе данных.

Кроме того, на разработку интерфейса повлияли программы-аналоги.

ЛИТЕРАТУРА

1. http://x-soft.tomsk.ru/

АВТОМАТИЗАЦИЯ ВВОДА ФОРМ

Д.О. Дмитриев, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, ddo_87@mail.ru

Вряд ли найдется человек, которому хотя бы раз в жизни не доводилось заполнять бланки. Анкеты, счета и другие подобные документы давно существуют в различных областях человеческой деятельности. С другой стороны, сегодня для хранения и обработки информации повсеместно используются компьютеры и компьютерные сети. Неудивительно, что перенос информации с бумажных бланков в компьютерное хранилище данных стал одной из самых актуальных задач в области документооборота.

Данная статья посвящена автоматизации работы приемной комиссии, в обязанности которой входит обработка большого количества документов. Как правило, используется ручной ввод информации в базу данных, хотя этот подход не оптимален как с точки зрения надежности, так и с точки зрения трудозатрат.

Альтернативный метод заключается в применении системы автоматизированного ввода данных. Рассмотрим особенности и основные стадии обработки форм этим методом:

– пачку заполненных форм сканируют при помощи скоростного сканера (обычно применяют аппараты с производительностью не менее 10 страниц в минуту);

– подавляющее большинство символов распознается автоматически;

– символы, относительно которых сложилось несколько гипотез, автоматически передаются для проверки оператору системы ввода;

– подтвержденная информация экспортируется в базу данных.

Таким образом, для создания автоматизированной системы необходимо выбрать аппаратные и программные средства, удовлетворяющие соответствующим требованиям.

К программной части предъявляются следующие требования: невысокая стоимость, хорошее качество распознавания рукописного текста, возможность обрабатывать документы различных типов, дружелюбный интерфейс, невысокие системные требования. Был проведен обзор наиболее известных современных программных продуктов, таких как: система ABBYY FormReader, «ЕВФРАТ-Документооборот», ЭЛАР «Саперион», система «Дело» компании ЭОС.

В результате анализа представленных продуктов было решено, что наиболее предпочтительной для нашего случая является система ABBYY FormReader, так как она обладает необходимым набором характеристик, при этом в ней отсутствуют функции, не используемые в данной предметной области. Тем более, что функция потокового ввода

форм многих сторонних программных продуктов реализована с применением технологии, разработанной фирмой ABBYY, например в системе «ДЕЛО» компании «Электронные офисные системы». Также данная система наиболее универсальна и проста в использовании.

От параметров выбранного сканера будут зависеть и скорость, и качество обработки данных. Следует сразу отметить, что при большом количестве форм обычные планшетные сканеры неприменимы. Эти устройства широко распространены в офисах, они неплохо справляются с оцифровкой фотографий и обычных документов, но для потокового ввода непригодны.

Для полноценного, быстрого и качественного ввода большого количества форм нужен специальный аппарат, предназначенный для ввода большого числа документов.

Основными требованиями к характеристикам сканера в условиях приемной комиссии являются: небольшие габаритные размеры, производительность начального уровня (до 20 страниц в минуту), оптическое разрешение сканирования не менее 300 dpi, возможность двухстороннего сканирования, максимальный формат документов не более A4, наличие USB-интерфейса.

На современном рынке не очень много фирм, занимающихся выпуском подобных сканеров, поэтому выбор был ограничен тремя наиболее известными марками: Canon, Kodak и Panasonic. В качестве наиболее подходящих были выбраны сканеры начального уровня: Canon DR-2080C, Kodak i250 и Panasonic KV-S1025C.

Таким образом, были выбраны наиболее подходящие программные и аппаратные средства для автоматизации ввода форм, которые могут быть использованы в работе приемной комиссии. В качестве программы для автоматизированного ввода форм была выбрана система ABBYY FormReader. В качестве аппаратных средств был выбран сканер Canon DR-2080C.

ЛИТЕРАТУРА

1. http://www.eos.ru – официальный сайт компании ЭОС.

2. http://saperion.ru – официальный сайт компании ЭЛАР.

3. http://www.evfrat.ru – официальный сайт компании Cognitive Technologies.

АВТОМАТИЗАЦИЯ РАБОТЫ ПРИЕМНОЙ КОМИССИИ

Д.О. Дмитриев, студент 5-го курса, каф. КИБЭВС,
Н.А. Новгородова, ассистент каф. КИБЭВС
г. Томск, ТУСУР, ddo_87@mail.ru

Работа приемной комиссии очень кропотлива и трудоемка. В ее задачи входит прием и учет абитуриентов, подавших заявления на поступление в вуз. При этом многие операции производятся вручную. От руки заполняются заявления о сдаче вступительных экзаменов, договоры о приеме студентов на основе полного возмещения затрат на обучение. Вся информация о студентах вводится в базу данных также вручную. Ежегодно в вуз поступают тысячи студентов, поэтому задача автоматизации является очень актуальной.

Целью работы является максимальная автоматизация процессов работы приемной комиссии. Работы ведутся в трех направлениях:

– ввод информации в базу данных о студентах и абитуриентах с помощью программного средства;

– ввод информации с помощью системы автоматизированного ввода форм;

– ввод всей информации абитуриентом через Web-интерфейс.

Первое направление представляет собой программу, которая позволяет напрямую работать с информацией, хранимой в базе данных. Программа способна редактировать абсолютно всю информацию о студентах: личные данные, контактная информация, информация о принятых документах, результаты экзаменов и тестирований, информация о родственниках и др. Также в программе реализован удобный поиск среди студентов и абитуриентов. Данное направление уже используется на практике и показало себя с лучшей стороны, однако были выявлены и недоработки, которые постепенно устраняются.

Второе направление представляет собой систему автоматизированного ввода печатных форм. Заполнение заявлений и договоров при этом происходит вручную на бумажных формах. Далее происходит сканирование бумажных носителей с помощью потокового сканера, который способен быстро и качественно сканировать большое количество документов. После этого полученные изображения передаются в программу, которая распознает заполненные поля форм и заносит полученную информацию в базу данных. На данный момент такая система практически готова к работе. Для работы приемной комиссии были оптимально подобраны аппаратные и программные средства. В качестве аппаратных средств был выбран сканер Canon DR-2080C. В качестве программной части была выбрана система ABBYY FormReader 6.5.

Третье направление представляет собой ввод информации в базу данных с помощью Web-интерфейса. Абитуриент самостоятельно вводит необходимую информацию на Web-сайте, а затем отправляет эту информацию на сервер. Это значительно облегчает работу как приемной комиссии, так и самих абитуриентов. Им теперь не нужно приезжать в вуз только для того, чтобы подать заявление на поступление. На данный момент это направление находится в стадии разработки.

ЛИТЕРАТУРА

1. http://abbyy.ru – официальный сайт компании ABBYY.
2. http://www.tusur.ru – официальный сайт ТУСУР.

СИСТЕМА АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ВЫСШИМ УЧЕБНЫМ ЗАВЕДЕНИЕМ. ПОДСИСТЕМА СРАВНЕНИЯ УЧЕБНЫХ ПЛАНОВ

Р.А. Добрынин, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, romsato@sibmail.com

Характерными особенностями образовательных учреждений и в целом системы образования Российской Федерации являются многоплановость их видов деятельности, региональные отличия, индивидуальная специфика каждого образовательного учреждения в организации учебного процесса, управлении научными исследованиями, в управлении административно-хозяйственной и финансово-экономической деятельностью, в проведении кадровой политики, в реализации социальных программ и т.д. Поэтому решение проблем управления образовательными учреждениями немыслимо без их полной информатизации на основе одной из современных информационных систем и без создания инфраструктуры управления развитием образования [1].

Основой построения ИС и реализации в ней современных управленческих методик является процессный подход. Деятельность учебного заведения рассматривается как последовательность взаимосвязанных процессов, проходящих через все подразделения, задействующих все службы и ориентированных на реализацию поставленных стратегических целей.

Благодаря тому, что в основе всего учебного процесса лежит учебный план (УП), подсистема управления учебными планами является одной из основополагающих в таких системах. Сегодня в каждом учебном заведении существует большое количество изучаемых дисциплин, которые входят в состав учебных планов различных специальностей. Отсюда вытекает вопрос о сравнении учебных планов.

Сравнение УП позволяет:

− установить возможность перевода студента с одной специальности на другую;

− отслеживать динамику изменения состава предметов, часовой нагрузки, способа отчетности и другой статистической информации;

− выполнять сравнение УП различных специальностей и/или различных годов;

− сравнивать ГОСТы различных специальностей;

− проверять соответствие учебного плана ГОСТу специальности;

− осуществлять поиск претендентов на переподготовку.

В ходе работы должно быть разработано Windows-приложение, выполненное по клиент-серверной технологии.

Основные требования к клиентской части:

− должна быть реализована процедура идентификации и аутентификации;

− приложение должно иметь возможность открывать базу данных учебных планов, находящуюся на удаленном сервере;

− критерии сравнения задаются пользователем;

− представление выходной информации в виде отчетов о результате сравнения.

Алгоритм сравнения двух учебных планов представлен на рис. 1. Четыре блока данного уровня отражают последовательность действий для решения задачи [2].

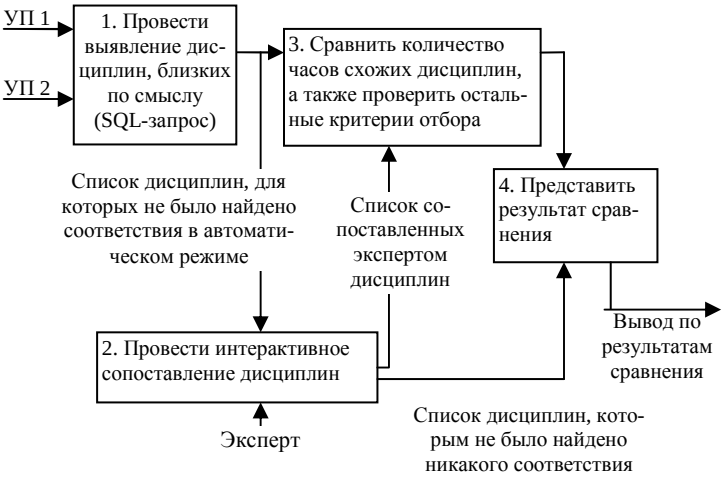


Рис. 1. Алгоритм сравнения учебных планов

Из рис. 1 видно, что разрабатываемая система относится к классу экспертных. Сокращение нагрузки на эксперта осуществляется применением алгоритмов нечеткого поиска и представлением списка дисциплин, для которых не было найдено четкого соответствия в автоматическом режиме, после применения данных алгоритмов и установления нечетких связей.

Изменения, происходящие как в экономической жизни страны, так и системе высшего образования, не могли не отразиться на тех требованиях, которые предъявляются к информационной системе современного российского вуза. Сегодня стоит вопрос о трансформации вузовских систем из систем учета в системы управления, позволяющие интегрировать задачи управления с текущей деятельностью функциональных подразделений и администрации вуза [3].

Подсистема управления учебными планами (как и подсистема сравнения учебных планов в частности), с возможностью интегрирования в глобальную систему автоматизации управления учебным заведением, будет крайне полезна как для работников деканатов, кафедр и т.п. в их повседневной деятельности, так и для других подразделений, способных оперативно получать необходимую информацию и на ее основе принимать управленческие решения.

ЛИТЕРАТУРА

1. «Университет» управляет университетом // «КомпьютерПресс». № 5. 2000.

2. Эпп В.В. Информационная поддержка согласования регионального рынка труда и выпуска специалистов с высшим образованием. Пенза, 2007.

3. Иевенко М.В. Использование встроенных методик ERP-решений при внедрении системы «Университет». М., 2004.

ПОВЕРКА ПОГРУЖНЫХ ВИХРЕВЫХ РАСХОДОМЕРОВ ИМИТАЦИОННЫМ СПОСОБОМ

А.С. Фролов, аспирант, каф. электротехники

г. Красноярск, ГОУ ВПО «Сибирский государственный технологический университет»

Как в промышленности, так и в коммунальном хозяйстве существует потребность достоверного измерения расхода воды или различных растворов. В последнее время в России появился новый класс вихревых расходомеров и водосчетчиков, называемый погружными кондуктометрическими. В них тело обтекания (ТО) устанавливается непосредственно в рабочий трубопровод. Приемник-преобразователь

вихревых колебаний (ППВК) помещается в специальном канале тела обтекания, который называется каналом обратной связи (КОС). Он представляет собой два электрода, один из которых колеблется в такт с частотой вихреобразования, при этом частота изменения электрического сопротивления межэлектродного промежутка является выходным сигналом, несущим информацию о расходе. Для поверки таких водосчетчиков и расходомеров применяются два метода поверки: проливной и беспроливный (имитационный) метод.

Проливной метод осуществляется на соответствующей проливной установке – это устройство (эталон), предназначенное для поверки и регулировки счетчиков жидкости.

Достоинством проливных установок является возможность поверки на них расходомеров и водосчетчиков практически любых конструкций. В большинстве случаев они позволяют испытывать приборы при «нормальных» условиях: измеряемая среда – вода, оссимметричный стационарный поток, трубопровод протяженный, отсутствие сторонних помех и т.п.

К сожалению, проливная установка, особенно на большой диаметр условного прохода (более 300 мм), – крайне дорогое и редкое в России оборудование [1].

Кроме того, обслуживание проливной установки процесс очень дорогостоящий, трудоемкий, установке требуется отдельное помещение, что весьма удорожает поверку приборов.

В настоящее время практика имитационной поверки преобразователей расхода широко распространена, но, к сожалению, не подходит ко всем существующим типам расходомеров.

Беспроливный (имитационный) метод поверки осуществляется на специальных имитационных стендах. Для вихревых кондуктометрических расходомеров суть этого метода поверки заключается обычно в электрическом моделировании напряжения на электродах первичного преобразователя расходомера, являющегося носителем информации о величине расхода [2].

Также условия испытания на существующих имитационных стендах весьма далеки от рабочих. Обычно они ограничиваются подачей на вход прибора заранее заданных электрических сигналов и наблюдения за реакцией на выходе, то есть эти методики позволяют проверить только электрический тракт прибора при сигналах, форма которых может быть далека от реального [3].

Качество имитационной поверки можно повысить, если создать стенды, которые будут имитировать не электрические сигналы, а реальные гидродинамические явления, происходящие в расходомере. Стенд, который соответствует этому принципу работы, изображен на

рис. 1. Он представляет собой цилиндрическую камеру *1*, торцевые стенки которой представляют собой мембраны *2* и *3*. Камера заполняется жидкостью через патрубки *8* и *9*. Через пробку *10* из нее выпускается остаточный воздух. Поперек камеры устанавливается перегородка *4*, в которую вставляется тело обтекания испытываемого расходомера *5*. Боковые стенки тела обтекания с отверстиями канала обратной связи (КОС) должны быть направлены параллельно перегородке [4].

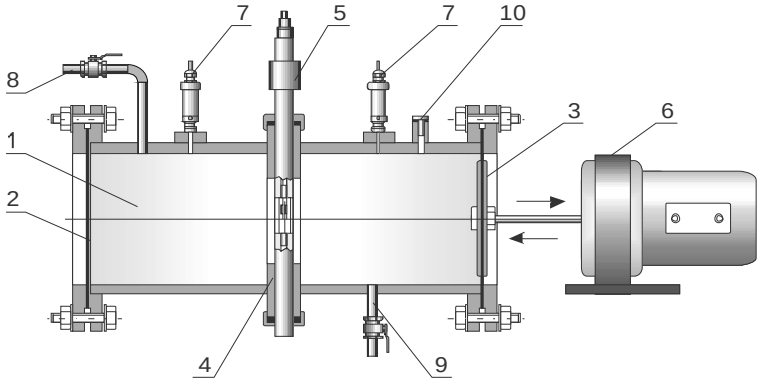


Рис. 1. Стенд для испытаний погружных вихревых расходомеров

Одна из мембранных стенок камеры, снабженная жестким центром *3*, приводится в колебательное движение специальным электромагнитным приводом *6*. При этом на торцевые стенки ТО, т.е. на срез канала обратной связи ТО, будет действовать знакопеременный перепад давления, имитирующий вихреобразование. Камера снабжается датчиком перепада давления на перегородке. Им служат два измерительных преобразователя давления SITRANS P (фирмы Siemens) *7*, включенные по дифференциальной схеме.

Задачей стенда является создание на срезе КОС (боковых поверхностях тела обтекания) перепада давления, по величине и форме соответствующего реальному, который действует в вихревом расходомере. При этом внутри КОС установится знакопеременный переток жидкости по форме и величине, также соответствующий реальному. Таким образом, на стенде будут имитироваться реальные гидродинамические процессы, протекающие в КОС, и взаимодействие их с чувствительным элементом расходомера – кондуктометрическим ППВК.

ЛИТЕРАТУРА

1. Вельт И.Д., Михайлова Ю.В. // Приборы и системы управления. 1997. № 11.

2. Лурье М.С. Имитационное моделирование вихревых расходомеров / М.С. Лурье, С.П. Жуков // Вестник КрасГАУ. 2005. № 7. С. 254–258.

3. Лурье М.С. Имитационная поверка погружных кондуктометрических вихревых расходомеров / М.С. Лурье, В.Н. Волынкин, Э.М. Шейнин // Измерительная техника. 2005. № 12. С. 38–41.

4. Пат. 2282830 РФ, МПК G 01 F 25/00. Имитационный стенд для поверки вихревых расходомеров, Лурье М.С., Плотников С.М., 24.01.2005. Зарегистрирован в Государственном реестре изобретений РФ 27.08.2006.

МОНИТОРИНГ СОБЫТИЙ В КОМПЬЮТЕРНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Д.О. Гайдай, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, sk8erboi@rambler.ru

В работе каждого администратора наступает момент, когда больше нет ни желания, ни возможности самостоятельно следить за состоянием оборудования и за состоянием того или иного сервиса. В такой ситуации на помощь приходят системы мониторинга, позволяющие ограничить круг наблюдаемого ПО и оборудования только наиболее критичным и собственно контролем работы мониторинга. В зависимости от задач, для которых они создавались, системы мониторинга имеют различный уровень функциональности и сложности. В данной работе будет использоваться мониторинг событий системы [1].

Мониторинг – методика и система наблюдений за состоянием определенного объекта или процесса, дающая возможность наблюдать их в развитии, оценивать, оперативно выявлять результаты воздействия различных событий. Результаты мониторинга дают возможность вносить корректировки по управлению объектом или процессом [2].

Файлы регистрации событий – ценный инструмент для мониторинга сети и производительности, которые часто используются в недостаточной мере из-за их сложности и объема. По мере роста организации ей требуется более структурированный подход к управлению файлами регистрации событий и их хранению. Недавнее исследование, проведенное институтом SANS, обнаружило, что 44% системных администраторов не хранят файлы регистрации более одного месяца [3].

Цель работы заключается в разработке и реализации частной политики безопасности на основе мониторинга событий компьютерных информационных систем.

Актуальность работы обеспечивается:

– разработкой частной политики безопасности для нескольких информационных систем;

– исследованием мониторинга, направленным на повышение информационной безопасности в системах обработки данных;

– разработкой и введением в работу инструкций по настройке и безопасности информации.

Хорошая стратегия безопасности включает мониторинг относящихся к безопасности критических событий в режиме реального времени и периодического анализа журналов безопасности систем таким образом, чтобы можно было обнаружить и своевременно отреагировать на внутренние и внешние атаки. В действительности, производя обзор управления в организации, аудиторы и органы государственного регулирования определяют мониторинг журнала безопасности.

Для будущей работы была выбрана система мониторинга GFI EventsManager.

Преимущества системы:

– сокращение административных и технических расходов на управление, хранение и стоимость преобразования очевидно бессмысленных файлов регистрации событий в значимые отчеты о безопасности для администрирования;

– определение закономерности событий и предупреждение атак с помощью мощной базы данных правил GFI EventsManager;

– предупреждения в реальном времени помогут избежать затрат на восстановление, которое в противном случае последовало бы из-за сетевых атак;

– используя превентивный подход, уменьшается риск нарушения непрерывности бизнеса, чего, возможно, избежали бы благодаря надлежащему управлению файлами регистрации;

– повышение производительности благодаря сокращению ручного труда сотрудников;

– информационная система и сетевая безопасность;

– непревзойденная система обнаружения событий, масштабируемая до более 6 млн событий в час;

– предварительно настроенные правила обработки для эффективной классификации событий и управления;

– настройка с помощью мастера упрощает управление и обслуживание [4].

Основной целью работы является составление алгоритмов и написание скриптов, чтобы следить за состоянием системы и для автоматизации управления по мониторингу событий в компьютерных информационных системах и упрощению работы администратора.

ЛИТЕРАТУРА

1. Курс «Методология внедрения» Лекция № 13. Мониторинг Active Directory [Электронный ресурс] – Режим доступа: http://www.intuit.ru/department/os/msactivedir/13/

2. Википедия – свободная энциклопедия [Электронный ресурс] – Режим доступа: http://ru.wikipedia.org/

3. CompoWiki: Журнал событий [Электронный ресурс] – Режим доступа: http://wiki.compowiki.info/ZhurnalSobytijj

4. GFI – факс-сервер, антивирус Exchange, антиспам, управление безопасностью и архивирование почты [Электронный ресурс] – Режим доступа: http://gfi.ru/eventsmanager/

ОПТИМАЛЬНОЕ РАЗМЕЩЕНИЕ МОДУЛЕЙ ВТОРОГО УРОВНЯ В ГЕРМЕТИЧНОМ БЛОКЕ ЭЛЕКТРОННОГО СРЕДСТВА

С.В. Гавриш, студент 5-го курса, КИБЭВС

г. Томск, ТУСУР, mind@ms.tusur.ru

Обеспечение нормального теплового режима является одним из основных факторов, определяющих надежность аппаратуры различного целевого назначения. Поэтому проблема обеспечения одинаковых условий (по температурным воздействиям) для всех модулей аппаратуры стоит достаточно остро. Эта проблема может быть разрешена полностью или частично еще на ранних стадиях проектирования аппаратуры за счет правильной компоновки и размещения модулей различного уровня конструктивной иерархии: электрорадиоэлементов и интегральных микросхем на печатной плате, типовых элементов замены (ТЭЗ), ячеек и др. в блоках и блоков в рамах (стойках) [1].

При конструировании блоков электронных средств используются две тепловые модели блоков с герметичным корпусом, представленные на рис. 1 и 2.

Типовые элементы замены с размерами l_x, l_y и с эффективными толщинами d_n, которые определяются из условия равенства объемов печатной платы с элементами и гладкой пластины [2].

Расчетная модель введена в программный комплекс и позволяет производить расчет температурных режимов и надежности, а также ставить эксперименты по нахождению наилучшего варианта расстановки плат. В программе протестированы 4 стандартных вида расстановок плат: «MiniMax», «MiniMax2», «Седло», «Седло2».

Для проведения сравнительного анализа методов размещения модулей использовались одинаковые входные данные.

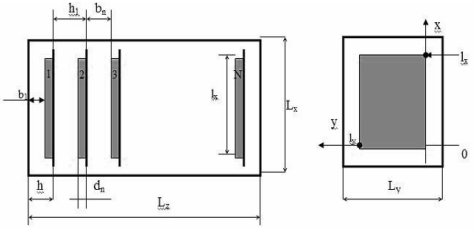


Рис. 1. Тепловая модель GERM1 блока
с герметичным корпусом

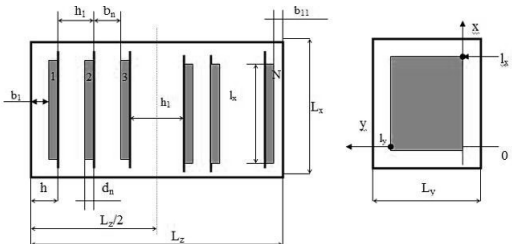


Рис. 2. Тепловая модель GERM2 блока
с герметичным корпусом

Таким образом, наиболее важными для анализа являются параметры:

– максимальное значение температуры;

– минимальное значение температуры;

– минимальная разница значений температуры;

– минимальная разница значений надежности,

из которых каждый должен стремиться к своему минимальному значению.

Для каждого из методов проводилось 100 перестановок модулей и сохранялись варианты расстановки и номер хода при минимальном значении каждого параметра. Для удобства сравнения результаты были сведены в таблицы и сгруппированы по исследуемым параметрам.

По результатам проведенных расчетов установлено, что модель GERM-1 имеет минимальный разброс температур среди предложенных вариантов, равный 4,15 град, что обеспечено высоким значением минимальной температуры для модели метода «Седло». Минимальный разброс надежности составляет $869{,}3 \cdot 10^{-9}$ 1/ч («MiniMax»). В свою очередь разброс значений по модели GERM-2 равен: для температуры 3,71 град («MiniMax2»); для надежности $866{,}6 \cdot 10^{-9}$ 1/ч («MiniMax»).

В ходе сравнения результатов также было выявлено, что:

– при достижении одним параметром минимального значения другие параметры могут принимать довольно высокие, отрицательно сказывающиеся на надежностно-тепловых свойствах ЭС в целом;

– нет одного явно выраженного метода с наиболее оптимальными низкими значениями исследуемых параметров;

– два метода размещения сохраняют низкие значения остальных параметров при достижении минимального значения одного, а именно «MiniMax» и «Седло2»;

– наиболее весомым является показатель максимальной температуры и разницы значения надежности, которые позволяют все же выделить метод «Седло2».

Сравнительный анализ результатов моделирования позволяет принять за основной метод расстановки модулей 2-го уровня в ЭС «Седло2» для модели Germ2. Этот метод дает в целом наиболее низкие значения максимальных температур модулей, при этом позволяя достигать минимальных значений остальных важных параметров. Данная закономерность объясняется физической моделью метода. В модели Germ2, как видно из рис. 2, используется большой зазор между развернутыми модулями, размещенными в центре. Разворот модулей позволяет направить тепловой поток к краям, где происходит охлаждение за счет контакта корпуса с внешней средой, а также максимально снижается нагрев центральных плат. Метод расстановки модулей «Седло2» на место центральных ставит модули с наибольшим тепловыделением. За счет объединения свойств метода и модели значения температур наиболее низкие, а следовательно, и надежность модулей повышается.

ЛИТЕРАТУРА

1. Дульнев Г.Н. Методы расчета теплового режима приборов. М.: Радио и связь, 1990. 312 с.

2. Карапетян А.М. Автоматизация оптимального конструирования ЭВМ. М.: Сов. радио, 1973. 152 с.

ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОГО ОБЪЕМА АВТОМАТИЗАЦИИ ПРИ РАЗРАБОТКЕ АСУ ТП

Н.А. Гиркин

г. Сургут, ОАО «Сургутнефтегаз»,
т. 8-914-255-44-18, nikitagirkin@mail.ru

В настоящее время объем автоматизации объектов капитального строительства ОАО «Сургутнефтегаз» постоянно увеличивается. Отличительной особенностью автоматизации объектов ОАО «Сургут-

нефтегаз» является большое количество однотипных объектов, что позволяет накапливать опыт эксплуатации и постоянно совершенствовать технологии.

При разработке очередной АСУ ТП возникает необходимость определения оптимального объема автоматизации – числа регистрирующих датчиков, исполнительных механизмов, средств визуализации, предупредительной и аварийной сигнализации, дистанционного управления.

Недостаточный объем автоматизации может привести к повышенной нагрузке на оперативный персонал объекта, снижению качества технологического процесса, возникновению нештатных и аварийных ситуаций. Избыточный объем автоматизации может привести к повышенной нагрузке на персонал служб АСУ и КИПиА, увеличить стоимость строительства и эксплуатации АСУ ТП.

Для разработки методов определения оптимального объема автоматизации предлагается использовать ряд методов, два из которых изложены в данной статье.

Первый метод основан на расчете и последующем сравнении, с одной стороны, стоимости и трудоемкости разработки, наладки и эксплуатации АСУТП, с другой стороны – экономического и технологического эффекта от эксплуатации АСУТП.

Предлагается для расчета и последующего сравнения выделить основные функции, выполняемые АСУТП, и по каждой функции рассчитать объем выполнения.

Рассмотрим основные функции АСУ ТП и выделим т.н. «единицу выполнения функции» (стоимость и эффект которой можно потом отдельно рассчитать):

1. Регистрация и визуализация значений технологических параметров. Единица выполнения функции – визуализация значения одного параметра.

2. Дистанционное управление. Единица выполнения функции – управление одним исполнительным устройством.

3. Автоматические защиты и блокировки. Единица выполнения функции – защита одной единицы оборудования.

4. Автоматическое регулирование. Единица выполнения функции – регулирование одного технологического параметра.

5. Хранение информации в базе данных и формирование отчетных форм. Единица выполнения функции – запись и хранение в базе данных значений одного параметра.

6. Предупредительная и аварийная сигнализация. Единица выполнения функции – сигнализация по значению одного параметра.

7. Диагностика работоспособности оборудования АСУ ТП. Единица выполнения функции – контроль работоспособности одного датчика, входа/выхода контроллера, связи с одним контроллером и сервером.

Для каждой функции АСУ ТП предлагается определить набор оборудования и программного обеспечения, необходимый для выполнения единичной функции.

Используя статистические данные по уже эксплуатируемым АСУ ТП, предлагается рассчитать среднюю суммарную стоимость разработки, строительства, наладки и длительной эксплуатации комплекса технических и программных средств, выполняющих единичные функции АСУ ТП.

С другой стороны, предлагается рассчитать технологическую эффективность длительной эксплуатации единичных функций АСУ ТП через повышение эффективности работы оперативного персонала, оперативное предупреждение возникновения нештатных и аварийных ситуаций, повышение стабильности регулирования технологических процессов.

В результате применения первого метода у заказчика АСУ ТП появляется набор статистических данных, которые он может использовать по своему усмотрению при определении объема автоматизации. Например, усредненные данные по тому, сколько будет стоить установить один датчик и какой технологический эффект от этого будет получен.

Второй метод основан на использовании имеющегося опыта эксплуатации АСУ ТП однотипных объектов и определении излишних и недостающих средств автоматизации на уже запущенных объектах.

Для определения излишних средств автоматизации предлагается проанализировать записи значений технологических параметров в базах данных серверов верхнего уровня по каждому отдельному технологическому узлу, агрегату, площадке за длительный период времени.

Так, предлагается анализировать зарегистрированную в базе данных частоту регистрации изменения показаний по отдельному датчику и для датчиков с редко меняющимися показаниями, не обладающими высокой важностью, принимать решение о замене таких регистрирующих датчиков на индицирующие датчики в новых АСУ ТП.

Для контуров автоматического регулирования предлагается анализировать зарегистрированную в базе данных продолжительность работы в ручном и автоматическом режиме, а также скорость изменения управляющего воздействия, и для контуров, большую часть времени находящихся в ручном режиме или в одном из положений, принимать решение об изменении таких контуров в новых АСУ ТП.

Для определения недостающих средств автоматизации предлагается проанализировать записи в сменных журналах и отчетах о работе оперативного персонала объектов. Дополнительно предлагается проанализировать причины и подробности возникновения нештатных и аварийных ситуаций на эксплуатируемых АСУ ТП.

Анализ работы оперативного персонала объектов автоматизации и аварийных ситуаций дает возможность определить технологические узлы, агрегаты, площадки, которые могут быть автоматизированы с наибольшим эффектом при разработке следующей АСУ ТП.

Описанные методы определения оптимального объема автоматизации являются достаточно трудоемкими и далеко не исчерпывающими. Предлагается проводить перерасчет и анализ работы действующих АСУ ТП один раз в год, и в течение года использовать полученные данные при разработке новых АСУ ТП.

СИСТЕМА АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ НАСОСОМ ОТКАЧКИ ПОДЗЕМНОЙ ЕМКОСТИ

Е.С. Хамова, студентка 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-404-24-87, milenochka_87@mail.ru

Система сбора и подготовки нефти является одной из важнейших частей нефтегазодобывающих предприятий. Поэтому ей нужно уделять особое внимание т.к. цена на нефть полностью зависит от качества переработки нефти, а качество переработки нефти в свою очередь зависит от эффективности работы системы сбора и подготовки нефти.

Объектом исследования в данной работе является цех подготовки и перекачки нефти (ЦППН) НГДУ «Быстринскнефть», ОАО» Сургутнефтегаз». ЦППН расположен на территории Быстринского месторождения – центрального пункта сбора и подготовки нефти, газа и воды.

Спроектированная система автоматического управления насосом откачки подземной емкости на ЦППН предназначена для поддержания заданного оптимального уровня нефтяной эмульсии в подземной емкости, контроля за ходом технологического процесса, управления насосами и задвижками, сбором информации о параметрах материальных потоков нефти и о состоянии всего технологического оборудования. Разработанная система на базе микропроцессорного контроллера ГАММА-8М позволяет автоматизировать процесс откачки, сократить число аварий, увеличить производительность установки, повысить точность и надежность измерений.

В данной работе рассмотрен технологический процесс откачки нефтепродуктов из подземной емкости в резервуарный парк на объекте

ЦППН, обоснован выбор технических средств автоматизации управления насосом откачки (подземная емкость, датчики уровня и давления, контроллер, кабельная продукция и т.д.).

Подземные емкости предназначены для подземного хранения и последующей откачки темных и светлых нефтепродуктов, а также хранения агрессивных и неагрессивных химических продуктов. На объекте ЦППН эта емкость используется для слива нефти, остатков нефтепродуктов из технологических аппаратов (печей, электродегидраторов). Нефтяная эмульсия из подземной емкости ЕП-1 поступает в резервуарный парк для отстаивания и разделения эмульсии на нефть и воду, а товарная нефть поступает в товарный парк для дальнейшей транспортировки потребителям. Образовавшийся в емкости газ поступает на прием компрессорной станции [1].

Для перекачки нефти в резервуарный парк используется насос внешней откачки высокой производительности. Для охлаждения баббитовых подшипников вала насоса применяется техническая вода, которая после охлаждения утилизируется в дренажную емкость. После того как емкость наполнилась жидкостью из утечки сальниковых уплотнителей насоса, она откачивается в резервуар – отстойник (РВС) [2].

При наполнении емкости до верхнего запрограммированного допустимого уровня, включается насос откачки подземной емкости и происходит ее откачка. При достижения минимального запрограммированного уровня, происходит остановка насоса откачки, и емкость снова наполняется.

Система автоматизации процесса откачки нефти из емкости в резервуарный парк обеспечивает автоматическое регулирование следующих параметров:

– контроля уровня в подземной емкости;

– температуру измеряемой среды;

– контроля давления насоса откачки.

Для управления насосом откачки на подземную емкость устанавливаются два датчика, с помощью которых производится измерение уровня, температуры и давления. Уровень жидкости в емкости измеряется датчиком уровня с встроенным датчиком температуры [3]. Давление контролируется датчиком давления [4].

Вся информация поступает в виде сигналов с датчиков на контроллер ГАММА-8М, который расположен в местном пункте управления (МПУ), затем по интерфейсу RS485 передается на верхний уровень в операторную, где оператор с помощью графического интерфейса производит контроль и управление технологическим процессом. Автоматизированное рабочее место оператора находится в операторной на территории ЦППН. Оператор всегда имеет необходимую ин-

формацию о технологических параметрах и состоянии технологического оборудования и в случае необходимости может осуществить требуемые операции для обеспечения безопасности (отключить технологические агрегаты, выполнить необходимые переключения потоков, остановить технологический процесс).

Определенную сложность представляет сбор информации на центральный пункт оператору, а в целом рассмотренный технологический процесс позволяет эффективно управлять откачкой нефти на объекте ЦППН. Также данный объект интересен в плане последующего сокращения издержек и оптимизации расходов на подобного вида сооружения. Система автоматического управления может быть использована на любых системах подобного назначения, является расширяемой.

ЛИТЕРАТУРА

1. Технологический регламент УПСВ «Б» Быстринского месторождения НГДУ «Быстринскнефть». ТР-39-4528-08.

2. Лутошкин Г.С. Сбор и подготовка нефти, газа и воды. М.: Недра, 1987. 192 с.

3. http://www.albatros.ru. Каталог продукции ЗАО «Альбатрос». Техническая документация. М., 2008.

4. http://www. teplocomplect.ru. Каталог продукции сайта ООО Теплокомплект. Датчики давления ДМ 2005. М., 2005.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЛЯ УЧЕТА И КОНТРОЛЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТУРЫ В ЛОКАЛЬНОЙ СЕТИ

А.О. Ирхин, студент 5-го курса, каф. КИБЭВС,
Н.А. Новгородова, ассистент каф. КИБЭВС
г. Томск, ТУСУР, bring@sibmail.com

В основе проекта лежит разработка базы данных для учета программного обеспечения и аппаратуры на компьютерах в организации и управление этой базой данных: ручное и полуавтоматическое заполнение базы данных информацией.

Эта тема актуальна на сегодняшний момент, так как в любой организации, крупной или малой, ведется учет компьютеров и их обеспечения, как программного, так и аппаратного. Чем больше организация, тем больше компьютеров, тем больше оргтехники, подключенной к ним, и программ, используемых на них.

Для удобства компьютеры объединены в локальную сеть (local area network, LAN) – компьютерную сеть, т.е. систему связи двух или более компьютеров или компьютерного оборудования (серверы, прин-

теры, факсы, маршрутизаторы и другое оборудование). Обычно размещается в одном здании и принадлежит отдельной организации.

Компьютерной сетью управляет администратор вычислительной сети (также называемый сетевой администратор, англ. network administrator) – сотрудник, отвечающий за работу компьютерной сети предприятия в штатном режиме.

Перед каждым сетевым администратором стоит задача не только следить за работой компьютеров в локальной сети, но и вести учет этих компьютеров и всей информацией о них. Хорошо, если компьютеров в локальной сети не очень много, но если их количество превышает десятки, тогда сбор информации о компьютерах будет отнимать довольно много времени. Чтобы облегчить работу администратора по учету компьютеров и их комплектующих, существует множество программ, которые могут собирать информацию о программном и аппаратном обеспечении в локальной сети. Несомненным достоинством при этом является наличие единого хранилища, базы данных.

При работе над данным проектом преследуется цель – ускорить работу по сбору информации, а также автоматизировать заполнение базы данных этой информацией.

Задачи, которые ставятся для достижения данной цели:

– подбор программного обеспечения для сбора информации о компьютерах в локальной сети;

– проектирование базы данных для хранения информации о компьютерах в локальной сети;

– автоматизация процесса заполнения базы данных информацией о компьютерах в локальной сети.

На рис. 1 представлена модель «сущность–связь» разработанной базы данных.

Также было выбрано программное обеспечение, которое будет собирать полную информацию о компьютерах локальной сети.

В настоящее время решается задача автоматического заполнения базы данных. Разрабатывается алгоритм, пишется программный код, который будет отвечать за заполнение базы данных собранной информацией.

Реализация данного проекта будет способствовать ускорению сбора информации, а также будет значительно снижать время, которое затрачивает администратор на учет компьютеров в локальной сети.

ЛИТЕРАТУРА

1. Контолли Т., Бегг К., Страчан А. Базы данных: проектирование, реализация и сопровождение. Теория и практика. М.: Диалектика, 2000. 1120 с.

2. Новиков Ю.В., Кондратенко С.В. Основы локальных сетей. М.: Интернет-университет информационных технологий, 2005. 360 с.

ОПРЕДЕЛЕНИЕ ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ С ПОМОЩЬЮ СИНТЕЗА РЕЧЕВОГО СООБЩЕНИЯ

В.А. Ягницын, студент 5-го курса, каф. КИБЭВС,
Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС
г. Томск, ТУСУР, khalem@ms.tusur.ru

Современный уровень развития вычислительной техники и ее повсеместное внедрение в человеко-машинных системах управления делают актуальной организацию общения человека и компьютера в одной из наиболее удобных для человека форм – в форме речевого диалога на естественном языке. Речевой способ общения в человеко-машинных системах имеет принципиальные преимущества, главными из которых являются следующие:

– удобство, естественность и простота общения, не требующая специальной подготовки, что существенно расширяет круг потенциальных пользователей вычислительных систем и повышает эффективность их использования;

– разгрузка зрительного канала при выводе информации и устранение ручных манипуляций при вводе, что увеличивает оперативность взаимодействия с компьютером и уменьшает число ошибок оператора [1].

Создание систем речевого общения с ЭВМ требует решения двух основных проблем: проблемы автоматического синтеза и проблемы автоматического анализа и распознавания речи.

Несмотря на широкий набор разработок, проблема синтеза речи до сих пор считается решенной лишь удовлетворительно. До сих пор нет общего мнения, какой из существующих подходов дает наилучшие результаты, какие модели синтеза речи являются наиболее перспективными.

В то же время в связи с широким распространением компьютерных технологий сильно возросла потребность в определении того, кем является пользователь системы: человеком или компьютером.

Для решения этой проблемы был предложен тест Тьюринга, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером. Однако для систем, основанных на распознавании символов, существуют методы, позволяющие с достаточно большой вероятностью обмануть эту систему.

Целью данной работы является разработка и реализация системы определения пользователя компьютера с помощью синтеза речевого сообщения, позволяющей использовать преимущества систем синтеза речи и недостатки систем распознавания речи, а также национальные и языковые особенности русского языка.

Все способы синтеза речи можно подразделить на три группы:

– параметрический синтез;

– конкатенативный, или компиляционный (компилятивный) синтез;

– синтез по правилам.

Современная интерпретация теста Тьюринга звучит следующим образом: «Человек взаимодействует с двумя компьютерами. 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».

По состоянию на 2008 г. ни одна из существующих компьютерных систем не приблизилась к прохождению теста [3].

Наиболее распространенной реализацией теста Тьюринга является CAPTCHA.

CAPTCHA (от англ. «Completely Automated Public Turing test to tell Computers and Humans Apart») – компьютерный тест, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером. 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.

CAPTCHA чаще всего используется при необходимости предотвратить использование Интернет-сервисов ботами, в частности, для предотвращения автоматических отправок сообщений, регистрации, скачивания файлов, массовых рассылок и т.п.

В наиболее распространенном варианте CAPTCHA от пользователя требуется ввести символы, как правило, изображенные на предлагаемом ему рисунке в искаженном виде, иногда с добавлением шума или полупрозрачности [4].

Могут также применяться другие плохо алгоритмизуемые задачи, например: узнать, что находится на картинке, отметить все картинки с кошками или ответить на вопрос, связанный со знаниями или менталитетом людей (например, «висит груша, нельзя скушать»).

Существуют программы, распознающие конкретные реализации CAPTCHA, к примеру, PWNtcha. Кроме того, существует возможность подключать модули из программ распознавания текста общего назначения (например, FineReader) в программы сторонних разработчиков для распознавания картинок CAPTCHA.

В качестве альтернативы широко распространенной CAPTCHA, использующей картинку с изображением, предлагается использовать синтез речевого сигнала. Причем, применяя синтез речи в подобных системах, можно сразу определить ряд преимуществ данного метода:

– использование фраз, оборотов и других языковых особенностей русского языка заметно повышает устойчивость к машинной обработке;

– уровень развития современных систем распознавания речи не способен в большинстве случаев верно ответить на вопросы, связанные с менталитетом или другими национальными особенностями, причем при искусственном зашумлении речевого сигнала точность распознавания резко ухудшается;

– речевое общение между компьютером и человеком требует очень высокого уровня осмысления речевых сообщений, на которое современные компьютеры просто не способны.

ЛИТЕРАТУРА

1. Лобанов Б.М. Компьютерный синтез и клонирование речи / Б.М. Лобанов, Л.И. Цирульник. Минск: Белорус. наука, 2008. 343 с.

2. http://ru.wikipedia.org/wiki/Синтез_речи.

3. http://ru.wikipedia.org/wiki/Тест_Тьюринга.

4. http://ru.wikipedia.org/wiki/Captcha.

КОЛЛЕКТИВНОЕ ПОВЕДЕНИЕ АВТОНОМНЫХ РОБОТОВ

К.В. Картавцев, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, konstanteen@sibmail.com

В последние годы в области робототехники и искусственного интеллекта активно разрабатываются мультиагентные робототехнические системы. При этом роботы рассматриваются как интеллектуальные агенты, имеющие собственные базы данных и знаний и каналы связи для обмена информацией между собой в процессе решения общей задачи.

Целью данной работы является разработка и реализация алгоритма взаимодействия и коллективного поведения группы автономных роботов.

При решении рассматриваемой задачи был применен мультиагентный подход. В рамках данного подхода задача работы сводится к разработке:

1) программной модели автономного робота, обладающего бионической нейроноподобной системой автономного адаптивного управления;

2) модели кооперативного поведения автономных роботов;

3) модели окружающей среды;

4) модели и механизмов взаимодействия агентов.

Данный метод позволяет решить следующие задачи интеллектуального управления моделями робототехнических систем:

– оптимальное планирование маршрута движения роботов в среде с препятствиями с использованием локальной (сенсорной) или глобальной информации (информации, поступающей от других роботов);

– распознавание в виртуальном пространстве ситуаций и принятие оптимальных решений;

– программирование и адаптивная коррекция движений агентов по спланированным маршрутам;

– адаптивное управление движением агентов.

При построении модели коллективного поведения автономных роботов необходимо проанализировать методы разрешения конфликтов.

Для предотвращения столкновений (конфликтов) роботы-агенты могут передавать по каналам связи команды о своей временной остановке или об изменении скорости и ускорения их движения в зависимости от сложившейся ситуации. Эта ситуация оценивается другими роботами. Идея разрешения конфликтов заключается в заблаговременном изменении роботами скорости движения по спланированным маршрутам.

При возникновении опасности столкновения один из роботов может изменить скорость движения.

Другие способы разрешения конфликтов относятся к тактическому уровню. Они основываются на локальных моделях виртуальной реальности и на обмене информацией о маршруте и скорости движения между локальными системами управления роботов.

Каждого робота можно рассматривать как интеллектуальный объект с собственной базой данных и знаний, который может адаптироваться к заранее неизвестным или изменяющимся характеристиками среды с препятствиями. Поэтому большая часть этой работы должна быть посвящена методам обучения и адаптации отдельных автономных роботов на локальном уровне управления.

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.

Свойствами и особенностями автономных роботов являются:

– способность к коллективному целенаправленному поведению;

– автономность, т.е. способность самостоятельно решать локальные задачи перемещения;

– способность автоматически приспосабливаться к неопределенным условиям среды, способность обучаться;

– мобильность, т.е. способность активно перемещаться.

Внешний вид разрабатываемой компьютерной модели автономного робота изображен на рис. 1.

Модель робота имеет круглый корпус и снабжен визуальным и тактильным датчиками. Визуальный датчик обеспечивает регистра-

цию препятствий, находящихся в секторе – области видимости робота, с заданной фиксированной площадью и геометрией. Также робот обладает тактильными датчиками, которые должны сигнализировать о соприкосновении препятствия с корпусом робота.

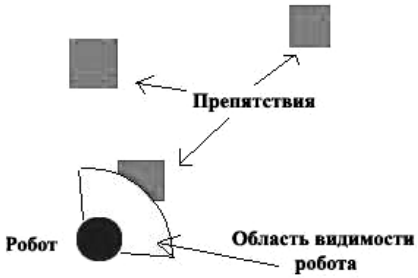


Рис. 1. Модель автономного робота

Система управления автономным роботом должна включать в себя следующие подсистемы:

– подсистему формирования и распознавания образов;

– базу знаний;

– подсистему оценки состояния;

– аппарат эмоций;

– подсистему выбора действия – аппарат принятия решений [3].

Управляющая система должна будет взаимодействовать со средой с помощью блока датчиков и исполнительных органов.

В управляющей системе автономного адаптивного управления взаимосогласованно решаются несколько задач, соответствующих перечисленным подсистемам.

Подсистема формирования и распознавания образов предназначена для решения задачи автоматической классификации и структурирования информации, поступающей с визуального и тактильного датчиков.

Каждая конкретная ситуация запоминается в базе знаний, благодаря чему возможно проведение сравнений, выбора наилучшего действия.

ЛИТЕРАТУРА

1. Тимофеев А.В. Мультиагентные системы планирования поведения транспортных роботов в среде с препятствиями // Экстремальная робототехника. X научно-техническая конференция. СПб., 1999.

2. Станкевич Л.А. Мультиагентная технология в когнитивных системах управления автономными роботами // Экстремальная робототехника. X научно-техническая конференция. СПб., 1999.

3. Крыжановский М.В., Магомедов Б.М. Организация нейросетевой базы знаний в интеллектуальных управляющих системах. М., 1980.

4. Уоссерман Ф. Нейрокомпьютерная техника: теория и практика. М.: Мир, 1982.

К ВОПРОСУ УПРАВЛЕНИЯ РЕЖИМАМИ ТЕРМИЧЕСКОЙ ОБРАБОТКИ ТРАНСПОРТНОГО МЕТАЛЛА

И.С. Хлыст, студент 6-го курса, каф. ПрЭ
г. Томск, ТУСУР, т. 633-503, khlyst@mail.npptec.ru

Отвод тепла от нагретого тела всегда занимал обособленное место в разных сферах деятельности человека, будь то электронные устройства или транспортный металл (рельсы). Для получения требуемых показателей от рельсов необходимо управлять процессом термообработки. Сразу возникают вопросы по расчетам теплообмена, по подбору сред и рабочих условий, по проведению экспериментов и других мероприятий с целью получения способа и технологии.

Существующие нормативные документы, проект ГОСТ 51685–2000 и стандарт EN13674-1 требуют от рельсов дифференцированной термообработки и фиксированных показателей структуры металла. Для обеспечения заданных показателей были проведены исследования и построен экспериментальный стенд по контролю режимов термообработки транспортного металла, который станет технологическим базисом для автоматизированной системы дифференцированной термообработки рельсов.

Основной задачей экспериментального стенда является управление процессом охлаждения металла.

Был проведен анализ различных сред охлаждения по экологическим и технико-экономическим показателям, результатом которого является широкое использование воздуха и водовоздушных сред для термической обработки рельсов.

Составом проектной группы научно-производственного предприятия «Томская электронная компания» были сформированы основные требования к стенду, в которых говорится о необходимости использования стали марки 76ЭФ для рельсов; обеспечения скорости охлаждения фазы аустенитного состояния металла от 2 до 8 °С/с; измерения состояния параметров узлов системы и температуры образцов; применения оборудования, отвечающего промышленным стандартам и обеспечивающего надежную работу стенда; использования SCADA-системы для визуализации и параметрирования стенда.

При разработке стенда было необходимо сформировать структуру системы управления таким образом, чтобы можно было с достаточной легкостью проводить эксперименты и максимально приблизиться к структуре автоматизированной системы управления дифференцированной термообработкой рельсов. Функциональная схема системы управления представлена на рис. 1.

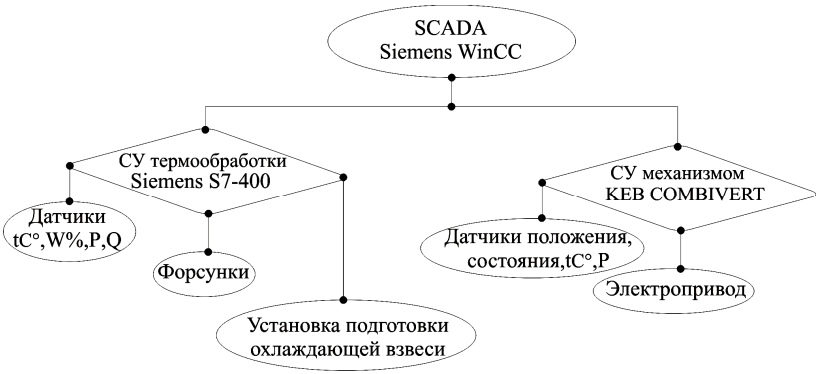


Рис. 1. Функциональная схема системы управления экспериментальным стендом

В качестве охлаждающей среды была выбрана водовоздушная взвесь, которая давала максимальную скорость охлаждения металла 24 °С/с. Длина экспериментальных образцов рельсов 700 мм.

Экспериментальные исследования показали, что для достижения требуемых свойств рельсов процессы и режимы охлаждения должны иметь непрерывный характер, но при определенной дискретизации подачи охлаждающей среды и воздуха инерционность металла сводила дискретный процесс к непрерывному (рис. 2).

В результате цикличной и постоянной подачи на образец водовоздушной взвеси были получены значения скоростей охлаждения образца рельса в диапазоне от 1 до 24 °С/с.

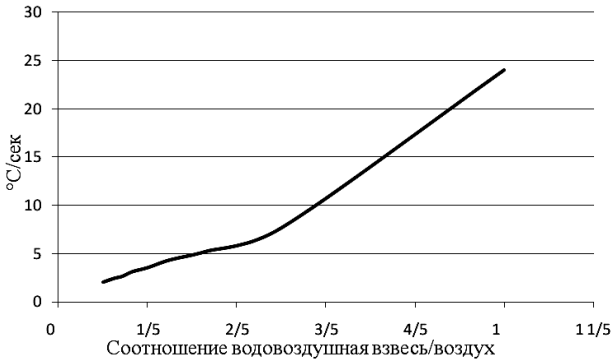


Рис. 2. Зависимость скорости охлаждения экспериментального образца от соотношения подачи водовоздушная взвесь/воздух

При разработке программно-алгоритмического обеспечения пришлось столкнуться с проблемой одновременного управления многими параметрами установки, т.к. они взаимосвязаны между собой. Например: необходимо обеспечить заданную температуру, влажность и давление водовоздушной среды.

Исследования продолжаются и вскоре перейдут к этапу математического описания основных экспериментальных зависимостей и характеристик, с помощью методов теплообмена и математических аналогий. Проводится анализ режимов и скоростей процессов охлаждения рельсов. Эти данные помогут в моделировании процессов управляемого охлаждения в программных пакетах, например: CosmosFloWorks или ANSYS. Необходимо провести корреляцию между реальными процессами и симулируемыми, для того чтобы в дальнейшем использовать модель для оптимизации режимов дифференцированной термообработки и работы с рельсами различного химического состава. Параллельно с моделированием будет набираться статистический материал для подтверждения математических расчетов моделей.

ЛИТЕРАТУРА

1. Вороненко В.П., Егоров В.А., Косов М.Г. Проектирование автоматизированных участков и цехов. М.: Высш. шк., 2003. 272 с.

2. Павлов В.В., Темлянцев М.В., Корнева Л.В. Дефекты и качество рельсовой стали. М.: Теплотехник, 2006. 218 с.

3. Siemens Simatic. Компоненты для комплексной автоматизации: «Техника автоматизации и приводы». М.: Сименс, 2007. 169 с.

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ОТДЕЛЬНЫМ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ ИЛИ ОБОРУДОВАНИЕМ ДЛЯ УГОЛЬНЫХ ШАХТ

К.В. Климентьев, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-403-32-74, klim42rus@mail.ru

Система Davis Derby Ltd использует современное, испытанное и проверенное оборудование, отвечающее требованиям современной угольной шахты.

Полная система может быть описана как ряд подсистем, соединенных с комнатой поверхностного диспетчера. По сути, шахтная система контроля и управления состоит из распределенных по шахте разнообразных датчиков, которые через подземные контроллерные станции (подстанции), посредством искробезопасной системы передачи данных, соединены с поверхностной компьютерной SCADA-системой, которая обеспечивает необходимый пользовательский интерфейс,

а также представляет управленческую информацию и необходимые пользователю мнемонические дисплеи.

Это система контроля и управления в реальном времени, которая имеет сетевую структуру. Она обеспечивает полный контроль безопасности, производства продукции, имеет функции управления и администрирования, а также средства для сбора данных в реальном времени, передачи, обработки, отображения, записи и распечатки параметров, характеризующих состояние контролируемого процесса или оборудования. Эта система, распространенная на контроль за основными технологическими операциями в шахте, является основной для обеспечения безопасности людей и механизмов.

Основными применениями, где необходим контроль и управление, являются следующие:

1. Общий контроль рудничной атмосферы по таким параметрам, как концентрация метана CH_4, скорость воздуха, содержание кислорода, оксида углерода и других токсичных газов, позволяет быстро реагировать на изменение газовой ситуации.

2. Автоматическое отключение электроэнергии, в случае высоких концентраций метана и других взрывчатых газов, предотвращает подземные взрывы, вызываемые электрическим искрением и искрением машин. Многие системы контроля рудничной атмосферы дополнительно осуществляют контроль и управление проветриванием.

3. Подземные вентиляторы могут быть включены/выключены с поверхности, что позволяет исключить сбои в режиме вентиляции в шахте. Автоматизация шахтного водоотлива приводит к уменьшению затрат на ремонт и обслуживание.

Контроль и управление конвейерами увеличивает коэффициент использования оборудования и позволяет рационально использовать обслуживающий персонал.

Использование в системе управления конвейерами экстренного останова натяжного типа существенно повышает безопасность персонала, работающего или перемещающегося вдоль конвейера.

Защита конвейерных лент от проскальзывания позволяет избежать риска возгорания ленты из-за ее ослабления или провисания. Блок управления конвейером может также использоваться для автоматического управления лебедкой натяжения ленты, предотвращая, таким образом, проблемы с ее чрезмерным или недостаточным натяжением.

Зашита пересыпов и контроль смещения ленты избавляют от риска нарушения ленты и приводов конвейеров.

Система управления конвейером может включать поверхностное управление цепочкой подземных конвейеров последовательным за-

пуском и остановом «одной кнопкой», что увеличивает время продуктивной работы транспортной системы.

Дополнительный непрерывный контроль температуры и вибрации моторов и редукторов позволяет спланировать обслуживание / замещение моторов/редукторов и организовать эти операции во время естественной остановки, что позволяет избежать их поломок и повысить надежность и производительность.

Контроль мощности, потребляемой механизмами, а также времени их работы дает ценную информацию специалистам шахты для расчетов расписания техобслуживания и эффективности работы механизмов.

Предлагается эффективная двухсторонняя громкоговорящая связь между поверхностным диспетчером и подземными абонентами, например хорошо зарекомендовавшая себя система связи DIS5. Ее использование позволяет повысить безопасность горных работ путем легкой переадресации сообщений, а также за счет объединения предстартовой сигнализации с системой управления. Система громкоговорящей связи может также использоваться для автоматического извещения шахтеров об аварийной ситуации в определенном месте шахты.

Многие функции контроля и управления могут быть объединены в одном общем блоке контроля и управления. Обычно система способна включать в себя до 60 подземных подстанций (Minewatch 3) или кластеров (Minewatch PC21). При использовании подстанций Minewatch 3 общая емкость такой системы составляет 1920 дискретных входов, 840 аналоговых и примерно 480 выходов управления. Однако система может быть легко расширена на большее количество входов/выходов.

ПРОГРАММНАЯ ЧАСТЬ КОНТРОЛЛЕРА ДЛЯ ЖКХ

Е.Ю. Копьев, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, xxxmasterxxx@sibmail.com

Целью данной работы является разработка программной части контроллера для жилищно-коммунального хозяйства (ЖКХ).

Бизнес-идея данного проекта – это аппаратно-программный комплекс, который может быть использован в сфере жилищного хозяйства.

Данный контроллер должен измерять сигналы, поступающие от аналоговых и дискретных датчиков технических параметров, формировать дискретные и аналоговые выходные сигналы для управления исполнительным оборудованием, формировать, хранить и передавать предупредительные и аварийные сигналы.

Начальным этапом создания контроллера для ЖКХ является анализ аналоговых устройств. Проведен анализ необходимых датчиков и исполнительного оборудования для контроллера. Были изучены контроллеры МС8 и МС12, предназначенные для автоматизированного управления, контроля и мониторинга разнообразных технологических процессов на объектах ЖКХ. Определены технические характеристики, программное обеспечение, функциональные возможности, количество и виды датчиков, необходимых для работы контроллера, выявлены управляемые объекты.

В состав программного обеспечения контроллеров входят следующие компоненты:

Операционная система (ОС). ОС обеспечивает связь с другими контроллерами внутри сети, между контроллерами и оборудованием (датчики, исполнительные органы и т.д.), между Master-контроллером и верхним уровнем, осуществляет выполнение функционального алгоритма: загрузка, инициализация, исполнение или отключение. Кроме того, ОС выполняет функцию самодиагностики. ОС записывается в контроллеры производителем и не может быть изменена потребителем.

Функциональный алгоритм (ФА). Контроллеры МС8 являются свободно программируемыми. ФА разрабатывается при помощи графической инструментальной системы КОНГРАФ. Загрузка исполняемого кода в контроллер осуществляется программой КОНСОЛЬ. Для организации диспетчеризации (мониторинг и управление) предлагается различное программное обеспечение: КОНТАР SCADA (используется глобальный Интернет-сервер, доступ к которому обеспечивается с любого компьютера, подключенного к Интернет через обычный Web-браузер), КОНТАР АРМ и OPC-сервер для применения других SCADA-систем. Программы КОНГРАФ, КОНСОЛЬ, КОНТАР-АРМ, OPC-сервер поставляются вместе с контроллером на CD-диске.

ЛИТЕРАТУРА

1. Сайт KIPIA.SU

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПО УЧЕТУ НАГРУЗКИ ПРЕПОДАВАТЕЛЕЙ И ЗАТРАТ НА КОМАНДИРОВКИ

Ю.А. Коптелина, студентка 6-го курса, каф. КИБЭВС,
Н.А. Новгородова, ассистент каф. КИБЭВС
г. Томск, ТУСУР

Базы данных и интерфейсы к ним становятся наиболее актуальной и динамически развивающейся областью в сфере информационных

технологий. Учебный план, нагрузка преподавателей и учет затрат на командировки не являются исключением в этой области.

Разрабатываемая автоматизированная система состоит из двух подсистем:

– подсистемы для учета нагрузки на преподавателя;

– подсистемы для учета затрат на командировки.

Вся информация в системе хранится в реляционной базе данных.

Сущность «преподаватель» обладает следующими атрибутами:

– ФИО;

– должность;

– фото;

– звание;

– степень;

– др.

Сущность «группа» обладает следующими атрибутами:

– номер группы;

– год набора;

– учебный план.

Сущность «нагрузка» обладает следующими атрибутами:

– вид обучения;

– преподаватели;

– семестр;

– учебный план.

По учету затрат на командировки учитываются приказы, преподаватели, затраты. Поездка преподавателя может быть по разным направлениям.

Сущность «приказы» обладает следующими атрибутами:

– номер приказа;

– преподаватели;

– дата;

– др.

Сущность «направления» обладает следующими атрибутами:

– откуда;

– куда;

– приказы.

Сущность «список затрат» обладает следующими атрибутами:

– название затрат;

– дата;

– сумма;

– документы.

Для работы с базой данных в настоящее время создается программный модуль автоматизированной системы. Основными функ-

циями данной системы являются учет нагрузки на преподавателя и учет затрат на командировки. Программа представляет собой программу «клиент», работающую с базой данных, установленной на сервере.

КОНТРОЛЛЕР ДЛЯ ЖКХ

Л.С. Краев, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, xxxmasterxxx@sibmail.com

Всего лишь несколько лет назад контроллер российского производства был диковиной. В настоящее время более 30 отечественных фирм производят контроллеры и активно продвигают их на рынок. Интерес предпринимателей к разработке и выпуску этой продукции обусловлен растущей потребностью в автоматизации производства и сокращении обслуживающего персонала в условиях тотального дефицита квалифицированных специалистов, возможностью небольшим коллективом в десяток конструкторов и минимальными затратами, изготовить любую конфигурацию контроллера на базе микропроцессорных компонентов и типового программного обеспечения зарубежных производителей.

Целью данной работы является разработка аппаратной части контроллера для ЖКХ.

Бизнес-идея данного проекта – это аппаратно-программный комплекс, который может быть использован в сфере жилищного хозяйства.

Данный контроллер должен измерять сигналы, поступающие от аналоговых и дискретных датчиков технических параметров, формировать дискретные и аналоговые выходные сигналы для управления исполнительным оборудованием, формировать, хранить и передавать предупредительные и аварийные сигналы.

Функциональная схема контроллера МС12 приведена на рис. 1.

Объектом исследования являются данные, относящиеся к работе информационной системы по учету студентов ГПО.

Начальным этапом создания контроллера для ЖКХ является анализ аналоговых устройств. Проведен анализ необходимых датчиков и исполнительного оборудования для контроллера. Были изучены аналоги контроллеров МС8 и МС12, предназначенные для автоматизированного управления, контроля и мониторинга разнообразных технологических процессов на объектах ЖКХ. Контроллер позволяет осуществлять сбор информации от любых источников (датчики температуры, давления, расхода, тепло-, водо-, электросчетчики и т.п.) и передавать ее на верхний уровень с использованием различных каналов свя-

зи. Контроллер МС12 содержит универсальный блок питания, рассчитанный на питание как от источников переменного тока (от 12 до 30 В), так и постоянного тока (от 11 до 36 В, например, от аккумуляторов). Блок питания обеспечивает нечувствительность прибора к форме питающего напряжения, что особенно важно при плохой форме сети, вызываемой работой силовых частотных преобразователей.

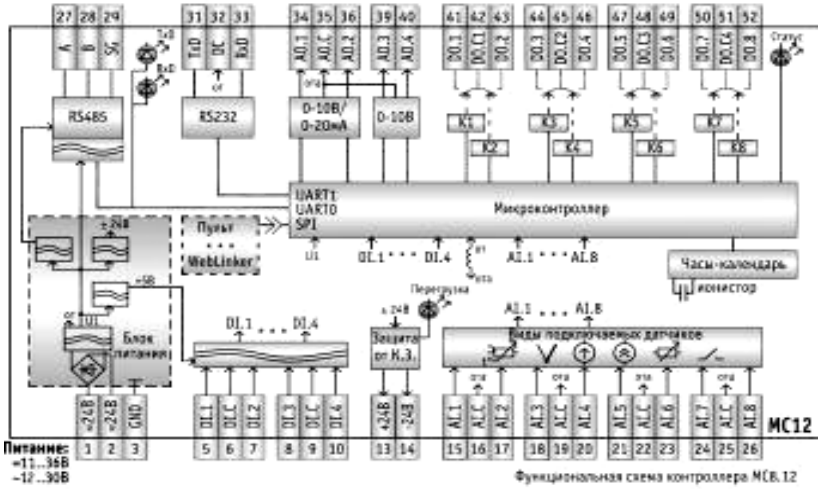


Рис. 1. Функциональная схема контроллера МС12

Прибор имеет 12 выходов: 4 аналоговых и 8 дискретных. Дискретные выходы выполнены в виде контактов электромеханических реле (0,3 А, 250 В).

Прибор имеет стабилизированный источник для питания датчиков (24 В, 80 мА), гальванически отделенный от остальных цепей. Этот узел оснащен защитой от долговременного короткого замыкания во внешних цепях, возникающего при ошибках монтажа на объекте. Наличие такого замыкания индицируется специальным светодиодом перегрузки [1]. Определены технические характеристики, программное обеспечение, функциональные возможности, количество и виды датчиков, необходимых для работы контроллера, выявлены управляемые объекты.

ЛИТЕРАТУРА

1. Сайт KIPIA.SU

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ПРОЕКТИРОВАНИЮ ПОРТА ВВОДА-ВЫВОДА

Е.А. Кузнецов, студент 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, jokerasu@sibmail.com

В соответствии с инновационной стратегией группового проектного обучения по теме «Устройство цифрового управления объектом (ГОС СД.05 от 2000 г.)» с октября 2006 г. была начата работа группы КИБЭВС-11 по созданию порта ввода-вывода на «монтажной ИЛИ».

Аппаратные средства поддержки обмена процессора с периферией включены в регистровое арифметико-логическое устройство (РАЛУ). Здесь возможны следующие соглашения: «Каждый регистр подключен к каналу, и каждый регистр связан с каждым», как предложено в [1].

Примем для РАЛУ следующие СОГЛАШЕНИЯ – «о статусе шин, поддерживающих эти требования», т.е. выделим управляемые шины BUS2, BUS3 и BUS4 для следующих целей: шина BUS2 – для чтения данных с регистров и передачи их на обработку; шина BUS3 – для записи данных на регистры; шина BUS4 – для загрузки шины адресов-данных (KAD) системного канала со стороны процессора (рис. 1).

Системный канал представлен шиной адресов-данных (KAD).

Рассмотрим СОГЛАШЕНИЯ:

1) выход на шину BUS4 имеют только рабочие регистры RA и RD; 2) выход на шину BUS2 должны иметь все РОН и рабочие регистры RD, RGK; 3) шина REZ подключена к шине BUS3; 4) все РОН и рабочие регистры могут принимать данные с шины BUS3; 5) данные системного канала загружают шину BUS3 через управляемую шину DA.

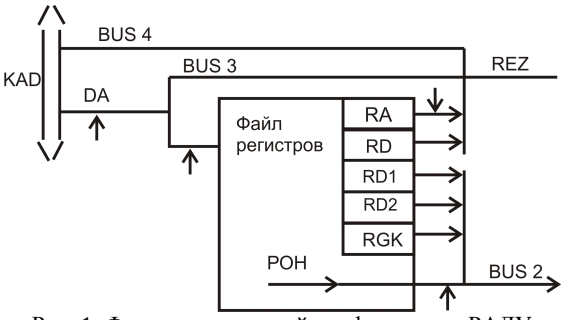


Рис. 1. Фрагмент принятой конфигурации РАЛУ

Анализ требований предложенных выше СОГЛАШЕНИЙ приводит к следующим результатам:

1) выход REZ необходимо подключить к BUS3 для фиксирования результата обработки на одном из регистров; 2) выходы рабочих регистров RA и RD необходимо подключить к шине BUS4. Другие регистры РАЛУ (RD1, RD2, RGK) имеют возможность передавать данные через шину BUS2 в блок обработки данных.

Примем следующие СОГЛАШЕНИЯ:

1) выход на шину BUS4 имеют только рабочие регистры RA и RD; 2) выход на шину BUS2 должны иметь все РОН и рабочие регистры RD1, RD2, RGK; 3) все РОН и рабочие регистры могут принимать данные с шины BUS3; 4) данные системного канала загружают шину BUS3 через управляемую шину DA.

Требования принятого выше блока СОГЛАШЕНИЙ поясняет рис. 1.

Таким образом, только регистры RA и RD подключены к каналу, а остальные регистры РАЛУ имеют возможность передать данные через шину BUS2.

Расчет мощности для варианта «Монтажное ИЛИ». Для начала необходимых расчетов понадобится определить количество элементов в схеме, число паек. Все данные отражены в табл. 1.

В табл. 1 число элементов, паек рассчитаны для 4-разрядной секции, а для 16-разрядной – соответственно будет в 4 раза больше.

Потребляемая мощность всей схемы рассчитывается суммированием всех мощностей микросхем (табл. 2):

$$P_{\text{общ}} = P_1 + P_2 + P_3 + \ldots P_n,$$
$$P_1, P_2 \ldots = I_{\text{пот}} * U_{ип}.$$

Таблица 1

Число элементов, паек

Наименование элементов	Количество элементов в схеме	Количество паек
1. Резисторы постоянные	16	32
2. Конденсаторы керамические	23	46
3. Разъем	2	64
4. Интегральные схемы:		
К155ЛН-1	2	28
К155ЛА-8	5	80
К155ТМ-8	4	64
К1533АП-26	1	16
К155ТМ-7	1	16
К155ИД4	1	16
К1533ИП-2	6	96
ИТОГО	61	458

Таблица 2

Расчет мощности

Наименование элемента	Количество элементов, *n*	Ток потребления, мА	Напряжение питания, В	Потребляемая мощность, мВт
К155ЛН-1	2	33	5	330
К155ЛА-8	5	22		550
К155ТМ-8	4	45		900
К1533АП-26	1	130		650
К155ТМ-7	1	53		265
К155ИД-4	1	40		200
К1533ИП-2	6	26		780
ИТОГО	20			3675

Следовательно, общая потребляемая мощность составляет: $P_{\text{общ}} = 3{,}675$ Вт.

В табл. 2 расчет мощности рассчитаны для 4-разрядной секции, а для 16-разрядной – соответственно будет в 4 раза больше.

ЛИТЕРАТУРА

1. Прищепа Л.С. Аппаратные средства вычислительной техники: В 5 разд. Разд. 2. Базовые модели учебных ЭВМ: учеб. Пособие. Томск: В-Спектр, 2006. 162 с.

РАСЧЕТ НАДЕЖНОСТИ ДЛЯ ВАРИАНТА С «МОНТАЖНЫМ ИЛИ»

Е.А. Кузнецов, студент 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, jokerasu@sibmail.com

Надежность – это свойство изделия выполнять заданные функции, сохраняя свои эксплуатационные показатели в течение требуемого промежутка времени или требуемой наработки.

Для расчета надежности необходимо рассчитать такие значения, как интенсивность отказов, суммарная интенсивность отказов, наработка на отказ, вероятность безотказной работы.

В табл. 1 рассчитаны минимальные и максимальные значения интенсивности отказов.

Суммарная интенсивность отказов высчитывается по формулам:

$\lambda_{\max} = \sum N * \lambda_{i\max}\, 10^{-6}$ ч$^{-1}$;

$\lambda_{\min} = \sum N * \lambda_{i\min}\, 10^{-6}$ ч$^{-1}$;

$\lambda_{\max} = (1{,}12 + 37{,}72 + 0{,}124 + 4{,}58 + 14{,}2) = 18{,}904 * 10^{-6}$ ч$^{-1}$;

$\lambda_{\min} = (0{,}16 + 1{,}426 + 0{,}124 + 4{,}58 + 0{,}19) = 6{,}48 * 10^{-6}$ ч$^{-1}$.

Таблица 1

Минимальные и максимальные значения интенсивности отказов

Наименование элементов	Количество элементов в схеме N	$\lambda_{i\,\max}$ 10^{-6}, ч$^{-1}$	$\lambda_{i\,\min}$ 10^{-6}, ч$^{-1}$	$N \cdot \lambda_{i\,\max}$ 10^{-6}, ч$^{-1}$	$N \cdot \lambda_{i\,\min}$ 10^{-6}, ч$^{-1}$
Резисторы постоянные	16	0,07	0,01	1,12	0,16
Конденсаторы керамические	23	1,64	0,042	37,72	1,426
Разъем	2	0,062	0,062	0,124	0,124
Пайки	458	0,01	0,01	4,58	4,58
Интегральные микросхемы	20	0,71	0,0095	14,2	0,19

Наработка до отказа:

$T_{\max} = 1/\lambda \min\ 10^{-6}$ ч$^{-1}$;

$T_{\min} = 1/\lambda \max\ 10^{-6}$ ч$^{-1}$.

С учетом коэффициента $a = 10$ (при работе в лаборатории):

$T_{\max} = 1/*18{,}904 * 10^{-5}$ ч$^{-1} = 5289$ ч;

$T_{\min} = 1/*6{,}48 * 10^{-5}$ ч$^{-1} = 15432$ ч.

Вероятность безотказной работы:

$P_{\max}(t) = e^{-\lambda \max * t}$, где $t = 1000$;

$P_{\min}(t) = e^{-\lambda \min * t}$;

$P_{\max}(t) = 0{,}135$;

$P_{\min}(t) = 0{,}607$.

Технико-экономическое обоснование разработки. При *обосновании целесообразности проведения работы* учитывались следующие аспекты.

При проектировании электронно-вычислительных средств и комплексов на их основе используют новейшие методы, например имитационное моделирование экспериментальных установок с привлечением средств вычислительной техники. Так, после представления вычислительной системы на уровне структурной, а затем функциональной электрической схемы необходима проверка принятых решений еще до этапа разработки опытно-конструкторской документации. Вариантом проверки решений может быть исследование объекта на программных (имитационных) моделях.

В данной работе последовательно рассмотрен концептуальный подход к проектированию порта ввода – вывода регистрового АЛУ.

Структурная схема доведена до уровня функциональной, а после выбора элементной базы представлен вариант решения электрической принципиальной схемы.

Технико-экономическое обоснование выполняется для определения целесообразности проведения работы. Для этого выполняется комплекс работ: организационно-экономическое обоснование, расчет сметы затрат на разработку.

Расчет эксплуатационно-технического уровня. Для обобщенной характеристики качества модели можно использовать обобщающий индекс эксплуатационно-технического уровня J, который можно определить как произведение частных индексов. Для учета значимости отдельных параметров может быть рекомендован балльный индексный метод:

$$J = \sum_{i=1}^{n} B_i \cdot X_i,$$

где J – комплексный показатель качества модели по группе показателей; n – число рассматриваемых показателей; B_i – коэффициент весомости i-показателя; X_i – относительный показатель качества, устанавливаемый экспертным путем по выбранной шкале оценивания.

Расчет показателя составляющих и самого показателя J представлен в табл. 2.

Таблица 2

Расчет показателя качества балльным индексным методом

Показатели качества	Коэффициент весомости	Разрабатываемый ПП с «Монтажным ИЛИ»		Разрабатываемый ПП с мультиплексируемой шиной		Аналог	
		X_i	$X_i \cdot B_i$	X_i	$X_i \cdot B_i$	X_i	$X_i \cdot B_i$
1. Качество работы	0,2	6	1,2	7	1,4	4	0,8
2. Возможность дальнейшей автоматизации	0,2	4	0,8	5	1	1	0,2
3. Экономия ЭРЭ	0,1	10	1	10	1	2	0,2
4. Простота в управлении	0,2	7	1,4	7	1,4	3	0,6
5. Рациональность	0,3	8	2,4	8	2,4	5	1,5
		$J_1 = 6{,}8$		$J_2 = 6{,}8$		$J_3 = 3{,}1$	

Как видно из таблицы, разработанная система имеет гораздо более высокий показатель эксплуатационно-технического уровня J по сравнению с аналогом.

Вычислим коэффициент технического уровня:

$$A_к = \frac{J_П}{J_А},$$

где $J_П$ – комплексный показатель качества разрабатываемого продукта; $J_А$ – комплексный показатель качества аналога.

$$A_к = 6{,}8 \div 3{,}1 = 2{,}19,$$

$$A_к = 6{,}8 \div 3{,}1 = 2{,}19.$$

Видно, что проведение работы с технической точки зрения оправдано.

ЛИТЕРАТУРА

1. Прищепа Л.С. Аппаратные средства вычислительной техники: В 5 разд. Разд. 2. Базовые модели учебных ЭВМ: учеб. пособие. Томск: В-Спектр, 2006. 162 с.

РОБОТИЗИРОВАННЫЙ КОМПЛЕКС ДЛЯ УПРАВЛЕНИЯ ВНУТРИСЕРДЕЧНЫМ ЭЛЕКТРОДОМ

Я.Г. Лазарев, А.А. Захаров, студенты 3-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-407-78-45, bacer90@mail.com

Аритмии сердца – это нарушения частоты, ритмичности и последовательности сокращений отделов сердца. Причины ее – это врожденные аномалии или структурные изменения проводящей системы сердца при различных заболеваниях, а также вегетативные, гормональные или электролитные нарушения при интоксикациях и воздействиях некоторых лекарств. В норме электрический импульс, родившись в синусовом узле, расположенном в правом предсердии, идет по мышце в предсердно-желудочковый узел, а оттуда по пучку Гиса непосредственно к желудочкам сердца, вызывая их сокращение. Изменения могут произойти на любом участке проводящей системы, что вызывает разнообразные нарушения ритма и проводимости. Они бывают при нейроциркуляторной дистонии, миокардитах, кардиомиопатиях, эндокардитах, пороках сердца, ишемической болезни сердца. Аритмии часто являются непосредственной причиной смерти [1].

Это определяет важность высокотехнологической помощи больным с нарушениями ритма и разработки современной операционно-диагностической аппаратуры, которая смогла бы обеспечить высокую эффективность и качество лечебного процесса.

Эндоваскулярные операции по устранению аритмии сердца получили широкое распространение в современной кардиохирургии. Основным инструментом при таких операциях являются различные виды катетеров. Методика таких операций заключается в следующем. В тело пациента вводится катетер, который помещается в больную область сердца. Посредством этого катетера происходит обнаружение больной

области сердца и лечения ее, путем деструкции аномальных проводящих путей и других источников аритмий [2].

В процессе проведения эндоваскулярных операций от хирурга требуется постоянный контроль сердечной деятельности пациента и точное управление катетером. Для облегчения работы кардиохирурга предлагается часть функций по управлению катетером возложить на ЭВМ. В последние время в России и за рубежом разрабатываются целые комплексы для проведения такого рода операций [3]. Основные функции, которые выполняют эти системы:

1. Регистрация и анализ с тела пациента различных видов сигналов (ЭГ, ЭКГ, артериальное давление и т.д.).

2. Определение местоположение рабочего органа катетера в сердце пациента (система навигации).

3. Генерирование и передача высокочастотной энергии в облучающую область катетера.

4. Визуализация процесса операции при помощи ЭВМ и т.д.

Все эти системы существенно помогают хирургу в процессе операции. В настоящее время во всем мире широко разрабатываются системы, которые позволяют дистанционно проводить операции без непосредственного вмешательства хирурга.

Целью работы является разработка системы управления катером при кардиохирургических операциях, которая позволит существенно повысить точность позиционирования катетера, обеспечит дистанционное управление катетером и будет способна использоваться катетерами разных фирм (рис. 1).

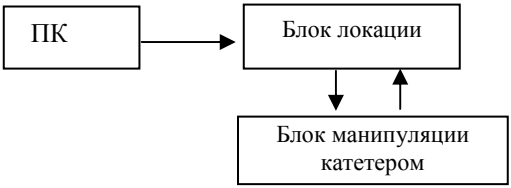


Рис. 1. Структура комплекса

Блок локации отвечает за наблюдение за ходом операции с экранов мониторов. Входящее в состав блока ПО выстраивает удобную 3D картинку сердца, с помощью которой хирург наблюдает за ходом операции и через ПК может задавать нужные действия. Блок соединен с блоком манипуляции катетера, который, собственно, и отвечает за перемещение катетера. Блок манипуляции получает команды от блока локации, и с помощью обратной связи определяется местоположение рабочей части катетера.

Возможно дистанционное управление комплексом, которое позволит проводить операции, в которых хирург будет находиться в другом городе или стране. Разработка такого комплекса позволит сделать подобные операции доступнее для большего количества пациентов.

ЛИТЕРАТУРА

1. Шумаков Е.В., Оферкин А.И., Попов Я.В., Алякин И.Н. Система автоматического управления катетером // Сборник статей по материалам четвертого конгресса молодых ученых и специалистов «Науки о человеке», Томск, 15–16 мая 2003 г. Томск, 2003.

2. Wellens H.J. Катетерная аблация для лечения аритмий сердца // N. Eng. J. Med. 2004.

3. Al-Ahmad A., Grossman J.D., Wang P.J. Ранние эксперименты по управлению катетера роботизированной системой // J. Interv. Card. Electrophysiol. 2005.

СОЗДАНИЕ SCADA-СИСТЕМЫ «РЕЗЕРВУАРНЫЙ ПАРК» ПРИ ПОМОЩИ INFINITYSCADA

А.Е. Леонов, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-403-32-71, lae@sibmail.com

InfinitySCADA – SCADA-система для сбора, обработки, хранения и визуализации технологических данных, регистрации событий и трансляции сообщений, передачи команд пользователей на исполнительные устройства, оповещения о событиях и авариях в технологическом процессе.

Для создания мнемосхемы «резервуарный парк» используется программное средство InfinityHMI.

Назначение InfinityHMI:

– разработка и исполнение графических мнемосхем;

– отображение информации о ходе выполнения технологического процесса в реальном времени;

– управление технологическим процессом;

– навигация по мнемосхемам.

InfinityHMI предоставляет расширенный набор функций по созданию и редактированию графических элементов. Для ускоренной разработки интерфейса оператора пользователь может сам создать образы технологических объектов, а также использовать библиотеку элементов. При этом библиотека позволяет сохранять используемые образы с приписанными им функциями анимации и конкретным набором

свойств, который изменяется в зависимости от реальных технологических условий и параметров. Для оптимизации действий пользователя поддерживается технология Drag&Drop, позволяющая перемещать и копировать графические и динамические объекты из одной открытой мнемосхемы в другую, а также взаимодействовать с другими приложениями. Возможна произвольная группировка объектов мнемосхем для оптимизации визуального представления технологического процесса. Технология псевдонимов динамически меняет источники данных во время исполнения. Для выполнения математических, логических, функциональных и других операций с данными используется встроенный редактор выражений. Редактор поддерживает целочисленные, вещественные, логические и строковые типы данных.

InfinityIHM позволяет упростить отладку проектов SCADA и минимизировать ошибки за счет:

1) встроенного механизма имитации сигналов;

2) предоставления информации, в режиме разработки сводных сведений, об источниках данных с разрешенными и неразрешенными псевдонимами и об используемых сигналах в мнемосхеме;

3) отображения невидимых объектов, линий нулевой толщины;

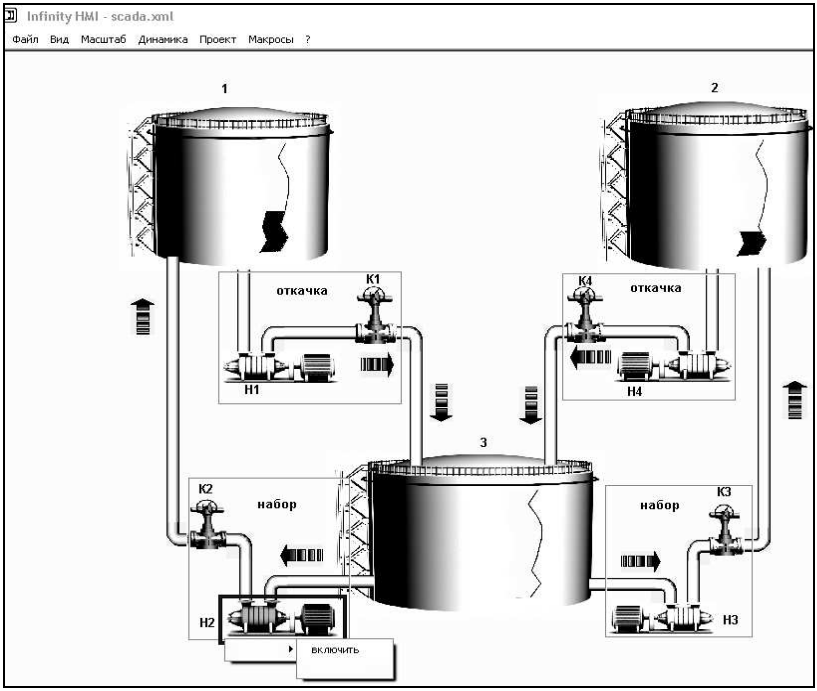
4) встроенной системы контекстно-ориентированной помощи.

Визуализация работы автоматизированной системы в SCADA-системе.

В InfinityHMI создается мнемосхема (элементы мнемосхемы находятся в библиотеке элементов) и ко всем элементам применяется требуемая цветовая динамика (цветовая политика: желтый – отключено, зеленый – включено, красный – аварийное состояние) и настройка псевдонимов (источники сигнала берутся из дерева сигналов на сервере). Для оптимизации схемы создается динамика «Всплывающее меню» для клапанов и насосов, которое будет отвечать за включение / выключение насосов и клапанов независимо от режима работы. При настройке псевдонимов трубопровода необходимо учесть несколько важных аспектов:

1) зеленый цвет при открытом клапане и при одновременной работе клапана и насоса, при включенном насосе и выключенном клапане линия на участке от насоса до клапана принимает аварийный (красный) цвет;

2) при открытом клапане и выключенном насосе из верхнего резервуара жидкость идет самотеком, поэтому нужно отобразить этот процесс, линия на участке становится зеленой, а стрелка направления потока жидкости показывает направление самотека прерывистым отображением.



Рабочая мнемосхема «Резервуарный парк»

Также следует добавить в мнемосхему динамику, которая будет отвечать за то, чтобы при включении режимов работы тумблерами блокировался режим управления клапанами и насосами из формы (т.е. блокировалось всплывающее меню). При комбинации тумблеров 0-0-1 (режим «Стоп»), управление из формы возможно.

Таким образом, получена рабочая мнемосхема «Резервуарный парк», управляемая контроллером.

ПРОЕКТНОЕ РЕШЕНИЕ АСУ ТП ПАРКА НЕФТЕПРОДУКТОВ

О.С. Лугачева, студентка 4-го курса, каф. АиКС

г. Томск, ТПУ, т. 8-905-991-71-49, olka.l88@mail.ru

Сегодня основным методом автоматизированных систем управления в таких областях, как промышленность, энергетика, являются SCADA-системы. Выбор SCADA-системы обоснован возможностью реализации поставленных задач. Использование SCADA-систем по-

зволяет сократить сроки разработки проектов по автоматизации и затраты на их разработку.

Постановка задачи. Основной задачей явилось разработать SCADA-систему АСУ ТП парка нефтепродуктов МП ЭМР «Байкитэнерго», которая должна быть ориентирована на работу в жестком реальном времени и обеспечивать реакцию системы на возникающие события, определенные для конкретного события сроки.

В системе должны быть представлены световая и звуковая сигнализация об отклонении технологических параметров, визуализация результатов контроля параметров процесса и управления технологическим режимом, автоматическое формирование управляющих сигналов и сигналов защиты, также должна быть решена задача разделения прав и доступа пользователей системы.

Решение задачи. Основой для реализации АСУ ТП является система MasterSCADA. MasterSCADA полностью совместима с любыми «фирменными» контроллерами, благодаря технологии «OPC в ядре системы» [1]. Наличие этой возможности при разработке рассматриваемой системы позволило связать выбранный контроллер компании Wago с другой системой программирования и MS через OPC-сервер.

С помощью функции резервирования каналов связи, операторских станций, архивных серверов была выполнена задача по архивированию трендов и алармов. Система имеет возможность горячего рестарта, восстановления всех элементов памяти и алгоритмов системы после сбоя.

Благодаря специализированной библиотеке для пакета программ MasterSCADA, включающей визуальные разнообразные исполнительные механизмы, в разработанной системе была решена задача визуализации результатов контроля параметров технологического процесса и управления технологическим режимом, также реализованы визуализация процесса и архивное хранение всех необходимых промежуточных данных.

Для создания мнемосхем использована встроенная библиотека готовых объектов (исполнительные механизмы, аппараты, датчики); библиотеки графических символов (рис. 1).

В разработанной системе реализована светозвуковая аварийная и предупредительная сигнализация. В непредвиденных случаях срабатывает тревожная сигнализация о недопустимом снижении или превышении уровня в резервуарах и емкостях, ответом на данное состояние системы будет автоматическое срабатывание клапанов и включение-выключение насосов. В случае аварийной сигнализации производится аварийный останов агрегатов. Также предусмотрено дистанционное управление электрозадвижками из операторной при необходи-

мости включения или отключения подачи сырья. Система выполняет следующие функции: сбор и обработка данных от датчиков, сигнализация предупредительных и аварийных отклонений параметров, отображение динамики процесса на мнемосхемах операторских станций, представление информации в виде трендов, таблиц, журналов и отчетов.

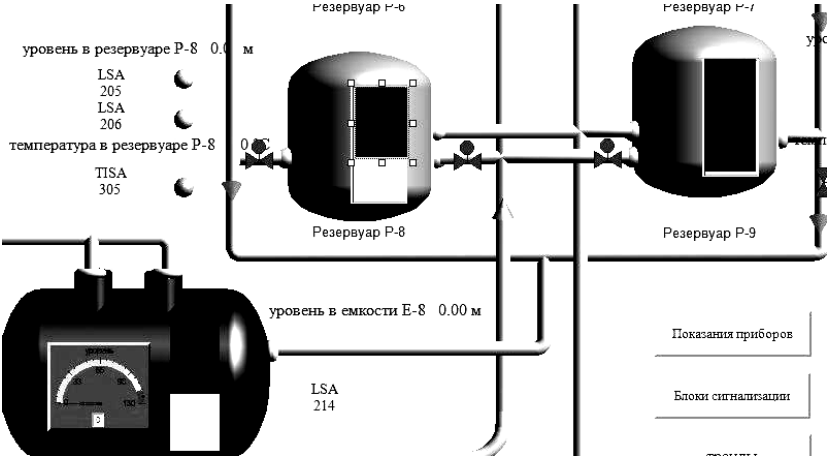


Рис. 1. Фрагмент разработанной мнемосхемы

Системой автоматизации парка нефтепродуктов предусматривается: контроль уровня в резервуарах, контроль температуры в резервуарах.

Разработанная система отвечает требованию работы в жестком реальном времени, решена задача прав доступа пользователей системы. В системе сбор информации и выдача управляющих воздействий осуществляются в реальном времени.

Сроки разработки проектируемой системы сократило многократное использование одного и того же объекта со всеми созданными для него документами, в том числе при разработке различных систем [2].

Заключение. Выбор SCADA-системы MS обусловлен функциональными возможностями, которые позволили решить поставленные задачи в разработанной системе в полном объеме.

Система автоматизации предназначена обеспечить повышение качества управления технологическим процессом за счет более точного измерения и регулирования технологических параметров, скорости управления процессом, снижения затрат на обслуживание оборудования; функциональные особенности MS позволили сократить сроки разработки SCADA-системы.

ЛИТЕРАТУРА

1. Функциональность MasterSCADA // Промышленные АСУ и контроллеры [Электронный ресурс]: Электрон. журн. – Режим доступа к журн.: http://asucontrol.ru
2. Master SCADA // Программное обеспечение [Электронный ресурс] – Электрон. дан. М.: компания ОАО «ИнСАТ». Режим доступа: http://www.insat.ru/products/?category= 9

АВТОМАТИЗИРОВАННОЕ АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ

В.В. Макаров, Р.Ю. Гороховский, студенты 3-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-913-809-32-92, lbls@sibmail.com

Рассмотрим администрируемую локальную компьютерную сеть ЛКС. В процессе администрирования выполняются задачи оптимизации системы и поддержания оптимизированного состояния процессов. Обычно средняя компьютерная сеть имеет одного специалиста, администрирующего машины, входящие в данную сеть. Такой специалист называется системным администратором – сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы парка компьютерной техники, сети и программного обеспечения в организации. На практике администрирование обычно происходит с помощью технологии удаленного доступа.

В процессе исполнения задач системного администрирования всегда возникают задачи автоматизации некоторых часто исполняемых действий, непосредственное вмешательство для решения которых составляет приблизительно половину рабочего времени системного администратора. Решение задач автоматизации системного администрирования позволяет увеличить производительность системного администратора по меньшей мере в два раза. Из таких задач в первую очередь можно выделить:

1. Мониторинг процессов, исполняемых операционной системой
2. Проверка оборудования компьютера.
3. Проверка памяти компьютера.
4. Резервное копирование.
5. Сбор данных производительности системы.
6. Управление учетными записями пользователей.

Также можно выделить ряд процедур конкретной бизнес-логики конкретного предприятия, например размещение новых данных на веб-сервере, формирование ежемесячных (ежеквартальных, ежегодных) отчетов и т.п. Простые задачи можно решить средствами, предос-

тавляемыми операционной системой администратору [1], однако не всегда этих средств достаточно [1].

Автоматизированное системное администрирование, в сравнении с администрированием «вручную», оказывается более эффективным решением даже для обслуживания одной машины [1, 2]. В существующих системах, предоставляющих расширенные возможности администрирования машин и сетей, обычно решаются узкие спектры задач. Например, системы, предоставляющие удаленный доступ, не предоставляют, как правило, каких-либо инструментов для работы с реестром удаленной ОС. И наоборот, инструменты для конфигурирования ОС не предоставляют обычно возможностей осуществления удаленного к ним доступа. Тем самым для одновременного решения задач работы с конфигурациями, реестром, мониторингом процессов, исполняемых на удаленной машине, применяются несколько независимых программных средств. Однако представляется объективным, что решение всех описанных выше задач в рамках единого программного комплекса увеличит производительность такого рода мероприятий и позволит предоставить более широкие возможности автоматизации администрирования удаленных машин при более легкой и быстрой работе.

Задачи дальнейших исследований:

1. Разработка программного комплекса автоматического администрирования работы компьютерной системы.
2. Разработка программного комплекса удаленного доступа и реконфигурирования административных параметров удаленной машины.

ЛИТЕРАТУРА

1. Станек У.Р. Microsoft Windows XP Professional: Справочник администратора. 2-е изд. М.: Русская редакция, 2003.
2. Стюарт М.-К. Безопасность сетей – готовые решения. 3-е изд.: пер. с англ. М.: Издательский дом «Вильямс», 2002.

ИССЛЕДОВАТЕЛЬСКИЙ РОБОТ

С.П. Берляков, Д.С. Бронников, Е.О. Воронина, Т.Р. Муксунов, студенты 3-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-411-60-02, katehok@sibmail.com

В настоящее время в развитых странах ведется создание мехатронных и роботехнических систем, способных вести работу в сложных условиях. Несмотря на активные изыскания в данной области, остается множество неразрешенных задач.

На данный момент существует несколько видов аналогов, которые основаны на работе сервопривода и шагового двигателя – это роботы, задача которых состоит в передвижении по поверхности, также существуют военные аналоги, но они в основном не публикуются, и достать какую-либо информацию о роботах практически невозможно.

Целью нашего проекта является создание шагающего робота, обладающего высокой проходимостью, высокоточной системой навигации и поиска пути в реальном времени. Поставленные задачи:

1. Создание управляемой динамичной платформы передвижения.
2. Создание системы навигации и управления.
3. Разработка программы, реализующей расчет передвижения.

Требования, которыми должен обладать робот:

1. Малые габариты.
2. Низкое энергопотребление.
3. Высокая проходимость.
4. Высокая устойчивость при движении.
5. Возможность работы при низких температурах.
6. Способность анализировать окружающую среду в реальном времени.

Робот будет представлен в виде симметричной системы ножек, соединенных с телом робота, имеющим вид куба. Ножка представляет собой сегментное устройство, подвижность которого осуществляется системой электроприводов (предположительно шаговых). От механизма передвижения требуется высокая точность, при этом скорость и динамика движений отходят на второй план. Такая форма робота последовала из соображений осуществления симметричной устойчивости системы. Так мы избегаем в дальнейшем написания сложных алгоритмов «вставания» робота в случае, если он перевернется. Кроме того, при передвижении робот остается минимум на 3 ножках, являясь самой устойчивой геометрической системой (аксиома о трех точках). При этом тело робота должно находиться не в центре куба, а над «устойчивым треугольником» для правильного распределения массы.

Перед нами встает задача выбора типа двигателя, мы имеем два варианта привода: сервопривод, являющийся классическим для мехатроники, и шаговый.

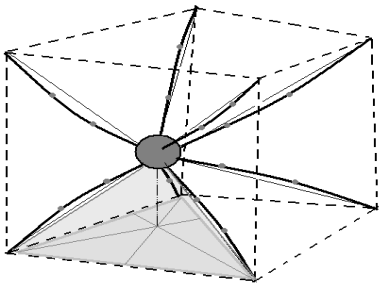


Рис. 1. Механическая модель

Сервопривод – устройство в системах автоматического регулирования или дистанционного управления, осуществляющее за счет энергии вспомогательного источника механическое перемещение регулирующего органа в соответствии с получаемыми от системы управления сигналами. То есть меняется положение регулирующего органа (рычага, кнопки, переключателя) – поток материала или энергии, поступающей на объект действия меняется и в результате идет воздействие на рабочие машины или механизмы [2]. Особенность сервопривода также в том, что его работа изменяет не только состояние рабочего объекта, но также перемещает и регулирующий орган системы. Угол поворота сервопривода определяется длительностью подаваемого на его вход импульса, а скорость – его амплитудой. Он характеризуется очень высокой точностью поворота, а следовательно, хорошим позиционированием, но для этого нужно надстраивать дополнительную систему обратной связи. Главное преимущество его – динамичность [3].

Шаговый электродвигатель – это синхронный безщеточный электродвигатель с несколькими обмотками, в котором ток, подаваемый в одну из обмоток статора, вызывает фиксацию ротора. Последовательная активация обмоток двигателя вызывает дискретные угловые перемещения (шаги) ротора. Угол поворота шагового двигателя задается количеством пришедших на его вход импульсов, а скорость – их частотой. Он хорошо позиционируется, достигает высокой степени дискретизации поворота, однако уступает сервоприводу по динамике. Шаговый привод в 1,5–2 раза дешевле его сервоаналогов. В нашем проекте мы на данном этапе остановились на шаговых приводах из-за экономических соображений и отсутствия высоких требований к динамике исполнительного узла [3].

Проанализировав данную предметную область, изучив аналоги, основные технические характеристики, мы сделали следующие выводы: наш проект является перспективным для нашего региона, поскольку отечественных аналогов подобных систем еще не существует, а потребность в них уже есть, и использование отечественных систем экономически выгоднее зарубежных [1].

ЛИТЕРАТУРА

1.http://www-robot.mes.titech.ac.jp\robot\snake_e.

2.Мехатроника: пер. с яп. Т. Исии, И. Симояма, Х. Иноуэ. М: Мир, 1988. 318 с.

3. Осипов Ю.М. Основы мехатроники. Томск: ТУСУР, 2007. 162 с.

ПРИНЦИПЫ ПРОГРАММИРОВАНИЯ НА «1С: ПРЕДПРИЯТИЕ 8»

Ю.А. Никонова, студентка 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-906-947-20-18, Ulyashka__87 @mail.ru

На сегодняшний момент существует множество программных средств, при помощи которых можно было бы решить все поставленные задачи. «1С:Предприятие» делает простым делом хранение, переработку и получение необходимой информации. Система «1С:Предприятие» включает в себя платформу и прикладные решения, разработанные на ее основе, для автоматизации деятельности организаций и частных лиц.

Платформа «1С:Предприятие» не является программным продуктом для использования конечными пользователями, которые обычно работают с одним из многих прикладных решений (конфигураций), разработанных на данной платформе. Такой подход позволяет автоматизировать различные виды деятельности, используя единую технологическую платформу.

Встроенный язык программирования «1С:Предприятие» – язык программирования, который используется в семействе программ «1С:Предприятие». Данный язык является предварительно компилируемым предметно-ориентированным языком высокого уровня. Средой исполнения языка является программная платформа «1С:Предприятие». Визуальная среда разработки («Конфигуратор») является неотъемлемой частью пакета программ «1С:Предприятие». Встроенный язык 1С:8 наиболее подобен по своему синтаксису языку Visual Basic. Платформой предоставляется фиксированный набор базовых классов, на основании которых можно создавать любое количество порожденных классов. Допускается только одна явная ступень наследования классов. Как правило, объекты порожденных классов представляют собой записи (или некоторые наборы записей) в базе данных. Такие классы образуют «Дерево метаданных». В терминах встроенного языка программирования 1С такие классы называются объектами метаданных. Основными видами объектов метаданных являются: Справочники, Документы, Отчеты, Обработки, Планы видов характеристик, Планы счетов, Планы видов расчета, Регистры сведений, Регистры накопления, Регистры расчета, Бизнес-процессы, Задачи.

Конфигуратор представляет собой специальный режим запуска системы «1С:Предприятие 8». Этот режим позволяет выполнять изменение существующих прикладных решений и создание новых, а также выполнять действия по администрированию информационной базы. Конфигуратор может быть вызван прямо из окна запуска «1С:Пред-

приятия». Конфигуратор предоставляет разработчику все необходимые инструменты для «визуального» описания структуры прикладного решения, создания форм диалогов и выходных документов, механизмов работы пользователей с данными (интерфейсов) и прав доступа различных групп пользователей к различной информации. Кроме этого, конфигуратор позволяет создать и настроить взаимодействие различных элементов прикладного решения друг с другом и написать модули на встроенном языке для обработки различных событий и реализации специфических алгоритмов взаимодействия, обработки входных и выходных данных.

ЛИТЕРАТУРА

1. http://v8.1c.ru
2. http://soft.emd.ru/1c80/
3. http://ru.wikipedia.org
4. http://www.dialogit.ru/1c/

ПРОДУКЦИОННЫЕ ЭКСПЕРТНЫЕ СИСТЕМЫ

М.А. Молчанов, О.О. Осипова, Д.А. Третьяков,
студенты 3-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-419-33-44, scintilla@mail2000.ru

Проект автоматизированной системы поиска, анализа и принятия решений необходим для предоставления информации пользователям и помощи в принятии решений в каком-либо вопросе, исходя из полученной (найденной) информации в сети Интернет.

Данная система обращается с запросом пользователя в сеть Интернет, полученную информацию анализирует, сравнивая с тематическими словарями, учитывая все поставленные отрицания и утверждения в предложении. Для принятия решений системе необходимо обратиться к экспертной системе, но они имеют узкую направленность, таким образом, для каждой предметной области необходимо применять соответствующую экспертную систему.

Рассмотрим особенности представления знаний и механизмы вывода в продукционных экспертных системах (рис. 1).

Механизм вывода часто называется *интерпретатором правил* или *планировщиком*. Правила – продукции $\alpha_i \rightarrow \beta_i$ интерпретируются с помощью конструкции:

ЕСЛИ α_i ТО β_i

Здесь α_i и β_i могут достаточно сложным образом зависеть от фактов a_i. Например, мы можем иметь продукцию вида

$$a_1 \cap a_3 \cap a_5 \cap a_9 \to a_{10},$$

где $\cap$ – знак конъюнкции (логическое «И»).

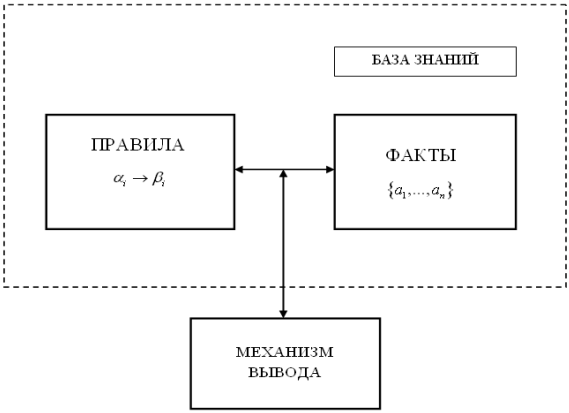


Рис. 1. Продукционная экспертная система

При решении задач оптимизации с помощью некоторой диалоговой системы оптимизации или пакета прикладных программ для выбора метода конечномерной оптимизации без ограничений может применяться ЭС, содержащая, например, следующее правило:

ЕСЛИ решаемая задача = задача конечномерной оптимизации без ограничений,

И, *количество переменных = 2,*

ТО *рекомендуемый метод = метод вращения осей Розенброка*.

Механизм вывода в продукционной ЭС может быть построен в соответствии с различными принципами. Предлагается рассмотреть основную идею.

Имеется базовое (неизменное) для данной ЭС множество возможных фактов

$$A=\{a_1,\ldots,a_n\},$$

формируемое при создании (разработке) ЭС. При этом важно понимать, что никакие новые факты не могут быть получены в результате работы ЭС. Основная и единственная задача ЭС – устанавливать определенные связи между фактами для конкретной ситуации, интересующей пользователя ЭС.

Будем различать два подмножества A_0, A_1

$$A=A_0 \cup A_1,\ A_0 \cap A_1 = \varnothing$$

исходного множества A. Множество A_1 будет называться *множеством констатированных* (*или помеченных*) *фактов*, а множество A_0 – *множеством непомеченных фактов*. Иногда множество A_1 называется *рабочим полем* ЭС. В начале работы ЭС множество A_1 содержит некоторое количество фактов (исходная информация), например:

$$A_1 = \{a_1, a_2, a_3\}.$$

Далее происходит последовательное пополнение множества A_1 за счет элементов множества A_0. Интегратор правил сопоставляет левые части продукций

$$\alpha_i \rightarrow \beta_i$$

с имеющимися во множестве A_1 фактами и выполняет то правило, левая часть которого α_i согласуется с фактами из A_1 (оказывается истиной). В результате множество A_1 пополняется за счет фактов, констатируемых в правой части продукции β_i.

Процесс модификации множества A_1 может оказаться более выгодным с использованием *обратной цепочки вывода*. Основная цель состоит в доказательстве существования ситуации (факта) a_9, и теперь будут выполняться только те правила, которые относятся к установлению этого факта.

На данном этапе в группе проекта принято решение опираться на поиск и анализ информации о каких-либо фирмах. И по средствам ЭС мы сможем спрогнозировать тот или иной факт, опираясь на полученные знания и информацию.

ЛИТЕРАТУРА

1. Черноруцкий И.Г. Методы принятий решений. СПб.: БХВ-Петербург, 2005.

СИСТЕМА АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ РАСПРЕДЕЛЕННЫМ ЛИФТОВЫМ ХОЗЯЙСТВОМ

Д.Ю. Осипов, Д.А. Сединков, студенты 5-го курса, каф. КИБЭВС,
М.И. Мельников, аспирант каф. КИБЭВС
г. Томск, ТУСУР, mmi@keva.tusur.ru

Автоматизация технологических процессов в настоящее время занимает важную роль в процессах развития человечества. Есть еще

много сторон человеческой деятельности, требующих автоматизации или нового взгляда на нее.

Разрабатываемая система призвана объединить распределенные системы в единое целое, на данный момент это лифтовое хозяйство. Предусматривается модульная структура с возможностью расширения функционала [1].

Общая схема работы системы автоматизированного управления приведена на рис. 1.

Рис. 1. Общая схема

Как видно их рис. 1, управляющая система состоит из следующих компонент: базы данных, интерфейса пользователя, OPC-сервера, интерактивного модуля оповещения и клиентской программы, установленной на кпк / смартфоне.

Общая идея функционирования системы заключается в том, что оператор автоматизированного комплекса может производить весь комплекс контрольно-диагностических и управленческих работ:

1. Опрос доступного оборудования на предмет корректности работы подконтрольных систем.
2. Прием и выдача заданий обслуживающему персоналу.

Большим плюсом является использование в системе таких элементов, как OPC-сервер и клиент [2], что позволяет использовать в качестве ядра системы различные SCADA.

На данном этапе происходит разработка модуля оповещения как серверной, так и клиентской части для мобильных устройств на базе Windows Mobile 6 [3], а также разработка структуры базы данных для системы управления в целом.

На данном этапе разрабатываются наиболее универсальные модули системы, что позволит ввести их в тестовую эксплуатацию не только в разрабатываемой системе, но и в других распределенных системах с большим количеством обслуживающего персонала, например для координации работ ремонтных бригад на нефтегазопроводах в автоматическом режиме.

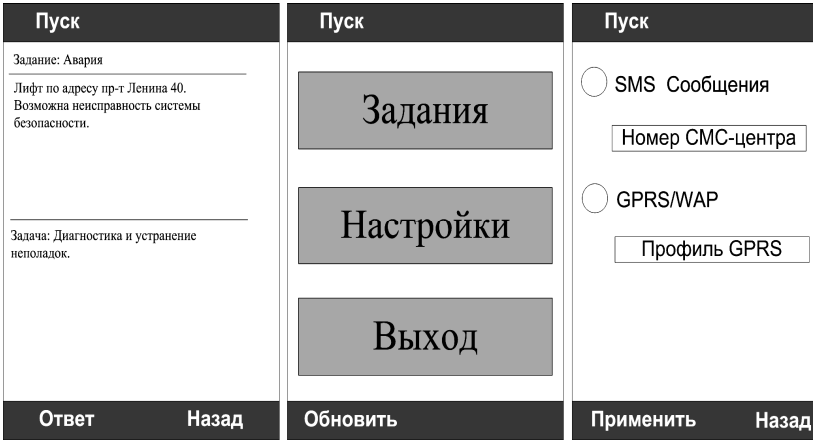


Рис. 2. Дизайн интерфейса для клиентской части модуля оповещения

В дальнейшем предполагается использование систем GPS и Глонасс для разработки и выбора кратчайших маршрутов и ближайших к месту аварии ремонтных групп.

ЛИТЕРАТУРА

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

2. OPC Foundation, OPC Specifications: http://www.opcfoundation.org/Downloads.aspx?CM=1&CN=KEY&CI=283

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

GSM/GPS МОДЕМЫ И МОДУЛИ

А.А. Прошутя, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-411-85-15, andrew42@sibmail.com

Современные промышленные системы управления и сбора данных нередко базируются на каналах сотовой связи как наиболее простых в развертывании и эксплуатации. Сотовые каналы связи все чаще используются для дистанционного контроля за состоянием различного технологического оборудования, транспорта, распределенных и удаленных технических систем. Там, где нет возможности использовать проводные коммуникации, но доступна сотовая связь, можно передавать информацию, используя встраиваемые или внешние сотовые модемы.

Для построения беспроводной линии связи необходимы только недорогой сотовый терминал и доступность сотовой связи в нужном месте.

В качестве сотового терминала предпочтительнее использовать специальные сотовые модули и модемы, так как они, в отличие от бытовых телефонов, обычно рассчитаны на более жесткие условия эксплуатации, обеспечивают большую надежность и легче интегрируются в состав промышленного и другого оборудования.

Разнообразие режимов сотовых модемов позволяет оптимизировать системы сбора данных по стоимости эксплуатации при точном соблюдении требований оперативности и полноты представления информации. Можно выделить несколько способов передачи данных от устройства контроля и/или учета на центральный пункт.

Услуга SMS (Short Message Service – услуга коротких сообщений) весьма популярна среди абонентов сотовых сетей. Основными достоинствами режима SMS являются простота использования, низкая стоимость, удобный сервис доставки. К недостаткам следует отнести в первую очередь негарантированность быстрой доставки и ограничение по длине сообщения – до 160 буквенно-цифровых знаков. Например, если опрос текущего состояния счетчика-накопителя проводится с удаленного диспетчерского пункта один раз в смену, то режим SMS подходит для такой задачи идеально. Этот режим также хорош для передачи тревожных сообщений о нештатных ситуациях.

Услуга передачи данных позволяет организовать передачу данных между двумя и более объектами, получение и отправку небольших объемов данных в реальном режиме времени (On-line). Основными достоинствами такой услуги являются более высокая надежность и скорость передачи информации. Скорость передачи данных в режиме On-line ограничена пропускной способностью голосового канала – 9 600 Кбит/с.

Для работы в сети Интернет, передачи факсимильных сообщений, электронной почты и др. приложений наилучшим образом подходит режим GPRS. GPRS – это технология пакетной передачи данных (General Packet Radio Service) в сетях GSM. Главной особенностью GPRS является то, что абонент постоянно подключен к сети, где ему предоставлен виртуальный канал, который становится реальным (физическим) радиоканалом на время передачи пакета данных. В остальное время этот физический канал используют для передачи пакетов других пользователей. Благодаря этому максимально возможная скорость доступа с помощью технологии GPRS теоретически может составлять до 170 Кбит/с.

Управление модемами осуществляется посредством AT-команд через последовательный порт (UART или RS-232). Получив от внешнего управляющего устройства (микроконтроллера или компьютера) AT-команду, модем выполняет ее и выдает обратно в последовательный порт сообщение о выполнении (если это предусмотрено в команде).

Традиционная схема подключения изображена на рис. 1.

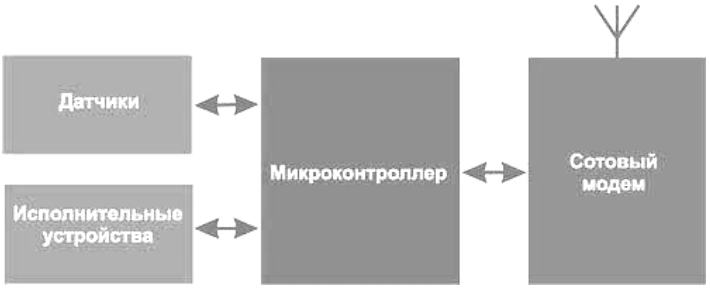


Рис. 1. Традиционная схема подключения сотовых модемов

Среди AT-команд имеются команды конфигурирования модемов, установления соединения, получения отчета о состоянии модема и сотовой сети, управления состоянием линий портов ввода-вывода и другие.

Использование AT-команд позволяет создать и отладить алгоритмы взаимосвязи устройства с терминалом GSM. Эти алгоритмы можно использовать при разработке программного обеспечения, например для микроконтроллера. Таким образом, у конструктора появляются наглядные отладочные средства, что упрощает разработку устройства в целом.

Самые простые оценки показывают, что управление модемом вполне под силу даже простым восьмибитным микроконтроллерам. Например, можно использовать популярные микроконтроллеры семейства PIC16 фирмы Microchip или AVR фирмы Atmel.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПО УЧЕТУ СТУДЕНТОВ ГПО

И.В. Салтыкова, студентка 5-го курса, каф. КИБЭВС,
Н.А. Новгородова, ассистент каф. КИБЭВС
г. Томск, ТУСУР, irkasaltikova@mail.ru

Целью данной работы является разработка автоматизированной системы по учету студентов ГПО.

Данная система должна обеспечить хранение и управление данными по студентам, их ролям в группах ГПО, успеваемости, преподавателям, группам ГПО, предложенным объявлениям, отчетам, заявлениям студентов, сведениям о работе студента в группе ГПО и аудиторной нагрузке.

Рис. 1. Модель сущность-связь

Вся информация в автоматизированной системе организована базой данных. Модель сущность-связь приведена на рис. 1. База данных находится под управлением СУБД Firebird. Программная часть автоматизированной системы разрабатывается в среде BDS.

ЛИТЕРАТУРА

1. Ковязин А.Н., Востриков С.М. Архитектура, администрирование и разработка приложений баз данных в InterBase Firebird Yaffil. М.: Кудиц-Образ, 2002. 432 с.

2. Бобровский С.И. «Delphi7. Учебный курс». СПб.: Питер, 2008. 736 с.

УСТРОЙСТВО СУТОЧНОЙ РЕГИСТРАЦИИ ЭКГ С ПЕРЕДАЧЕЙ ДАННЫХ ЧЕРЕЗ FLASH-КАРТУ

Д.А. Самойлис, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-913-811-94-79, photom@sibmail.com

Холтеровское мониторирование – это метод, с помощью которого осуществляется суточное наблюдение за работой сердца.

Для этого используется носимый портативный регистратор, который производит круглосуточную запись электрокардиограммы и передачу информации о работе сердца за сутки в компьютер.

Специальная программа обеспечивает выявление и анализ всех видов нарушения сердечного ритма, болевых и безболевых приступов ишемии миокарда. Этот метод позволяет не только точно поставить диагноз, но и существенно повысить эффективность лечения сердечно-сосудистых заболеваний (гипертония, инфаркт, атеросклероз, миокардиты).

Целью работы является создание устройства суточной регистрации, обладающего высокоскоростной передачей данных, для этого используется flash память типа SD (security digital), для проверки наложения электродов используется дисплей (рис. 1).

Устройство должно работать следующим способом. Биопотенциалы, возникающие сердце человека, за счет сокращения сердечной мышцы будут передаваться в блок усиления и фильтрации по средствам специальных проводов с липучками (отведений), расположенных в определенных местах на теле человека. Далее сигнал фильтруется и усиливается, затем поступает на вход АЦП контроллера и отображается на дисплее некоторое время для проверки крепления отведений и записывается в память.

Для передачи записанного сигнала необходимо достать карту памяти, подключить к компьютеру и с помощью специального программного обеспечения провести анализ сигнала ЭКГ (время передачи данных на компьютер не более 90 с).

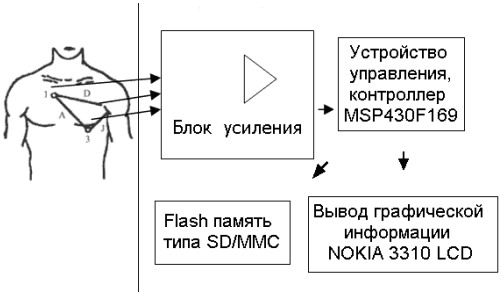


Рис. 1. Блок-схема устройства

Блок усиления служит для фильтрации и усиления сигнала, в состав блока входят операционные усилители LT6011 и микромощные инструментальные усилители AD627.

Блок управления состоит из контроллера MSP430F169.

Вывод графической информации осуществляется на черно-белый дисплей NOKIA 3310 LCD с разрешением 84×48 точек.

В качестве памяти используется карта Transcend SD, с объемом памяти 512 Мбайт.

В результате данной работы спроектировано устройство, позволяющее усиливать, оцифровывать и сохранять сигнал ЭКГ во flash память. При этом использование контроллера со сверхнизким потреблением и исключением гальванической развязки позволяет увеличить время работы устройства и его надежность. Низкая себестоимость устройства позволяет конкурировать с аналогичными разработками.

ОБЩЕЕ ОПИСАНИЕ ЧЕТЫРЕХРАЗРЯДНОГО БЛОКА ОБРАБОТКИ ДАННЫХ

А.А. Шилов, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, opk@ms.tusur.ru

В соответствии с инновационной стратегией группового проектного обучения по теме «Устройство цифрового управления объектом (ГОС СД.05 от 2000 г.)» с октября 2006 г. была начата работа группы КИБЭВС-11 по созданию регистрового арифметико-логического устройства (РАЛУ). Участниками были предложены и разработаны несколько вариантов реализации основной части РАЛУ – блока обработки данных (БОД) [1–3], на которых были отработаны основные принципы построения БОД. В ходе анализа полученных результатов были выявлены слабые стороны в виде использования широкого спектра устаревшей элементной базы, найти которую в продаже не представляется возможным и ограниченный функционал которой вынуждал использовать дополнительные схемотехнические решения для получения нужного результата. В связи с этим было принято решение о разработке улучшенной версии блока обработки данных, в критерии улучшения которого были включены такие пункты, как использование дешевой, доступной и современной элементной базы, минимизация числа и разнообразия элементов, максимальное удешевление конструкции. Кроме того, исходная концепция построения БОД на единой плате была заменена на вариант, где РАЛУ разбивается на ряд однотипных секций, комбинируя которые можно эффективно масштабировать всю систему. Результатом разработки стал четырехразрядный блок обработки данных (ЧБОД).

Четырехразрядный блок обработки данных является составной частью секционированного РАЛУ и предназначен для выполнения арифметических и логических операций над данными величиной 4 бита. Секционированное построение РАЛУ подразумевает объединение ряда однотипных блоков ЧБОД для обработки данных большей величины (8, 16, 32, … бита).

Условно ЧБОД можно разделить на три основных группы элементов, каждая из которых выполняет конкретную простую функцию, но взаимодействие которых создает сложный процесс обработки данных.

В первую группу входят элементы, необходимые для управления процессом обработки данных, в нее входят регистр кода операции PMS, регистр адреса PA с подключенным к нему дешифратором. Эти элементы совместно с системными управляющими сигналами управляют процессом исполнения операции по чтению и записи в регистры,

межрегистрового обмена, подачи данных на входы АЛУ и сохранения результата в регистре RGR.

Во вторую группу входят четыре регистра R0-R3, которые являются рабочими регистрами или регистрами общего назначения (РОН).

В третью группу входит непосредственно микросхема АЛУ с вспомогательным входным регистром (регистр временного хранения) и регистром результата (RGR).

Все входные и выходные сигналы, используемые в ЧБОД, в свою очередь разделяются на 2 большие группы. В первую входят линии шины BUS3 для связи РОН с АЛУ и внешними устройствами и линии шины BUS1 для связи АЛУ с регистрами порта ввода-вывода. Во вторую группу входят все управляющие линии связи: сигналы синхронизации элементов (y3 для чтения с РОН, y18 для записи в РОН), линии адресации РОН (A0,A1), линии кода операции PMS, флаги переноса АЛУ.

В общем случае процесс обработки в ЧБОД начинается с загрузки рабочих регистров (РОН) данными, поступающими из шины BUS3. Процесс загрузки регистра начинается с подачи адреса регистра двумя управляющими сигналами A0 и A1, которые сохраняются в регистре РА и передаются на входы дешифратора. При подаче сигнала y18 (запись) совместно с адресом с регистра адреса РА на дешифраторе активируется одна из линий D1-D8, которая подается на вход синхронизации РОН, тем самым разрешая им записать данные находящиеся в шине BUS3. Аналогично загружаются данные в остальные рабочий регистры.

Для подачи данных с рабочих регистров на входы АЛУ производится операция чтения содержимого РОН в регистр временного хранения АЛУ. Под действием управляющих сигналов A0, A1, y20, y4 и y3 (чтение) происходит загрузка шины BUS2 данными из адресуемого регистра и запись этих данных в регистр временного хранения АЛУ. Второй операнд подается непосредственно с шины BUS2 на входы АЛУ и удерживается там до окончания операции обработки данных.

В то время, когда идет загрузка второго операнда на шину BUS2, в регистре PMS сохраняется код операции, передаваемый управляющим автоматом извне, и поступает на соответствующие входы АЛУ.

Подав два операнда на входы АЛУ и управляющие сигналы кода операции, на выходе АЛУ формируется результат, который сохраняется в регистре результата RGR. Теперь результат может быть передан по шине BUS3 в любое доступное для этого место (регистры РОН, регистры порта-ввода вывода, любой приемник, подключенный к шине BUS3).

Одновременно с получением результата на регистре RGR АЛУ формирует бит переноса Cn для следующей секции РАЛУ, а также получает бит переноса P от предыдущей секции (если есть). Линии сигнала бита переноса P и Cn напрямую подключены к разъему, через который осуществляется соединение секций ЧБОД в единое РАЛУ.

В заключение необходимо отметить, что данный вариант блока обработки полностью спроектирован с использованием современного программного обеспечения, что позволило напрямую передать рабочие электронные документы предприятию изготовителю и получить полноценную печатную плату (рис. 1).

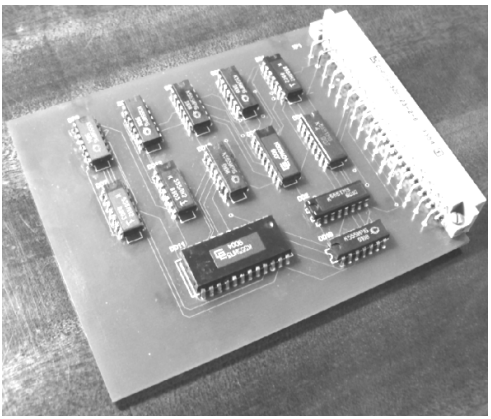


Рис. 1. Четырехразрядный блок обработки данных

ЛИТЕРАТУРА

1. Мацибаров В.Е., Часовникова Ю.Б. Блок обработки данных с мультиплексируемыми шинами // Научная сессия ТУСУР–2008. Томск, 2008.

2. Часовникова Ю.Б., Шилов А.А. Блок обработки данных с управляемой шиной «Монтажное ИЛИ» // Научная сессия ТУСУР–2008. Томск, 2008.

3. Шилов А.А., Часовникова Ю.Б. Блок обработки данных с управляемой шиной «Монтажное ИЛИ» и дополнительным регистром // Научная сессия ТУСУР–2008. Томск, 2008.

ЭНЕРГОПОТРЕБЛЕНИЕ, НАДЕЖНОСТЬ И ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ЧЕТЫРЕХРАЗРЯДНОГО БЛОКА ОБРАБОТКИ ДАННЫХ

А.А. Шилов, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, opk@ms.tusur.ru

Данная статья является дополнением к статье «Четырехразрядный блок обработки данных. Общее описание» и опирается на материалы, изложенные в ней.

Для того чтобы обосновать целесообразность разработки нового варианта четырехразрядного блока обработки данных (ЧБОД), прове-

дем сравнительный анализ энергопотребления и надежности двух вариантов реализации изделия. В качестве аналога возьмем вариант блока обработки, разработанного и описанного студентом В.Е. Мацибаровым в своей дипломной работе «Блок обработки данных с мультиплексируемой шиной» [1] и частично в статье [2].

Для проведения расчета энергопотребления, необходимо определить количество и состав элементов в схемах и привести их характеристики. Данные для нового варианта БОД приведены в табл. 1.

Таблица 1

Энергопотребление нового варианта БОД

Наименование	Кол-во	Ток потребления	Напр. питания	Потребляемая мощность, мВт
К555ЛН2	3	6,6	5	99
К555ТМ9	1	18		90
К555ИР16	6	21		630
К555ТМ8	1	18		90
К555ИД4	1	10		50
К555ИП3	1	37		185
Итого	13			1144

Для нового варианта суммарная потребляемая мощность составила ~1,2 Вт, что значительно меньше энергопотребления варианта аналога 4,8 Вт [1].

Далее проведем расчет надежности двух вариантов.

Надежность – это свойство изделия выполнять заданные функции, сохраняя свои эксплуатационные показатели в течение требуемого промежутка времени или требуемой наработки.

Для расчета надежности необходимо рассчитать такие значения, как интенсивность отказов, суммарная интенсивность отказов, наработка на отказ, вероятность безотказной работы.

В табл. 2 приведены минимальные и максимальные интенсивности отказов для нового варианта БОД.

Таблица 2

Минимальные и максимальные интенсивности отказов нового варианта БОД

Наименование	Кол-во	$\lambda_{i\max}$, 10^{-6} ч$^{-1}$	$\lambda_{i\min}$, 10^{-6} ч$^{-1}$	$N*\lambda_{i\max}$, 10^{-6} ч$^{-1}$	$N*\lambda_{i\min}$, 10^{-6} ч$^{-1}$
Разъем	1	0,062	0,062	0,062	0,062
Пайки	241	0,01	0,01	2,41	2,41
ИМС	13	0,1	0,017	1,3	0,221
Итого				3,772	2,693

Суммарная интенсивность отказов

$$\lambda_{\max} = \sum N \cdot \lambda_{i\max} = 3{,}772 \cdot 10^{-6} \ \text{ч}^{-1},$$

$$\lambda_{\min} = \sum N \cdot \lambda_{i\min} = 2{,}693 \cdot 10^{-6} \ \text{ч}^{-1}.$$

Наработка на отказ (с учетом коэффициента $a = 10$ при работе в лабораторных условиях)

$$T_{\max} = \frac{1}{\lambda_{\max} \cdot a} = 26511 \ \text{ч},$$

$$T_{\min} = \frac{1}{\lambda_{\min} \cdot a} = 37133 \ \text{ч}.$$

Вероятность безотказной работы в течение 1000 ч:

$$P_{\max}(t) = \mathrm{e}^{-\lambda_{\max} \cdot t} = 0{,}996,$$

$$P_{\min}(t) = \mathrm{e}^{-\lambda_{\min} \cdot t} = 0{,}997.$$

Таким образом, вероятность безотказной работы нового варианта БОД, равная 0,996, оказалась выше аналогичной вероятности БОД с мультиплексируемой шиной, равной 0,631 [1].

Чтобы обосновать целесообразность разработки нового варианта блока обработки данных, проведем расчет эксплуатационно-технического уровня (ЭТУ).

Оценим ЭТУ комплексным методом [3]:

$$J_{\text{ЭТУ}} = \sum_{i=1}^{n} m_i D_i,$$

где $J_{\text{ЭТУ}}$ – обобщающая количественная характеристика технического уровня изделия; D_i – единичный показатель качества i-го параметра этого изделия; m_i – весовой коэффициент, характеризующий относительную значимость i-го параметра изделия; n – количество показателей качества.

Данные расчета экспертной оценки приведены в табл. 3.

Таблица 3

Расчет ЭТУ

Показатель	Коэф. весомости m_i	Новый вариант БОД			Вариант-аналог		
		P_i	D_i	$m_i D_i$	$P_{баз}$	D_i	$m_i D_i$
Количество элементной базы	0,4	14	2,71	1,09	38	1	0,4
Энергопотребление	0,3	1,2	4	1,2	4,8	1	0,3
Надежность	0,3	0,996	1,58	0,474	0,631	1	0,3
Итого		$J_{\text{ЭТУ}} = 2{,}764$			$J_{\text{ЭТУ}} = 1$		

Так как ЭТУ нового варианта БОД значительно выше ЭТУ варианта-аналога (БОД с мультиплексируемой шиной), проведение разработки с технической и экономической точки зрения оправдано.

ЛИТЕРАТУРА

1. Мацибаров В.Е. Пояснительная записка к дипломной работе «Блок обработки данных с мультиплексируемой шиной». Томск, 2008.

2. Мацибаров В.Е., Часовникова Ю.Б. Блок обработки данных с мультиплексируемыми шинами // Научная сессия ТУСУР–2008. Томск, 2008.

3. Дерябина Е.В. Организация и планирование производства: учеб. метод. пособие. Томск: Томский межвузовский центр дистанционного образования, 2005. 192 с.

АВТОМАТИЗАЦИЯ РАБОТЫ ДЕКАНАТОВ ТУСУР С ОТЧЕТНЫМИ ДОКУМЕНТАМИ

Р.Ю. Широколобов, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, _scibern_@mail.ru

Ввиду большого объема информации, которую деканату приходится обрабатывать и вводить вручную, возникла потребность в автоматизации некоторых процессов, а именно: выдача и прием от студентов экзаменационных листов, а также ведомостей от преподавателей. Практика показала, что ввод в ЭВМ информации по ведомостям и экзаменационным листам составляет существенную часть времени работы деканата. Определенную сложность составляет и возможность восстановления истории обучения студента (переходы из группы в группу, история оценок студента) с целью замены зачетной книжки и в качестве информации для самих студентов.

Разрабатываемый продукт предназначен для использования в деканатах ТУСУР. Основной целью проектируемой системы является хранение и обработка значимых составляющих документарного обращения в деканатах ТУСУР, а также автоматизация процессов обработки, хранения и передачи данных экзаменационных листов и ведомостей, используемых в документообороте деканатов ТУСУР.

Существующая процедура выдачи и приема экзаменационных листов:

– студент приходит в деканат и просит экзаменационный лист, потому что он по какой-либо причине не сдал экзамен, зачет или курсовую работу вовремя;

– секретарь деканата выясняет причину;

– студент вручную заполняет реквизиты экзаменационного листа, а именно: название предмета, экзаменатор, ФИО студента, № зачетной книжки, факультет, курс, группа;

– секретарь вручную заполняет следующие реквизиты: срок действия, дата, подпись декана факультета;

– экзаменатор заполняет реквизиты: оценка, дата сдачи, подпись;

– экзаменатор возвращает экзаменационный лист немедленно после окончания экзамена;

– экзаменационный лист подшивается к основной ведомости группы.

Планируемая процедура выдачи и приема экзаменационных листов:

– студент в случае, если имеет доступ в Интернет, заходит на страницу выдачи экзаменационных листов и заполняет следующие реквизиты: название предмета, ФИО студента, причина получения экзаменационного листа;

– студент самостоятельно распечатывает экзаменационный лист, на котором нанесен штрих-код;

– если студент не имеет доступ в Интернет и пришел непосредственно в деканат, то он просит выдать ему экзаменационный лист у секретаря;

– секретарь заполняет те же самые реквизиты, что и студент, имеющий доступ в Интернет;

– секретарь распечатывает экзаменационный лист со штрих-кодом;

– после проставления отметки, даты сдачи и подписи, преподаватель приносит в деканат экзаменационный лист;

– секретарь сканирует штрих-код экзаменационного листа и вводит оценку.

Сформированное видение выдачи/приема экзаменационных листов, а также ведомостей позволяет спроектировать удобную систему приема/выдачи экзаменационных листов и ведомостей, существенно снизить затраты времени на обработку этих документов отчетности, уменьшить число ошибок, допускаемых сотрудниками деканата, а также хранить все необходимые сведения для восстановления полной истории обучения студента.

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ «СИСТЕМНЫЙ АНАЛИЗ» ДЛЯ РАЗВИТИЯ КОРПОРАЦИЙ В УСЛОВИЯХ КОНКУРЕНТНОЙ БОРЬБЫ

П.А. Соловей, студент 3-го курса, каф. КИБЭВС,
Н.А. Веретенникова, студентка 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, petrtusur@sibmail.com

В настоящее время можно указать большое число предметных областей и практических ситуаций, когда выбор решения может и дол-

жен основываться на привлечении хорошо подготовленных и квалифицированных системных аналитиков. Хорошо развитое программное обеспечение существенно уменьшит затраты сил и времени специалистов на обработку больших объемов информации, позволит моделировать различные практически значимые ситуации выбора в зависимости от состояния среды и условий риска.

Условно проект ГПО «Автоматизированная система поиска, анализа и принятия решений (ПУАРО)» можно разбить на следующие этапы:

1. Потребность клиента (круг решаемых задач, определение границ интересов).
2. Формирование запросов к информационной поисковой системе (с применением ассоциативного и расширенного поиска).
3. Формирование базы данных (скачивание документов из сети Internet, выявление и рубрикация фактов (морфологический анализ), взвешенная оценка тональности).
4. Системный анализ.
5. Формирование альтернатив и возможных исходов ситуаций, программная оценка принятия решений.

Взаимодействие процессов системного анализа базы данных представлено на рис. 1. Заполнив хранилище данных значительным объемов полученной информации и проведя индексирование документов посредством словарей-рубрикаторов и семантического анализа, программный модуль определяет, насколько это возможно, полный информационный портрет субъектов (объектов), выявляет источники потенциальных угроз и возможности развития корпораций. Далее определяется ценность информации на основании следующих критериев: достоверность источников, частота публикаций и значимость семантических связей.

Полученные результаты позволяют определить характер связи альтернатив с исходами, осуществить выбор критериев для оценочной функции, а также значительно сузить исходное множество альтернатив.

Следующий модуль реализуемого программного комплекса представляет собой экспертную систему, моделирующую возможные решения на основе фреймовых систем [1], используя полученную ранее карту семантических связей (представление знаний в виде объектов и отношений между ними).

В дальнейшем планируется расширить модуль принятия решений, дополнив его продукционными экспертными системами и нейлоровскими диагностическими системами для применения программного комплекса в любых областях человеческой деятельности.

Рис. 1. Структурная схема анализа базы данных

ЛИТЕРАТУРА

1. Черноруцкий И.Г. Методы принятия решений. СПб.: БВХ-Петербург, 2005. 410 с.

УПРАВЛЕНИЕ ОБЪЕКТАМИ ПО КАНАЛУ BLUETOOTH

П.Н. Сверчков, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, pavka_1@mail2000.com

Постановка задачи: обеспечить мониторинг и управление удаленными объектами посредством канала Bluetooth, в частности с мобильного телефона. Необходимо разработать стандартное решение для применения в быту, на предприятиях мелкой собственности, а также взять систему за основу для изучения программирования микроконтроллеров с управлением по каналу Bluetooth в качестве лабораторного стенда на кафедре КИБЭВС.

Результаты работы. Были подобраны реальные комплектующие из расчета низкой стоимости и средних технических показателей системы. Схема системы приведена на рис. 1.

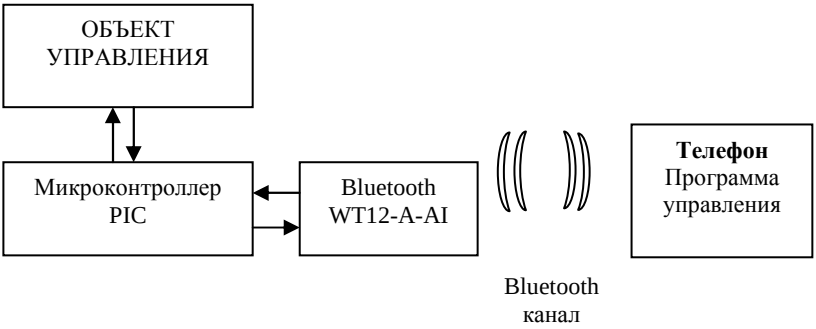


Рис. 1. Структура построения системы

В состав системы входят:

1. Микроконтроллер марки PIC фирмы Microchip семейства 16. Требование – наличие UART.
2. Bluetooth-модель для встраиваемых систем WT12-A-AI.
3. Устройство управления – мобильный телефон с поддержкой Bluetooth, желательно version 2.0. Необходима поддержка платформы J2ME.

Разработка системы состоит из 3 частей:

1. Интеграция микроконтроллера в объект управления. Это могут быть датчики, механизмы, двигатели. Написание программы для взаимодействия с объектом.
2. Соединение Bluetooth приемопередатчика с микроконтроллером через интерфейс UART и написание программы обмена данными для микроконтроллера.

3. Разработка интерфейса мидлета для мобильного телефона согласно командам объекта управления.

Особенности системы:

1. Расстояние взаимодействия телефона и Bluetooth приемопередатчика до 100 м.

2. Низкая себестоимость решения.

3. Простота реализации механизма управления посредством стандартных встроенных AT-команд.

4. Обширная область применения. Охранные системы, системы «умный дом», системы управления автомобилем, гибкие системы мониторинга на производственных предприятиях.

5. Бесплатность ПО для разработки программ, дешевое аппаратное обеспечение для программирования микроконтроллера, что сильно влияет на конечную себестоимость.

6. Низкое суммарное энергопотребление системы.

Анализ полученных результатов. Данная система была опробована для дистанционного управления игрушечной моделью автомобиля. На базе обычной радиоуправляемой игрушки был установлен микроконтроллер с Bluetooth передатчиком. Модель управлялась с мобильного телефона. На модель дополнительно была установлена беспроводная видеокамера и датчики температуры. Выигрыш данного решения перед GSM-системами в том, что процессы можно отслеживать в реальном времени, нет риска потери контроля из-за неполадок работы сервисов SMS оператора связи. Стоимость такой системы ниже аналогов по радиоканалам управления. Выигрыш в гибкости настройки за счет стандартного набора AT-команд.

Возможное развитие и применение решения: установка на модель датчиков для охраны помещения и программирование на автоматическое движение в целях мониторинга периметра; установка датчика и пускового механизма на автомобиль с целью предотвращения кражи и запуска процессов; создание автономных роботов с системой мониторинга и управления через Bluetooth; перенос клиента мобильного телефона на стационарный компьютер, что позволит более гибкое ими управлять и расширять возможности.

В качестве вывода хотелось бы выразить следующую мысль. Большим шагом в информатизации образования станет применение данной разработки в качестве стенда для лабораторных работ, например в курсе микропроцессорной техники.

ВЫБОР МОДЕЛИ РОБОТА ДЛЯ ЛАБОРАТОРНОГО ПРАКТИКУМА ПО ДИСЦИПЛИНЕ «ГАС И РОБОТОТЕХНИКА»

Е.В. Узбеков, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, jonh@sibmail.com

В качестве робота для лабораторного практикума были изучены четыре модели роботов. Робот «Robosapien RS Media (V3)» – это суперфункциональный робот с мультимедийными возможностями, пришедший на смену модели «Robosapien V2». Robosapien V2 – полностью функциональный робот с дистанционным управлением, воспринимающий голосовые команды. Управляемый с пульта робот Robosapien 8081 разработан одним из ведущих инженеров NASA Dr. Mark W. Tiden. Робот выполняет любое, даже достаточно сложное движение или комплекс движений. Lego NXT Mindstorms 8527 – это самый продвинутый конструктор на сегодняшний момент. Вы можете собирать из деталей любую конструкцию, будь то робот, скорпион, кран или что придет в голову, и управлять им через bluetooth модуль компьютера.

Проанализировав все достоинства и недостатки четырех моделей роботов, был выбран Lego-робот NXT Mindstorms 8527. У всех сравниваемых роботов имеется одинаковый набор датчиков, позволяющий им ориентироваться в пространстве, распознавать звуковые команды и цвета, выполнять простейшие команды. Роботы серии Robosapien RS Media (V3), Robosapien V2, Robosapien 8081 управляются и программируются с помощью пульта дистанционного управления, что уменьшает возможность создания более сложных программ. Lego-робот NXT Mindstorms 8527 имеет структуру конструктора, что позволяет создавать разнообразные модели роботов. Программирование осуществляется с помощью компьютера через Bluetooth. Для программирования NXT Mindstorms 8527 существует несколько языков программирования. Стандартный язык программирования «Drag and drop», что означает, перетащи и оставь, очень прост и заключается в составлении блок-схем с командами. Широкое применение получил язык NQC, очень похожий на C. NQC – Not Quite C (не совсем C) – простой язык с синтаксисом C-like, который может использоваться, чтобы программировать Lego NXT (от набора Mindstorms). Модели Mindstorms постоянно обновляются, появляются новые элементы конструктора: Web-камера, колесный и гусеничный привод, датчики температуры. Разновидность конструкций очень большая – от робота по сборке кубика-рубика до робота патрульного. Конструкции, которые можно собрать из Lego-робота NXT Mindstorms 8527, весьма разнообразны.

ЛИТЕРАТУРА

1. http://www.bombo.ru
2. http://www.ieeeboston.org
3. http://www.corestore.ru

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ДИСЦИПЛИНЕ «ГАС И РОБОТОТЕХНИКА»

Е.В. Узбеков, студент 5-го курса, каф. КИБЭВС;
Н.А. Новгородова, ассистент каф. КИБЭВС
г. Томск, ТУСУР, jonh@sibmail.com

В качестве робота для лабораторного практикума был выбран NXT MINDSTORMS 8527. Его структура конструктора позволяет создавать разнообразные модели роботов. NXT 8527 обладает набором датчиков, которые позволяют роботу ориентироваться в пространстве, распознавать цвета, реагировать на звуковые команды. Сенсор нажатия позволяет роботу осуществлять прикосновения и может определить момент нажатия на него чего-либо, а также момент освобождения. Сенсор аудио позволяет роботу слышать. Сенсор света является одним из двух сенсоров, которые заменяют роботу зрение (другой сенсор – ультразвуковой). Сенсор света позволяет роботу отличать свет от темноты. Он может считывать интенсивность света в помещении, а также измерять цветовую интенсивность окрашенных поверхностей. Ультразвуковой сенсор позволяет роботу видеть и обнаруживать объекты. Сенсор работает по тому же принципу, что и локатор летучей мыши: он измеряет расстояние путем расчета времени, которое потребовалось звуковой волне для возвращения после отражения от объекта, подобно эху. Три сервомотора дают роботу возможность двигаться. Программный блок NXT является «мозгом» робота. Это интеллектуальный, управляемый компьютером элемент конструкции робота.

Программный блок NXT программируется с помощью языка NQC. NQC язык очень похожий на C. NQC – Not Quite C (не совсем C) – простой язык с синтаксисом C-like, который используется, чтобы программировать NXT MINDSTORMS 8527. Программирование осуществляется с помощью компьютера через Bluetooth.

Лабораторный практикум состоит из нескольких работ, в которых для разных моделей робота ставятся разнообразные задачи. Модели роботов должны иметь максимальное количество датчиков. При использовании всех датчиков можно придумать технологически сложные задачи, для выполнения которых потребуется знание языка программирования и работы с ним.

Первая работа основана на изучении структуры робота, его сборки и знакомстве с датчиками. Во второй работе изучаются основы языка программирования NQC, основные процедуры, функции, переменные. Последующие лабораторные работы основаны на программировании моделей роботов для выполнения поставленных задач.

Данный курс лабораторных работ позволит на практике изучить и освоить возможности современной робототехники.

ЛИТЕРАТУРА

1. http://www.ieeeboston.org
2. http://www.corestore.ru
3. http://www.lego-go.ru
4. http://www.mindstorms.su
5. http://www.legospot.ru

МЕТОД ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ПОИСКОВЫХ СИСТЕМ ИНТЕРНЕТА

Н.А. Веретенникова, студентка 4-го курса, каф. КИБЭВС;
П.А. Соловей, М.В. Червяков, студенты 3-го курса, каф. КИБЭВС
г. Томск, ТУСУР, azazel_n@sibmail.com

В рамках проекта ГПО «Автоматизированная система поиска, анализа и принятия решений (ПУАРО)» одной из поставленных задач для нас являлось оценить эффективность функционирования информационно-поисковых систем, базируясь на результатах которой, в дальнейшем будет построена система для деловой разведки по открытым источникам.

Использованная нами концепция тестирования заключалась в вычислении двух величин – релевантности и глубины поиска для первых 10 страниц, выдаваемых информационно-поисковой системой (ИПС).

Релевантность определялась как отношение найденных релевантных документов к десяти первым рассматриваемым результатам.

Тестовые варианты содержали запросы, релевантность которых нельзя было определить без участия пользователя: по степени соответствия информации из документа и реальной информационной потребности пользователя; по степени близости предмета (тематики) информационной потребности и найденного документа; по степени полезности информационного ресурса для задачи, решаемой пользователем, с точки зрения временных затрат, способа взаимодействия пользователя с системой и т.п. [1].

Под глубиной пользовательского поиска понимается сумма двух величин $D = m + c$, где m – расстояние от первого результата до релевантного, а c – количество кликов «мышью», понадобившихся для выхода на релевантную страницу. Максимально лучший результат $D = 1$ достигается при $m = 1$ (релевантный документ находится на первом месте в ранжированном списке) и $c = 0$ (пользователь получает необходимую информацию из фрагмента текста). Под кликами понимались именно переходы со страницы на страницу с помощью кликов мыши; использование скроллера или клавиш «page up», «page down» не учитывалось. Каждая ИПС оценивалась по сумме величин D для первых десяти результатов. Если релевантные документы не были найдены в первых десяти результатах, то данная ИПС получала максимальное количество баллов – $D = (m = 10) + (c = 10) = 20$, что являлось наихудшим результатом, поскольку оценка проводилась по регрессивной шкале. Для нахождения релевантного документа делалось не более 10 кликов. Если после 10 кликов релевантный документ не был найден, системе приписывалось максимальное количество баллов. Поскольку на странице могло быть достаточно много (до нескольких десятков) ссылок на другие страницы, были сформулированы следующие правила перехода по ссылкам. Первой открывалась ссылка, в которой встречались все знаменательные слова запроса + термин, отражающий условия релевантности. Также приоритетом пользовались ссылки, в которых использовалось большее количество ключевых слов запроса. Если ключевые слова запроса не использовались в ссылках, то они открывались последовательно, до 10 кликов. Если при переходе по ссылкам открывалась страница другой поисковой системы и нужно было указывать ключевой термин для дальнейшего поиска, то это рассматривалось как отрицательный результат [2].

При составлении тестовых запросов, были учтены различные варианты возможных запросов, включающих в себя проверку обработки запросов с учетом морфологии, орфографии, семантических сетей, и ряд запросов, заданных на естественном языке. К запросам, поиск по которым был задан по ключевым словам, были добавлены логические операторы, стоп-слова, различные форматы написания дат, числовых значений и виды регистров.

Данные запросы можно разделить на запросы, предполагающие однозначную интерпретацию релевантности, и запросы, предполагающие многозначную трактовку релевантности. При определении релевантности документов, найденных по таким запросам, релевантными считались документы, содержащие любое описание указанных в запросе объектов.

В тестируемую группу были включены 17 ИПС (Google, Yandex, Nigma, Asknet, Rambler, Mail, Msn, Aport, Yahoo, Altavista, Meta, Alltheweb, Lupa, Ask, Mediumsearch, Goon, Metabot).

Проведенное тестирование показало неадаптируемость большинства иностранных систем по отношению к русскому языку, удовлетворяя только формализованную информационную потребность. Лучшие результаты тестирования показали ИПС Nigma и Yandex. Стоит отметить, что интеллектуальные возможности Yandex гораздо выше Nigma (включающие в себя приоритет источников информации, введение статистики запросов, гораздо более обширный расширенный поиск), что делает ее наиболее эффективной. На следующий уровень можно поставить ИПС: Google, AskNet, Yahoo. Возможности Google, включенные в расширенный поиск, позволяют достичь более высоких результатов, однако анализ статистики запросов большого числа пользователей к известным ИПС показал, что средняя длина запроса не превышает двух слов, и пользователи, как правило, используют самую простую форму запроса. Поэтому нельзя рассчитывать на то, что пользователь поисковой системы будет формулировать достаточно сложные эффективные запросы [3]. ИПС asknet адаптирована большей частью на естественные вопросы, не имея в своем арсенале расширенного поиска и включения в запрос операторов, также существенным недостатком является неизвестное количество найденных страниц, что делает невидимым границы при сужении поиска. В остальных системах следует отметить плохую индексацию и невозможность анализировать источники, т.к. большее количество результатов является рекламой.

ЛИТЕРАТУРА

1. Иванов В.К., Иванов К.В. Введение в информационно-поисковые системы. Ч. 1. Методические указания по изучению дисциплины «Мировые информационные ресурсы» для студентов специальностей «Прикладная информатика (в экономике)» и «Информационные системы и технологии». Тверь, 2005. 34 с.

2. Козлов М.В., Яцко В.А. Метод оценки эффективности функционирования современных информационно-поисковых систем Интернета. Абакан: Хакасский государственный университет им. Н.Ф. Катанова.

3. Сегалович И., Маслов М. Яндекс на РОМИП. Некоторые аспекты полнотекстового поиска и ранжирования в Яндекс, статья на www.romip.ru/romip2004/index.html, 2004.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ОАИСАУ

Т.С. Волгина, студентка 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-409-13-91, echidna69@gmai.com

В рамках работы была поставлена задача создать общий комплекс по лабораторным и индивидуальным заданиям по дисциплине «Основы автоматики и системы автоматического управления» [1], а также написать тестирующую программу. Коллаж из скриншотов главных форм комплекса и тестирующей программы представлен на рис. 1.

Комплекс включает в себя описание лабораторных и индивидуальных работ, а также методические указания по их выполнению. В качестве языка программирования был выбран именно html, так как документ, созданный в этой среде, может быть удобнее и функциональнее документа, созданного, например, в текстовом редакторе MS Word, а также он не требует от пользователя установки дополнительного программного обеспечения, потому что Интернет-обозреватель, позволяющий просматривать данный документ, поставляется вместе с операционной системой.

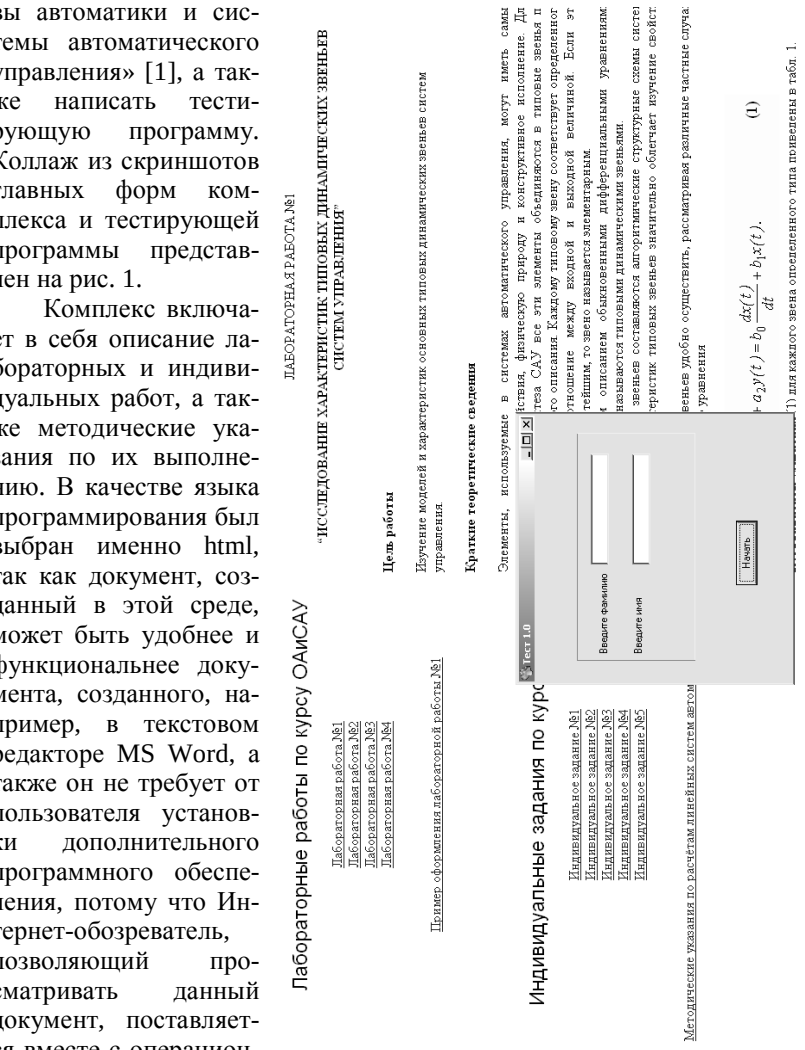


Рис. 1. Коллаж скриншотов комплекса

Для создания Web-страниц необходим текстовый редактор. Самым простым редактором, позволяющим создавать Web-страницы, является Блокнот, который встроен в операционную систему Windows. Однако работать с большим объемом информации в обычном блокноте неудобно, поэтому был сделан выбор в пользу текстового редактора Cool Editor 4.1 [2]. Он ускоряет редактирование и предварительный просмотр документов, но не избавляет от знания html-кода.

Инновационной составляющей данного проекта является то, что весь практикум по дисциплине находится в одном комплексе, что существенно облегчит работу студентам и преподавателям.

Бизнес-идея проекта – это программный комплекс, который может быть использован на кафедре.

На данном этапе работы были изучены основы программирования в html [3], вся информация по лабораторным и индивидуальным заданиям была переработана и оформлена средствами html, а также написана первоначальная версия тестирующей программы.

ЛИТЕРАТУРА

1. Бейнарович В.А. Основы автоматики и системы автоматического управления. Практикум по расчетам линейных систем автоматического управления. Томск: ТУСУР, 2004. 54 с.

2. http://www.cooleditor.nm.ru/

3. Глушаков С.В. Программирование Web-страниц. Харьков: ФОЛИО, 2005.

СИСТЕМА АРХИВИРОВАНИЯ ТЕХНОЛОГИЧЕСКОЙ ИНФОРМАЦИИ КОМПРЕССОРНЫХ СТАНЦИЙ

И.А. Юсупов, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, i_yusupov@mail.ru

Для наблюдения, регулировки, выяснения причин аварий, ремонта и других операций по обслуживанию систем промышленного комплекса необходим целый штат квалифицированных рабочих. Кроме того, неизбежны затраты на электроэнергию, дорогостоящий ремонт и замену оборудования, которых нередко можно было бы избежать, заранее имея быстрый доступ к информации о состоянии отдельных частей или системы в целом.

Возможность мониторинга в режиме реального времени, включение сирены аварийной сигнализации, создание архивов и другие функции позволяют не только снизить расходы, но и обезопасить целый комплекс от сбоя оборудования, аварий, пожаров, ошибок в действиях обслуживающего персонала и несанкционированного проникновения, позволяя переключиться на более важные проблемы.

Основой для внедрения промышленной автоматизации служат системы SCADA.

Цель работы – реализовать станцию архивирования исторических данных двух компрессоров комплекса облагораживания моторных топлив (КОМТ) с возможностью просмотра данных. Система должна обеспечивать:

1. Хранение исторических данных двух компрессоров за данный период времени.

2. Просмотр текущих и архивных данных в виде трендов.

3. Анализ технологического процесса, выявления сбоя оборудования и ошибок в действиях обслуживающего персонала.

Преимущества реализации:

1. Уменьшение времени простоя оборудования после останова, благодаря быстрому поиску неисправностей и ошибок управления по данным в архивном тренде.

2. Возможность анализа наиболее важных параметров технологического процесса одновременно (на одном экране) в виде тренда позволяет обеспечить долговременную работу оборудования без сбоев, безаварийную работу установки в целом.

В результате в основу системы архивирования была положена двухуровневая модель:

1. Уровень сбора данных и автоматического управления. Применяются контроллеры и распределенные модули сбора данных производства.

2. Уровень представления данных (диспетчеризации). Применяются АРМ под управлением Citect 5. Огромные возможности по разработке пользовательского интерфейса системы, доступ к большому списку оборудования, отображение трендов и другие дополнительные функции – вот причины использования Citect 5.

Нижний уровень: сбор и архивирование данных от контроллеров (коммуникационная функция); управление щитом диспетчера (отображение информации), фиксирование выхода их значений за уставки.

Верхний уровень (SCADA): сбор данных с объекта через контроллеры среднего уровня; поддержка работы с удаленными ПЭВМ и сетями удаленных ПЭВМ; поддержание оперативной БД, архивирование событий системы (переключение дискретных сигналов, выходы за уставки аналоговых сигналов); архивирование значений аналоговых сигналов, отображение трендов; визуализация состояния технологических параметров через тренды.

Функциональная схема станции архивирования представлена на рис. 1.

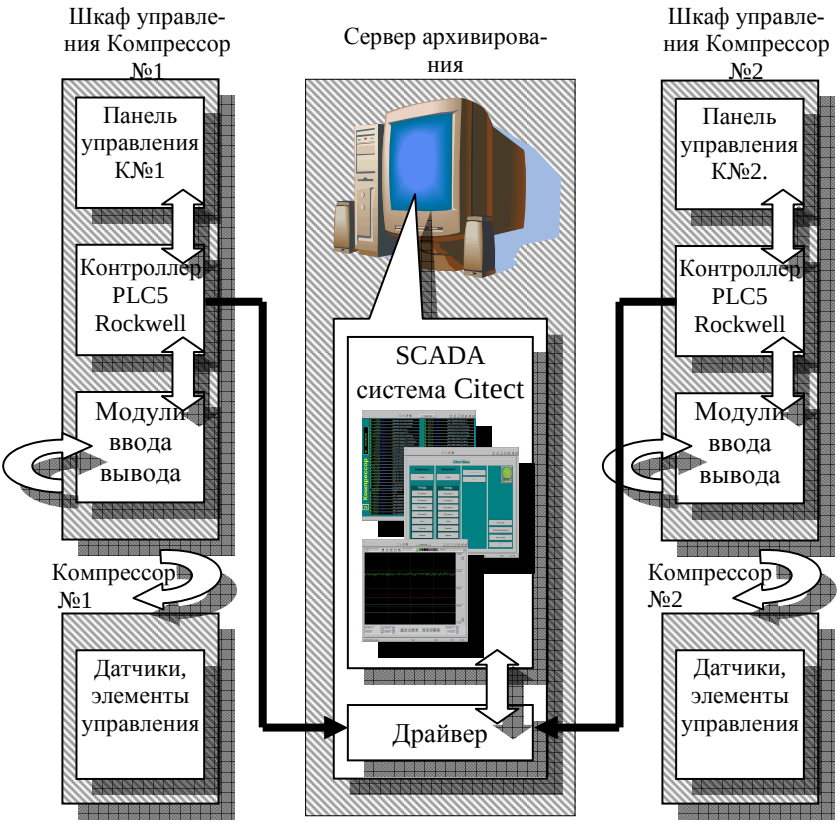


Рис. 1. Функциональная схема системы архивирования

Станция архивирования данных двух центробежных компрессоров КОМТ реализована на базе SCADA-системы Citect. Станция обладает следующими возможностями:

1. Предоставление показаний основных параметров компрессоров в online-режиме и в архиве.

2. Просмотр этих параметров в виде трендов.

3. Позволяет одновременно просматривать параметры обоих компрессоров.

4. Срок хранения данных по компрессорам составляет 1 мес.

Разумеется, внедрение SCADA-систем не является самоцелью или данью моде на всеобщую компьютеризацию. Основным и главным критерием является тот факт, что установка SCADA должна не только окупить затраты на ее внедрение, но и в кратчайшие сроки изменить

весь характер производственного процесса таким образом, чтобы повысить эффективность предприятия в целом.

ЛИТЕРАТУРА

1. http://www.autobuilding.ru/
2. http://www.uzoelectro.ru/techno/asu.htm
3. http://www.mka.ru/
4. Андреев Е.Б., Куцевич Н.А., Синенко О.В. SCADA-системы: Взгляд изнутри. М.: РТСофт, 2004.
5. http://www.asutp.ru/

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА УСПЕВАЕМОСТИ СТУДЕНТОВ

В.С. Забавский, студент 3-го курса, каф. КИБЭВС,
Н.А. Новгородова, ассистент каф. КИБЭВС
г. Томск, ТУСУР, nna@keva.tusur.ru

В настоящее время в ТУСУРе на кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ведется разработка автоматизированной системы учета успеваемости студентов. Идея разработки данной системы возникла давно, так как сейчас вся документация по учету успеваемости студентов и их истории обучения в вузе хранится в разных форматах. Эта информация разнородна и чрезвычайно объемна. В связи с большим количеством обучаемых студентов работа по ведению и синхронизации данных является трудоемкой и отнимает большое количество сил и времени, поэтому актуальность проекта очевидна.

Основой для разработки данной автоматизированной системы является учебный план. Это базовый документ, в котором описаны все дисциплины, необходимые для изучения по данной специальности на каждый семестр. Учебный план формирует вуз, руководствуясь государственным образовательным стандартом (ГОС), в котором описаны необходимые дисциплины для изучения, и добавляя свои, которые считает нужными для изучения в данном регионе.

Главными задачами данной системы являются учет успеваемости студентов на кафедре, отслеживание выполнения ими учебного плана. Также планируется вести архивацию истории обучения студента в вузе. Исходя из этого, основными программными модулями планируется соответственно сделать модуль отображения учебного плана студента по его группе, модуль отображения успеваемости студентов по номеру зачетной книжки и модуль, отображающий историю обучения студентов. В дальнейшем планируется публиковать эти сведения на сайте кафедры, чтобы студенты могли в любое время посмотреть

свою успеваемость. Функциональная модель учета успеваемости студентов выполняет следующие функции:

1) управление списками студентов;
2) управление списками учебных планов;
3) составление архива обучения студентов;
4) учет оценок;
5) получение рейтинга.

Достоинствами разрабатываемой системы являются:

– ведение архива;
– удобство занесения данных;
– наличие переводных карт.

Для реализации данного проекта используется среда FireBird 2.0. Программные модули реализуются на языке C++. Отдельно решаются вопросы по безопасности данных в системе.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ ДОБЫЧИ ВОДЫ

Д.Н. Замятин, аспирант каф. АСУ
г. Томск, ТУСУР, т. 676-724

Добыча и потребление воды возрастает с каждым днем, и проблема обеспечения качественной чистой воды и на сегодняшний момент остается актуальной. Процесс обеспечения потребителя качественной водой состоит из следующих этапов: добыча воды (1-й подъем), очистка и передача ее конечным потребителям (2-й подъем). Очевидно, что добиться производства качественной воды без применения автоматизированных систем управления технологическим процессом невозможно (рис. 1).

Автоматизированная система управления объектами водоснабжения (АСУ ТП ВЗ) предназначена для автоматизации процесса сбора и обработки информации о работе объектов сети водоснабжения, обеспечения качества воды и снижения затрат на электроэнергию, технического и эксплуатационного обслуживания, увеличения сроков работы оборудования, бесперебойной подачи воды.

Объектом управления являются артезианские скважины в количестве 10 штук. Скважины распределены по территории водозабора согласно ранее разведанной схеме залегания водных пластов. Глубина скважин в среднем составляет 150–200 м. Над каждой скважиной имеется закрытый павильон. В павильонах расположены трубопроводная обвязка скважин, а также первичные преобразователи и аппаратура управления. Температурный диапазон внутри павильона составляет

от +5 до +40°С. В скважинах на глубине 100–150 м расположены погружные насосы с электродвигателем до 45 кВт.

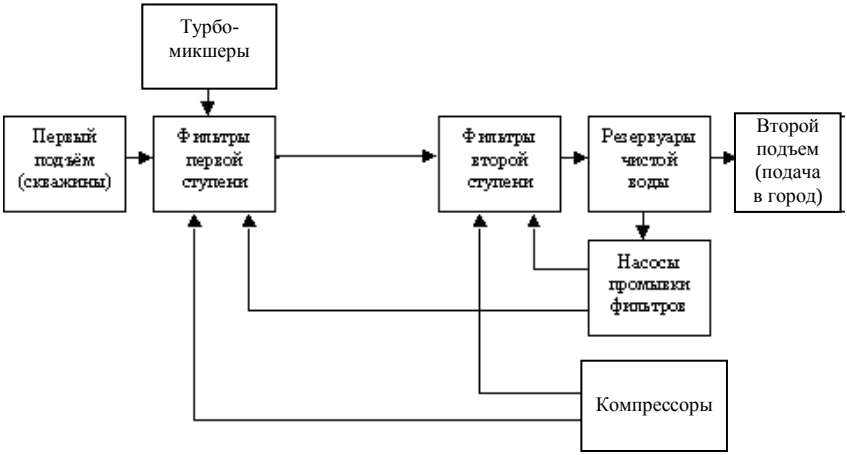


Рис. 1. Структурная схема обработки воды

Скважины работают в соответствии с технологическим планом подъема воды водозабора. Вода принудительно поднимается с помощью насосов типа ЭЦВ. Устьевое давление составляет 2,5 атм. С помощью системы трубопроводов скважины соединены между собой. Поднятая вода поступает на дальнейшую обработку.

Функции системы. Оснащение технологических объектов датчиками, исполнительными механизмами и другой аппаратурой предусматривается в объеме, позволяющем осуществить следующие функции системы по контролю и управлению технологическим процессом:

– сбор и первичная обработка технологической информации, поступающей от первичных преобразователей;

– контроль основных параметров технологического процесса;

– дистанционное управление исполнительными механизмами по заданным алгоритмам на основе собранной технологической информации и команд, поступивших от диспетчера;

– обмен информацией с уровнем управления технологическим процессом;

– отображение на дисплее диспетчера и регистрация информации о технологическом процессе в виде мнемосхем, графиков, отчетов;

– обнаружение, регистрация, сигнализация и отображение отклонений технологических параметров за установленные пределы;

– обнаружение и регистрация аварийных ситуаций.

Кроме того, осуществляется автоматическое выполнение следующих неоперативных информационных функций:

– ведение текущей документации (сводок, отчетов);

– накопление и хранение информации о ходе технологических процессов, состоянии системы;

– представление информации по запросам. Период накопления информации: сутки, месяц, год.

Структура системы. В качестве основных принципов при определении архитектуры построения АСУ ТП ВЗ приняты следующие:

– децентрализация функций сбора и обработки информации;

– модульность построения технических и программных средств;

– стандартизация взаимосвязей (функциональная, программная, конструктивная) между уровнями управления;

– функционирование большинства технологических объектов без постоянного присутствия обслуживающего персонала.

На основании перечисленных принципов разработана структурная схема, которая представляет собой 3-уровневую систему управления.

1. Низшим является уровень сопряжения с объектом, включающим в себя устройства сбора информации о конкретном узле технологического процесса, исполнительные механизмы и шкафы управления. В его состав входят:

– первичные преобразователи физических величин (технологические датчики, анализаторы, контрольно-измерительные приборы и др.);

– исполнительные устройства (пусковая аппаратура электроприводов);

– шкафы управления скважинами (ШУС);

– станции сбора и обработки информации (СОИ).

– позволяет вести поочередный ввод объектов в промышленную эксплуатацию без остановки уже действующего оборудования;

– приводит к значительной экономии, как контрольных, так и силовых кабелей.

Станции сбора и обработки информации (СОИ) обеспечивают сбор информации, поступающей со шкафов управления скважинами, и соединяются между собой по интерфейсу RS-485.

2. Средним уровнем является уровень управления технологическим процессом, который представлен промышленным компьютером Прк. В число функций системы на уровне управления технологическим процессом входят:

– сбор информации, поступающей от станций СОИ;

– контроль работоспособности модулей ввода/вывода приборов и исполнительных механизмов;

– исполнение команд с диспетчерского пункта;

– обмен информацией с диспетчерским уровнем;

– реализация алгоритмов управления работой скважин.

Работа станции производится в соответствии с заложенным в ней программным обеспечением, отрабатывающим всю логику управления и обеспечивающим взаимодействие с диспетчерским пунктом.

3. Диспетчерский уровень является верхним в иерархии. Он представлен сервером, АРМ диспетчера.

Функции сервера:

– управление обменом данных в АСУ ТП ВЗ-2;

– передача управляющей информации от терминалов;

– сбор данных и передача управляющих команд на уровень управления технологическим процессом;

– учет наработки технологического оборудования;

– подготовка регламентных отчетных документов;

– регистрация и хранение информации о контролируемых параметрах, аварийных ситуациях и действиях персонала;

– ведение архивов и предоставление информации в виде отчетных обзоров, графиков и диаграмм.

Функции станции диспетчера:

– мониторинг и дистанционное управление технологическим процессом;

– отображение в виде активных мнемосхем, осциллограмм, таблиц и других средств визуализации информации о состоянии оборудования и технологических процессов в реальном масштабе времени;

– обслуживание в диалоговом режиме запросов производственною персонала;

– опрос данных от сервера и передача команд управления на сервер.

АСУ ТП ВЗ предназначена для снижения затрат на электроэнергию, техническое и эксплуатационное обслуживание, для увеличения сроков работы оборудования, бесперебойной подачи воды.

ЛИТЕРАТУРА

1. Карамбиров С.Н. Математическое моделирование систем подачи и распределения воды в условиях многорежимности и неопределенности. М: МГУП, 2004. 197 с.

2. Труфакина А.И., Русановский А.С, Замятин Д.Н. Лабораторная информационно-менеджментская система. Сборник научных трудов научной сессии ТУСУР. 2006.

3. Исакович Р.Я. Автоматизация производственных процессов нефтяной и газовой промышленности. М., 1993. 425 с.

ВЫБОР ПЛК ДЛЯ ПРОЕКТИРУЕМОЙ АСУ ТП

П.В. Жувагин, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. +7-913-886-29-87, shtermer@sibmail.com

Автоматизированная система управления технологическим процессом (АСУ ТП) – комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на предприятиях. Термин «автоматизированный» в отличие от термина «автоматический» подчеркивает возможность участия человека в отдельных операциях как в целях сохранения человеческого контроля над процессом, так и в связи со сложностью или нецелесообразностью автоматизации отдельных операций. Составными частями АСУ ТП могут быть отдельные системы автоматического управления (САУ) и автоматизированные устройства, связанные в единый комплекс. Как правило, АСУ ТП имеет единую систему операторского управления технологическим процессом в виде одного или нескольких пультов управления, средства обработки и архивирования информации о ходе процесса, типовые элементы автоматики: датчики, контроллеры, исполнительные устройства [1]. Именно контроллеры являются основными управляющими звеньями подобных систем, выбор которых является одним из наиважнейших этапов проектирования АСУ ТП.

Несмотря на то, что программируемые логические контроллеры (ПЛК) являются типовыми элементами любых АСУ ТП, они являются основным вычислительным центром подобных систем, и их выбор оказывает существенное влияние на такие характеристики разрабатываемых систем, как стоимость, качество, время проектирования подобных систем. Но только сбором и обработкой сведений с датчиков, а также управлением системой возможности современных ПЛК не исчерпываются. В зависимости от требований к разрабатываемым системам определяются способы информационных связей всех подсистем, начиная от непосредственного кабельного соединения и заканчивая обменом информацией по различным радиоканалам. Основными характеристиками, влияющими на выбор ПЛК, являются состав разрабатываемой системы и способы информационных связей подсистем [2]. На окончательный выбор огромное влияние будет иметь стоимость ПЛК.

Практически любую разрабатываемую АСУ ТП можно реализовать на базе ПЛК, предлагаемых на рынке, за счет декомпозиции структуры системы и распределении задач между несколькими ПЛК. Исключения очень редки и связаны преимущественно с областью применения разрабатываемой АСУ ТП.

Современный рынок автоматики предлагает почти безграничный выбор ПЛК, как специализированных под конкретные задачи, так и

имеющих общее назначение. Все современные ПЛК можно разделить на несколько подвидов [3]:

1) классические ПЛК (OMRON, Siemens Simatic S7, Segnetics, Direct Logic, Овен ПЛК, Mitsubishi FX, Modicon TSX Quantum, Beckhof);

2) ПЛК на базе процессора i8088/8086/80186/ (ICPDAS, Advantech);

3) интеллектуальные реле (Siemens LOGO!, Mitsubishi Alpha, Zelio Logic, Omron ZEN, Moeller EASY);

4) программные ПЛК на базе PC-совместимых компьютеров;

5) распределенные системы управления DCS.

Рассмотрим классические ПЛК. К основным техническим характеристикам этих контроллеров можно отнести следующие (на примере контроллеров ОВЕН ПЛК 100/150 [4]):

1) ресурсы (центральный микропроцессор, объем оперативной памяти, объем энергонезависимой памяти и пр.);

2) дискретные входы (количество, максимальная рабочая частота и пр.);

3) аналоговые входы (количество, типы поддерживаемых датчиков и входных сигналов и пр.);

4) дискретные выходы (количество и пр.);

5) аналоговые выходы (количество, тип выходного сигнала и пр.);

6) интерфейсы связи (интерфейсы, протоколы и пр.);

7) программирование (среда программирования, языки программирования и пр.).

Большинство предлагаемых на рынке контроллеров имеют возможность использования для программирования одного из языков, соответствующих стандарту «IEC 61131-3: Programming controllers» [5].

Согласно определению, ПЛК – микропроцессорное устройство, предназначенное для управления технологическими процессами в промышленности и другими сложными технологическими объектами (например, системы управления микроклиматом), именно микропроцессоры являются сердцем любого ПЛК [3]. Следовательно, именно используемым в ПЛК микропроцессором (МП) определяются все его основные возможности и технические характеристики, начиная от типов и количества дискретных и аналоговых входов/выходов и заканчивая интерфейсами связи [6].

Лишь только в случае отсутствия на рынке необходимых решений или невозможности создания АСУ ТП с помощью имеющихся средств следует прибегать к разработке ПЛК, и то только в том случае, если это экономически оправдано. С одной стороны, включение в процесс проектирования АСУ ТП задач разработки ПЛК (соответствие стандарту IEC 61131-3 не является обязательным) очень сильно снижает

показатели экономической эффективности всей системы в целом из-за увеличения временных затрат на разработку ПЛК, с другой – позволяет создать ПЛК, наиболее оптимальный для данной системы.

Современный рынок средств автоматики предлагает огромный выбор как отдельных ПЛК, так и целых комплексов. Основными факторами, влияющими на выбор ПЛК, являются структура и требования к разрабатываемой АСУ ТП, в состав которой будет входить это устройство, а определяющим – стоимость предлагаемых решений.

Только в редких случаях следует прибегать к разработке ПЛК, входящего в состав разрабатываемой системы, и то лишь в том случае, если это экономически оправдано.

ЛИТЕРАТУРА

1. АСУ ТП – Википедия. http://ru.wikipedia.org/wiki/АСУ_ТП.

2. Хоске М.Т. ПЛК становятся миниатюрными, производительными, интеллектуальными – http://www.controlengrussia.com/focus2.php4?num=278#top.

3. Программируемый логический контроллер – Википедия – http://ru.wikipedia.org/wiki/Программируемый_логический_контроллер.

4. Контролер ОВЕН ПЛК 100/150. Программируемый логический контроллер. КИП-Сервис. Технические характеристики контроллеров ОВЕН ПЛК 100/150 – http://www.kipservis.ru/oven_plk.htm.

5. IEC61131-3 – Википедия – http://ru.wikipedia.org/wiki/IEC61131-3.

6. Балашов Е.П., Пузанков Д.В. Микропроцессоры и микропроцессорные системы: учеб. пособие для вузов / Под ред. В.Б. Смолова. М.: Радио и связь, 1981. 328 с.

ОПЕРАТИВНОЕ ПЛАНИРОВАНИЕ МЕЛКОСЕРИЙНОГО ПРОИЗВОДСТВА

П.А. Шадрин, студент 6-го курса, каф. ЭС

г. Томск, ТУСУР, p_hawk@sibmail.com

На производственных предприятиях важной задачей является составление календарного плана выполнения работ по заданной технологии [1, 2]. Рассмотрим проблему планирования мелкосерийного производства на примере мебельного производства.

Производство описывается номенклатурой изделий и комплектующих. Например, для изделия «стол № 2» в таблице представлены: в первом столбце – название конечного продукта производства (стол № 2), во втором столбце – названия промежуточных изделий (сборочных единиц), необходимых для изготовления конечного продукта, в третьем столбце – названия материалов, требуемых для изготовления промежуточных изделий.

Изделие «стол №2»

Конечные продукты (1)		Промежуточные изделия (2)		Требуемые материалы для промежуточных изделий (3)
Стол № 2	1	Столешница № 2	1	ДСП. 8 мм № 2
	2	Боковая стенка стола № 2	2	Пластик ленточный 2 м ш 8 мм
	3	Поперечная стенка № 2	3	Пластик листовой 0,3 см 0,5*0,5 м
	4	Подставка стола № 2	4	Пластик листовой 0,1 мм 3*3 м
	5	Штырь крепления	5	Саморез. д 10 мм
	6	Гайка крепления поворотная	6	Прут. мет.
			7	Прут. мет. д 10
			8	Клей

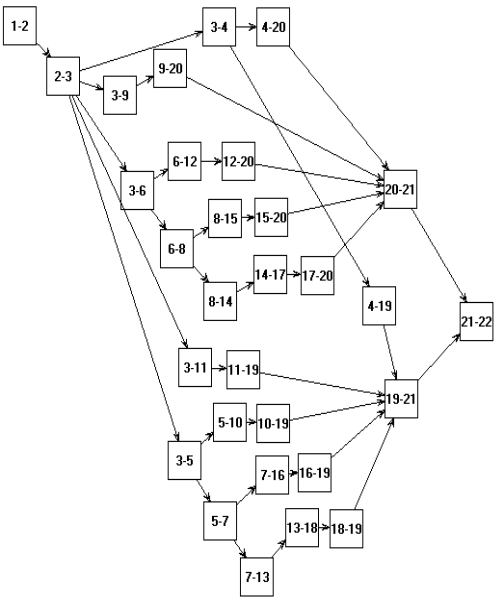
Аналогичным образом можно составить таблицы требуемых материалов и промежуточных изделий для других конечных продуктов производства (стол № 1, тумбочка, лоток, шкаф).

Для производства изделий, входящих в некоторый заказ поставки потребителю, необходимо выполнить ряд работ в определенной последовательности. При планировании производства составляется перечень работ для выполнения заказа.

Пусть, например, получен заказ на изготовление двух столов 2-го типа (стол № 2). Для их изготовления необходимо выполнить следующие работы (в скобах указаны их длительности): начало (0); отпилить ДСП (5); оклеить ДСП пластиком (8); обтянуть ДСП пластиком (7); вырезать подставку стола (4); выточить штырь крепления (13); выточить гайку крепления (11); сборка стола (15); прием заказа (1).

При выполнении работ должен соблюдаться порядок, при котором последующая работа не может быть начата до выполнения предшествующей ей работы. Порядок выполнения работ задается сетевым графиком. Для рассматриваемого здесь примера сетевой график выполнения работ имеет вид, представленный на рис. 1.

Справа приведены шифры работ, представленных на сетевом графике (выделены полужирным шрифтом). Шифр строится следующим образом: первое число шифра (*i*) каждой работы является вторым числом шифра предшествующей работы, а второе число шифра (*j*) есть первое число шифра последующей работы.



1-2 – Начало
3-6 – отпилить ДСП
6-8 – отпилить ДСП
8-14 – отпилить ДСП
6-12 – обклеить ДСП пластиком
8-15 – обклеить ДСП пластиком
14-17 – обклеить ДСП пластиком
12-20 – обтянуть ДСП пластиком
15-20 – обтянуть ДСП пластиком
17-20 – обтянуть ДСП пластиком
3-4 – вырезать подставку стола
3-9 – выточить штырь крепления
9-20 – выточить гайки крепления
20-21 – сборка стола
3-5 – отпилить ДСП
5-7 – отпилить ДСП
7-13 – отпилить ДСП
4-20 – вырезать подставку стола
5-10 – обклеить ДСП пластиком
7-16 – обклеить ДСП пластиком
13-18 – обклеить ДСП пластиком
3-11 – выточить штырь крепления
10-19 – обтянуть ДСП пластиком
16-19 – обтянуть ДСП пластиком
18-19 – обтянуть ДСП пластиком
11-19 – выточить гайки крепления
19-21 – сборка стола
2-3 – Прием заказа. Распределение работ
21-22 – конец
4-19 – Фиктивная

Рис. 1. Сетевой график выполнения работ

Для построения временной диаграммы выполнения работ (диаграммы Гантта) необходимо рассчитать моменты начала и окончания всех работ. В теории календарного планирования, кроме длительностей работ t, различают T_{rn} – ранний срок начала работы, T_{ro} – ранний срок окончания работы, T_{pn} – поздний срок начала работы, T_{po} – ранний срок окончания работы, R_p – полный резерв времени, R_c – свободный резерв времени. Вычисление ранних и поздних сроков начала и окончания работ производится по известным формулам [3].

Ранний срок начала работы – это самый ранний из возможных сроков начала работы с учетом сроков выполнения предшествующих работ. Ранний срок начала работы определяется продолжительностью самого длинного пути от начального события до начала данной работы по формуле

$$T_{rn}(i,j)=T_r(i)\,, \qquad (1)$$

где $T_r(i)$ – максимальная продолжительность всех работ от начального события до начала данной работы.

Ранний срок окончания работы – это срок окончания работы при условии ее начала в самый ранний из возможных сроков. Ранний срок окончания работы определяется путем суммирования раннего начала и продолжительности данной работы по формуле

$$T_{ro}(i,j)=T_r(i)+t(i,j)\,. \qquad (2)$$

Поздний срок начала работы – это самый поздний срок, при котором может быть начата работа без нарушения продолжительности критического пути, т.е. общего срока выполнения. Поздний срок начала определяется разностью критического пути и продолжительности данной работы по формуле

$$T_{pn}(i,j)=T_p(j)+t(i,j)\,, \qquad (3)$$

где $T_p(j)$ – критический путь.

Позднее окончание работы – это предельно допустимый срок, в который может быть окончена данная работа без увеличения продолжительности критического пути

$$T_{po}(i,j)=T_p(j)\,. \qquad (4)$$

Полный резерв времени – это время, на которое можно перенести начало работы или увеличить ее продолжительность, не нарушая общего срока выполнения

$$R_p(i,j)=T_p(j)-T_r(i)-t(i,j)\,. \qquad (5)$$

Свободный резерв времени – это время, на которое можно перенести начало работы или увеличить ее продолжительность без изменения раннего начала последующих работ

$$R_c(i,j)=T_p(j)-T_r(i)-t(i,j)\,. \qquad (6)$$

Результаты этого расчета представляются в виде диаграммы Гантта, позволяющей определить критический путь выполнения работ, на котором отсутствуют резервы времени. На рис. 2 представлена диаграмма Гантта (календарный план работ) для рассматриваемого здесь примера мебельного производства.

На диаграмме видны два критических пути. Они соответствуют параллельно выполняемым работам (изготовление двух одинаковых столов) одинаковой трудоемкости. Работы, не лежащие на критическом пути, расположены на диаграмме Гантта случайным образом в пределах допустимых интервалов.

График работ может быть перестроен таким образом, чтобы время исполнения всего заказа было минимальным. Например, вместо параллельного выполнения работ в случае ограниченных производственных

ресурсов можно использовать различные схемы диспетчеризации работ по мере освобождения необходимого для выполнения оборудования.

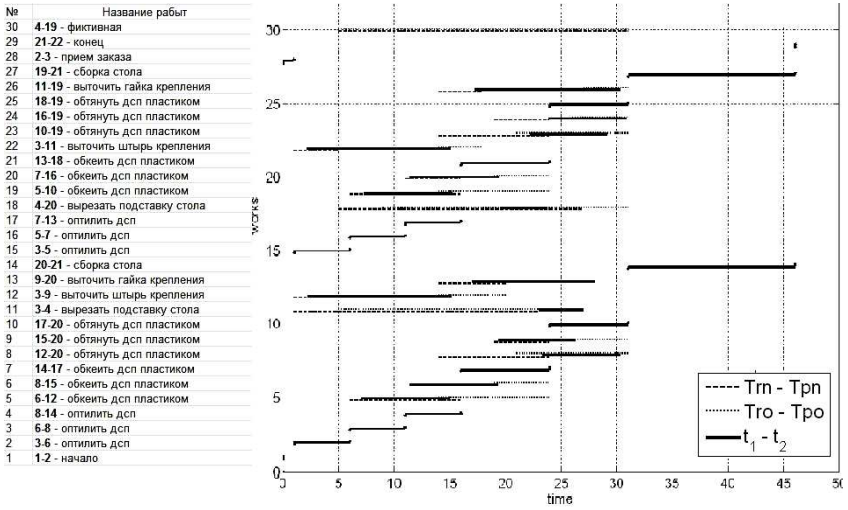


Рис. 2. Диаграмма Гантта

Алгоритмы построения сетевого графика с правильным упорядочением работ (и присвоением шифров), вычисления допустимых интервалов работ и построения диаграммы Гантта были реализованы программно в среде Delphi.

ЛИТЕРАТУРА

1. Организация, планирование и управление строительным производством / Под ред. И.Г. Галкина. М.: Высшая школа, 1978.

2. Оперативно-календарное планирование. Режим доступа: http://www.mtmlogistika.com/termslib/production_scheduling.htm

3. Майника Э. Алгоритмы оптимизации на сетях и графах. М.: Мир, 1978.

СЕКЦИЯ 14

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель – **Шелупанов А.А.**, зав. каф. КИБЭВС, д.т.н., профессор;*
зам. председателя – Мещеряков Р.В., к.т.н., доц. каф. КИБЭВС

ОПРЕДЕЛЕНИЕ КОЛИЧЕСТВЕННЫХ ХАРАКТЕРИСТИК КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Р.Ф. Акчурин, Е.Н. Анищенко, В.А. Трошин, студенты 3-го курса, каф. КИБЭВС, А.П. Зайцев, науч. рук., к.т.н., проф.
г. Томск, ТУСУР, т. 8-923-413-24-85, nurka12@rambler.ru

Существует множество различных каналов утечки информации. Радиопередающие устройства реализуют один из способов несанкционированного доступа к источникам конфиденциальной информации – подслушивание с передачей зафиксированных разговоров или звуковых сигналов техники.

Специалист в области защиты информации должен уметь обнаружить различные типы радиопередающих устройств, излучающих опасные сигналы, а также локализовать микрофон или устройство, передающее данный сигнал. С этой целью была создана учебная модель, состоящая из имитатора сигнала и устройства обнаружения.

В качестве радиопередающего устройства используется обучающий тренажерный комплекс «АВРОРА-Т», для обнаружения опасного сигнала используется компьютерный комплекс «RS-Turbo».

Обучающий тренажерный комплекс по подготовке специалистов в области поиска и обнаружения радиозакладных устройств «АВРОРА-Т» способен имитировать работу следующих радиопередающих устройств:

– с программной перестройкой несущей частоты радиосигнала (ППРЧ);

– с непосредственным расширением спектра исходного сигнала модуляцией несущей частоты псевдослучайной последовательностью (ШПС);

– с накоплением информации с последующей ее передачей в эфир (СКП);

– постоянно действующих радиосигналов с амплитудной (АМ), фазовой (ФМ) и частотной (ЧМ) модуляциями и их комбинации.

Диапазон рабочих частот комплекса «АВРОРА-Т» от 50 до 3000 МГц, максимальная полоса формируемого сигнала 50 МГц. Комплекс может работать в двух режимах: стационарный (управление передатчиком производится с помощью ПЭВМ) и автономный (работа передатчика ведется под управлением модели сигнала, предварительно записанной в одну из пяти программ его внутренней памяти). Модулирующий сигнал может быть внешним цифровым, внутренним цифровым, с внешнего микрофона или внутреннего микрофона [1].

Компьютерный комплекс RSturbo предназначен для быстрого обнаружения, идентификации, определения местоположения (локализации) и нейтрализации подслушивающих устройств и других источников несанкционированных излучений.

Комплекс RS turbo позволяет сканировать радиодиапазон вплоть до 12 ГГц, что полностью покрывает диапазон рабочих частот комплекса «АВРОРА-Т». Одновременно комплекс с достаточной точностью указывает местоположение обнаруженных радиомикрофонов с обычной частотной модуляцией, а при необходимости нейтрализует их излучения.

С помощью средств анализа программы оператор может детально исследовать характеристики интересующего сигнала, например, его радиоспектр, гармонический состав или реакцию на импульсы акустического зондирования и т.д., получая всю необходимую информацию для принятия обоснованного решения о наличии в помещении подслушивающих устройств [2].

Была разработана модель для имитации радиопередающих устройств с их последующим обнаружением для дальнейшего использования в учебном процессе. Модель была опробована на практике. С помощью комплекса «АВРОРА-Т» были смоделированы некоторые виды и формы сигналов, а с помощью компьютерного комплекса «RS-Turbo» обнаружено, что реальные форма и параметры сигнала совпадают с теоретическими расчетными спектрограммами.

Рассмотрим работу модели на примере шумоподобного сигнала с несущей частотой 1050 МГц. Расчетная спектрограмма созданной модели представлена на рис. 1.

После сканирования диапазона частот от 700 до 1300 МГц с помощью программно-аппаратного комплекса «RS-Turbo», была определена радиообстановка в помещении на заданных частотах без излучения сигнала комплексом «АВРОРА-Т» (рис. 2).

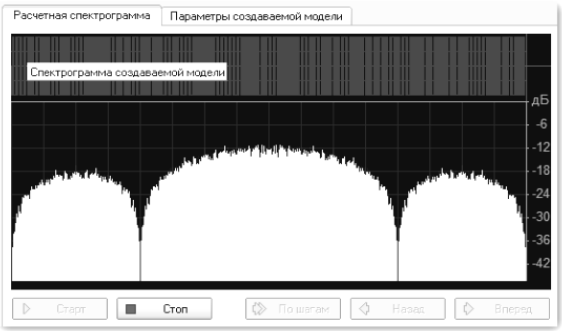


Рис. 2. Спектрограмма шумоподобного сигнала смоделированного с помощью комплекса «АВРОРА-Т»

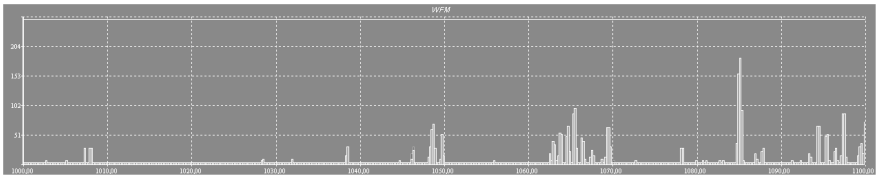


Рис. 2. Картина частотного диапазона до включения комплекса «АВРОРА-Т»

После начала излучения сигнала картина частотного диапазона меняется (рис. 3).

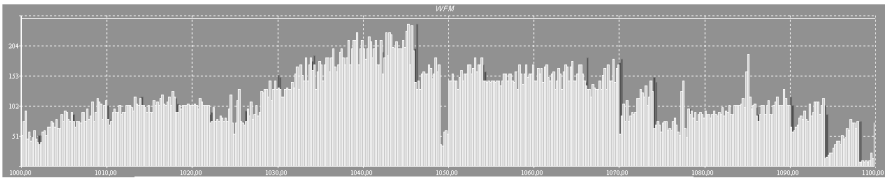


Рис. 3. Картина частотного диапазона после включения комплекса «АВРОРА-Т»

На рис. 1–3 видно, что практическая и расчетная спектрограммы в диапазоне от 1000 до 1100 МГц похожи по форме и обнаруженный сигнал имеет несущую частоту примерно равную 1050 МГц, что соответствует несущей частоте излучаемого сигнала.

Таким образом, показана возможность совместного использования программно-аппаратных комплексов «АВРОРА-Т» и «RS-Turbo», что служит основанием их изучения и дальнейшего использования в написании лабораторных работ.

ЛИТЕРАТУРА

1. ЗАО НПЦ Фирма «НЕЛК» Обучающий тренажерный комплекс по подготовке специалистов в области поиска и обнаружения радиозакладных устройств «АВРОРА-Т»: Инструкция по эксплуатации. М., 2006. С. 104.

2. Компания «Радиосервис» Компьютерные комплексы «RS-Turbo»: Инструкция по эксплуатации. М., 2003. С. 34.

РЕШЕНИЕ ПРОБЛЕМ АВТОРСТВА ТЕКСТОВ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА РАСТУЩЕГО НЕЙРОННОГО ГАЗА

Е.Н. Анищенко, Д.В. Кручинин, студенты 3-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-412-77-62, ayn_89@mail.ru

В настоящее время вопрос об авторстве очень актуален в свете появления документов сомнительного авторства и их воровства. Изменение имени автора или изменение содержания может привести к серьезным последствиям, а значит, необходимы механизмы защиты авторских прав и эффективные алгоритмы определения авторства.

В результате анализа материалов по определению авторства текста была поставлена задача программной реализации такой системы и анализа эффективности разработанного алгоритма. Система может применяться в авторoведческой экспертизе. Объектом авторoведческой экспертизы является текст. Задачи экспертизы разделяются на две группы: идентификационные и диагностические. Под идентификационными задачами предполагают проверку авторства, подтверждение авторства определенного лица, исключение авторства определенного лица, проверку того, что автором всего текста был один и тот же человек, а также проверку того, что исполнитель текста является одновременно его автором. Система предназначена для решения именно этих задач. Диагностические задачи, такие как определение личностных характеристик автора или определение факта сознательного искажения письменной речи, в работе не затрагиваются. Идентификационные задачи авторoведческой экспертизы решаются в тех случаях, когда требуется подтвердить или опровергнуть авторство определенного лица (лиц) по отношению к тому или иному тексту, причем предполагаемый автор текста известен и непосредственно доступен.

Как известно, существуют различные алгоритмы кластеризации, целью которых является уменьшение объемов неопределенной информации для упрощения дальнейшей обработки данных и принятия решений. Итак, основные концепции кластеризации. Кластеризация – это процесс объединения n-мерных векторов в группы, где члены

групп имеют схожие черты. Каждая группа представлена *n*-мерным вектором, называемым центральным. Векторное квантование – это процесс квантования *n*-мерных входных векторов на ограниченное количество *n*-мерных выходных векторов, называемых кодовыми векторами. Набор возможных кодовых векторов называется кодовой книгой, которая обычно генерируется кластеризацией заданного набора тестовых векторов.

В работе в качестве входного распределения используются *n*-мерные векторы, состоящие из частоты появления униграмм, биграмм или триграмм. Было решено, что будут использоваться 32-мерное пространство для униграмм, 100-мерное пространство для биграмм и триграмм, 500-мерное пространство для триграмм, 1024-мерное пространство для биграмм. На выходе с некоторой долей вероятности определяется принадлежность текста некоторому автору. В качестве алгоритма определения принадлежности текста автору был выбран алгоритм «растущего нейронного газа» («Growing Neural Gas»(GNG)).

Работа модели представлена на рис. 1.

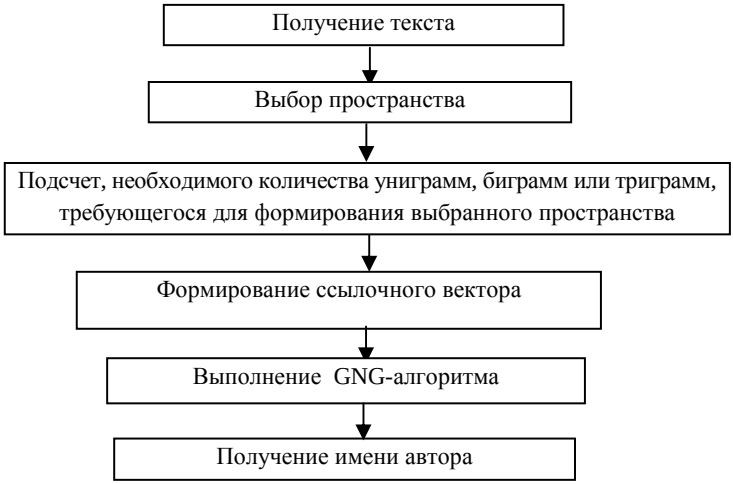


Рис. 1. Алгоритм работы программы

GNG-алгоритм – это неконтролируемый растущий кластерный алгоритм. Получая входное распределение, определенное в пространстве R^n, GNG создает растущий граф или сеть узлов, где каждый узел имеет свои координаты в пространстве R^n. В GNG кодовые векторы представлены как ссылочные векторы или позиции GNG-узлов. Также он

может быть использован для поиска топологических структур, что напрямую отражается на структуре входного распределения. GNG – это адаптирующийся алгоритм, т.к. входное распределение медленно меняется во времени, также узлы могут двигаться так, чтобы покрыть новое распределение.

Начиная с двух узлов, алгоритм строит граф, в котором узлы считаются соседними, если они имеют общую ветвь. Для каждого входного сигнала X два ближайших в эвклидовом пространстве узла соединяются ветвью (Competitive Hebbian Learning (CHL)). CHL – это существенная часть алгоритма GNG, т.к. он используется для определения места добавления нового узла.

Только GNG использует параметры, постоянные во времени. Также не требуется каждый раз решать, какое количество узлов использовать, т.к. узлы постоянно добавляются. Добавление новых узлов прекращается, когда оператор решает, что достигнут необходимый критерий или максимальный размер сети.

GNG-алгоритм предполагает, что каждый узел k включает:

1) w_k – ссылочный вектор, определенный в пространстве R^n;

2) error_k – местную переменную накопленную ошибку;

3) набор ветвей, определяющих топологических соседей узла k.

Ссылочный вектор может быть определен как позиция узла в пространстве. Местная переменная накопленная ошибка – это статистическое измерение для определения соответствующих точек вставки новых узлов. Также каждая ветвь имеет переменный возраст, который используется для определения момента удаления старых ветвей с целью обновления топологии [1].

Каждый кластер в сети определяется конкретным автором, а добавление узла или текста в кластер означает принадлежность текста данному автору. В результате будут сделаны выводы о том, какой из способов анализа текста наиболее эффективен: подсчет частоты униграмм, биграмм или триграмм; сколько мерных векторов целесообразно использовать. Также будут сделаны выводы о величинах параметров, используемых в GNG-алгоритме, таких как количество итераций λ, необходимых для добавления нового узла, величины α и β, определяющие изменение местной переменной ошибки, доли e_w и e_n, которые определяют перемещение узлов во время итераций, максимальный возраст $a_{\max}$ жизни ветви, которые бы обеспечили довольно точное определение автора текста при оптимальных затратах времени.

ЛИТЕРАТУРА

1. Jim Holmström, Growing Neural Gas: Experiments with GNG, GNG with Utility and Supervised GNG: www.booru.net/MasterThesisProj.pdf/download

МОДЕЛЬ АТАКИ И ЗАЩИТЫ НА АС

В.С. Аверченко, А.И. Михайловский, студенты 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-411-02-54, _demon_@sibmail.com

В двадцать первом веке движущей силой и главным объектом всех отраслей человеческой деятельности становится информация, и состояние каналов, сетей и безопасность серверов станут основой экономического развития. По мнению некоторых экспертов, информация становится главной международной валютой. К сожалению, сложные сетевые технологии достаточно уязвимы для целенаправленных атак. Причем такие атаки могут производиться удаленно, в том числе и из-за пределов национальных границ. Все это ставит новые проблемы перед разработчиками и строителями информационной инфраструктуры.

Разнообразие угроз, подстерегающих пользователя, работающего в сети, огромно. Часть из них является платой за использование сложных информационных технологий, уязвимых к внешним воздействиям, другая часть сопряжена с деятельностью людей. Некоторые угрозы носят объективный характер, например: нестабильность или низкое качество питающего напряжения, электромагнитные наводки или близкие грозовые разряды; другие могут быть связаны с невежеством или неаккуратностью самого пользователя (последнее обычно опаснее).

В последние десять лет число идентифицированных уязвимостей увеличивалось в среднем более чем на 50% ежегодно [1].

Если несколько лет назад атаки на сетевые объекты совершали в основном (около 90%) хулиганы, которые таким образом пытались самоутвердиться, сейчас вторжения на серверы и рабочие станции предпринимаются уже с корыстной целью.

Традиционная модель атаки строится по принципу «один к одному» (рис. 1) или «один ко многим» (рис. 2), т.е. атака исходит из одного источника. Разработчики сетевых средств защиты (межсетевых экранов, систем обнаружения атак и т.д.) ориентированы именно на традиционную модель атаки. В различных точках защищаемой сети устанавливаются агенты (сенсоры) системы защиты, которые передают информацию на центральную консоль управления. Это облегчает масштабирование системы, обеспечивает простоту удаленного управления и т.д. Однако такая модель не справляется с относительно недавно (в 1998 г.) обнаруженной угрозой – распределенными атаками [2].

В модели распределенной атаки используются иные принципы. В отличие от традиционной модели в распределенной модели используются отношения «многие к одному» (рис. 3) и «многие ко многим» (рис. 4).

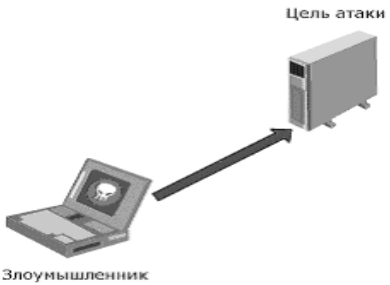


Рис. 1. Отношение «один к одному»

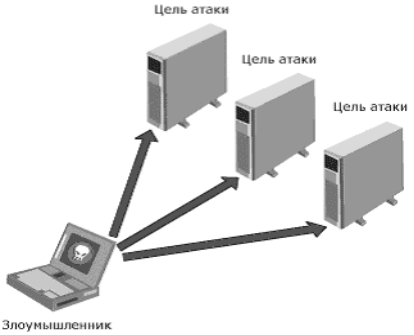


Рис. 2. Отношение «один ко многим»

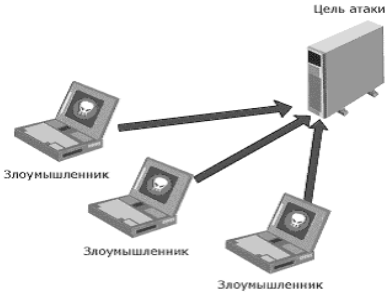


Рис. 3. Отношение «многие к одному»

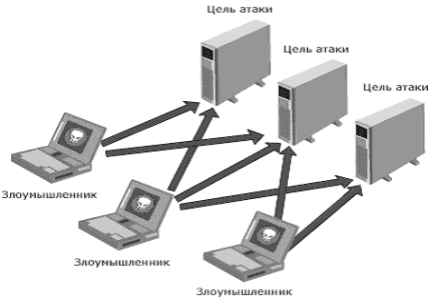


Рис. 4. Отношение «многие ко многим»

Основой проекта является классификация этих атак и детально показать, что воздействует на атаку в процессе ее совершения, а также построение моделей защиты, ориентируясь на модели атаки, с описанием конкретных действий и программ которые необходимо выполнить, чтобы закрыть уязвимость для атаки.

В работе рассмотрены различные методы взлома АС, которых просто огромное множество, и защитникам АС приходится очень нелегко в сложившейся ситуации. Новые атаки появляются каждый день, и в связи с этим происходит улучшение зажиты, то есть закрывание уязвимостей, которые обнаружились. Злоумышленник может получить всю ему нужную информацию, даже не прибегая к атаке АС, а просто используя метод социальной инженерии узнать информацию для повышения своих привилегий и полномочий в АС. Таким образом, построение модели злоумышленника и изучение атак на АС и соответственно построение защиты на эти АС является очень актуальной.

За безопасностью АС надо следить всегда и постоянно обновлять ее и проверять, так как появляются новые уязвимости и, следовательно, строятся новые методы защиты от них.

ЛИТЕРАТУРА
1. http://book.itep.ru/6/intrusion.htm#36
2. http://www.nestor.minsk.by/sr/2001/08/10812.html

СИСТЕМА ВИЗУАЛЬНОГО МОДЕЛИРОВАНИЯ ЗАЩИТЫ ПОМЕЩЕНИЙ

А.С. Данченко, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, ghost_300@sibmail.com

Защита информации основывается на комплексе разнообразных элементов, и одним из ключевых является организация защиты помещений. В процессе обеспечения должного уровня защиты помещения приходится анализировать и вычислять массу параметров, подбирать необходимое оборудование и знать, насколько эффективно оно себя покажет в данном конкретном случае.

Зачастую все шаги от выбора и проверки оборудования, расчета угла обзора камер, зоны покрытия датчиков и т.д. не автоматизированы, не наглядны и производятся вручную. Цель создаваемой системы заключается в наглядном представлении защищаемого помещения и всего установленного для защиты оборудования, а также анализ уровня защищенности и возможных источников угроз.

Разрабатываемая система визуального моделирования защиты помещений должна обеспечивать следующий функционал:

– загрузка растровых изображений (технический план помещения) в среду программы;

– создание из библиотеки примитивов отдельных элементов помещения, как то: стены, пол, потолок, окна, двери, межкомнатные перекрытия, с выбором параметров объектов, например: толщина стен, перекрытий, материал, из которого они изготовлены, и т.д.;

– добавление в созданное помещение линий коммуникации, электропитания и т.д., с выбором типа и заданием начальных характеристик;

– установка в виртуальном помещении объектов защиты и наблюдения – камер видеонаблюдения, датчиков движения, с выбором типа из библиотеки объектов программы;

– расчет зоны наблюдения помещения, расчет зоны покрытия камер и датчиков;

– анализ на основе исходных данных созданного помещения уровня его защищенности, с указанием возможных источников угроз и каналов несанкционированного доступа;

– формирование на основе проведенного анализа выходного отчета.

Программа разрабатывается в среде программирования Delphi с использованием графических библиотек OpenGL.

В аналитический модуль программы заложена математическая модель расчета различных параметров системы, как то: выход акустического сигнала за пределы помещения, сила порождаемого виброакустического сигнала и расчет массива оборудования, которое может его засечь, возможен ли визуальный съем информации из помещения и т.д.

В результате была создана программа, реализующая заданные функции, с расширяемыми модулями объектов, с возможностью внесения новых типов оборудования, элементов помещения и т.п.

ОБУЧАЮЩАЯ СИСТЕМА НА ОСНОВЕ ПОНЯТИЙНОЙ СТРУКТУРЫ

Н.С. Давыдов, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-962-785-95-97, nikitass@sibmail.com

Основная цель работы состоит в создании системы автоматизации процесса разработки учебно-методического материала, базирующейся на построении понятийной структуры дисциплины и формализации этой структуры, что позволит эффективнее решать задачи обучения и передачи накопленных знаний как живым, так и искусственно созданным системам.

На момент рождения ребенок не знает ни слов, ни правил, ни языка. Всю информацию он воспринимает в общем виде через ощущения. Эти ощущения представляют собой образы, которые ребенок запомнил. Самые первые образы образуют фундамент, на котором ребенок строит свое представление о мире. В дальнейшем каждый обобщенный образ приобретет конкретное представление, которое выльется в слова, словарный запас пополняется, складываясь уже в конкретное представление о мире, образуя предложения, те в свою очередь будут складываться в базовые знания, которые в свою очередь будут расширяться и уточняться. В результате получается структура, в основе которой лежат образы-понятия и которые расшифровываются в конкретное представление о мире. Так происходит обучение сложной системы, и без понимания базовых принципов обучения живой системы невозможно понимание каких-то конкретных понятий, поскольку невозможно объяснить только что родившемуся ребенку отличие, например, между «правдой» и «ложью», ведь для этого ему необходимо хотя бы понимание того, что есть «хорошо», а что «плохо».

По мере накопления знаний систематизация становится все более затруднительной. Часто, в ходе обучения, человеку приходится сталкиваться с каким-либо понятием, значение которого ему не известно. И в лучшем случае приходится делать выбор (в худшем случае выбора нет), изучить это понятие или продолжить обучение без его понимания, понадеявшись на образность своего мышления, то есть обучаться дальше, не вникая в детали, а только воспринимая саму «суть». Конечно, человек сможет разобраться в вопросе только поверхностно, если вообще сможет (понятие может оказаться фундаментальным). Если же знания в данной области жизненно необходимы, то придется вернуться и пройти все обучение заново. Этого может не произойти, если объяснение неизвестного понятия будет изначально заложено в обучающую систему, позволяющую «планировать» последовательность их изучения.

Таким образом, при автоматизации процесса обучения (применении ЭВМ в учебном процессе) возникает необходимость в разработке структурированной системы, которая повысит эффективность обучения за счет содержания систематизированной и формализованной структуры понятий, сведенной в базу знаний.

Прежде чем приступать к созданию базы знаний, необходимо сначала разработать инструмент для ее создания и дальнейшей работы с нею. Такой инструмент составляет основу разрабатываемой системы. Система состоит из двух приложений.

Первое представляет собой обычную систему обучения, содержащую лекционный материал, проверку знаний и некую систему защиты от несанкционированного доступа к ней (рис. 1), и некоторую распределяющую подсистему, которая предоставляет доступ к материалам в зависимости от уровня знаний студентов. После изучения материала студент проходит проверку, для того чтобы в дальнейшем получить доступ к следующему материалу, основанному на уже изученном. Результаты проверки записываются в журнал.

Второе приложение представляет собой конструктор лекций, вопросов для проверки знаний и понятийной структуры лекций. На основе понятийной структуры системой будет проверяться лекционный материал на предмет наличия в нем нарушения логической последовательности изучения материала. В дальнейшем планируется тесная интеграция конструктора лекций и понятийной структуры дисциплины: понятийная структура представляет собой «костяк», к каждому понятию которого привязан лекционный материал, и в зависимости от изменения положения понятий изменяется и структура лекций.

Особенностью реализации конструктора понятийной структуры является многомерность понятий (рис. 2). В обычной понятийной структуре любое понятие можно раскрыть через другие понятия, ле-

жащие в «плоскости» данной понятийной структуры. Но при этом каждое понятие можно связать с другой аналогичной понятийной структурой, которая будет раскрывать это понятие на другом уровне или в другой плоскости, для которой будут действовать те же правила. Таким образом, для одного понятия можно создать бесчисленное количество его описаний, отображающих всю его многомерность.

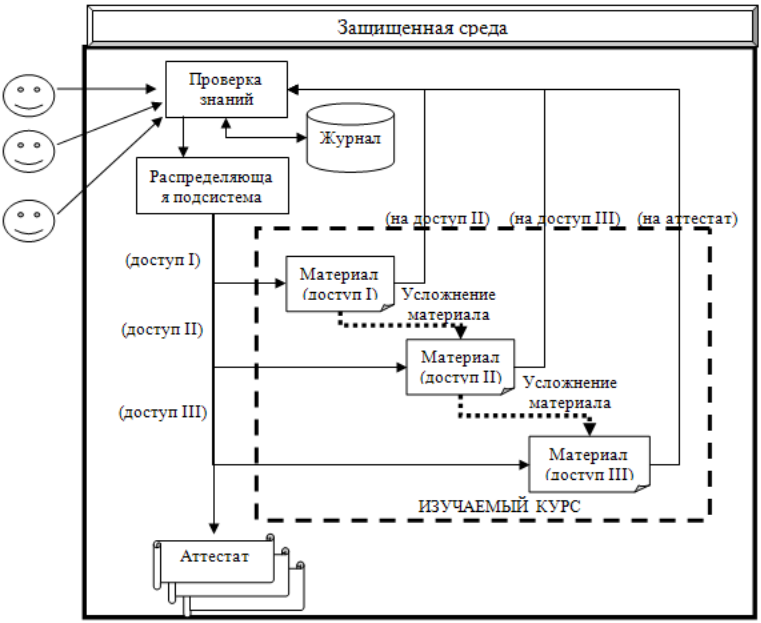
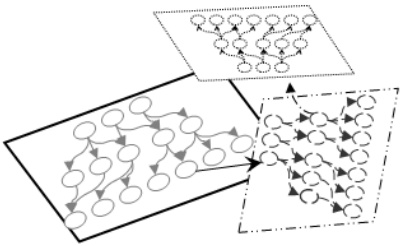


Рис. 1. Структура приложения пользователя



В среднем количество понятийных структур будет nm, где n – среднее количество элементов в понятийной структуре, m – среднее количество «плоскостей».

Рис. 2. Многомерность понятий

Система будет внедрена в учебный процесс для дисциплины «Дискретная математика». Предполагается дальнейшее развитие системы, которое лежит в создании системы искусственного интеллекта и применении разработанной системы для ее обучения на основе по-

строенной понятийной структуры. Представленная модель структуры достаточно гибка и универсальна, может быть использована для решения разных видов задач и имеет высокую степень расширяемости.

ЛИТЕРАТУРА

1. Лурия А.Р. Речь и интеллект в развитии ребенка. М., 1927.
2. Крылов В.Ю. Методологические и теоретические проблемы математической психологии. М., 2000.
3. Клацки Р. Память человека. Структуры и процессы. М., 1978.

АУТЕНТИФИКАЦИЯ В ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЕ ОБМЕНА СООБЩЕНИЯМИ

М.А. Девяткин, студент 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, max5252@sibmail.ru

В этой статье дан обзор системе аутентификации, которая была спроектирована в рамках группового проектного обучения по теме «Децентрализованная система обмена сообщениями в сети Интернет».

Аутентификация – процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует [1]. Самые известные и распространенные на сегодняшний момент способы аутентификации в централизованных системах не подходят для их реализации в данном проекте по нескольким причинам. Во-первых, отсутствует центральное звено, которое хранит базу с аутентификационной информацией (именами и паролями). Во-вторых, если такую базу будет иметь каждый участник сети, то возникнет сложность с синхронизацией аутентификационных данных. К тому же в этом случае любой участник обмена сообщениями в сети будет иметь доступ к базе, в которой хранятся имена и пароли других пользователей. Даже если хранить не сами пароли, а их хэши, то любой пользователь с помощью специальных программ сможет восстановить пароль, используя его хэш [1]. Таким образом, в ходе работы над проектом возникла необходимость в разработке способа аутентификации, который позволит осуществлять надежный обмен сообщениями в децентрализованной системе.

При проектировании системы было решено использовать двухключевой (асимметричный) криптографический алгоритм RSA (Rivest, Shamir, Aldeman). Безопасность данного алгоритма основана на трудоемкости факторизации больших чисел [2].

При каждом входе в систему пользователь должен указывать свое имя и пароль. Если вход в систему осуществляется впервые, то для

пользователя генерируется пара ключей: открытый ключ и закрытый ключ. При этом закрытый ключ должен держаться в секрете, а по открытому ключу невозможно подобрать закрытый ключ. В данной системе в алгоритме RSA используется ключ размером 512 бит. При первом входе в систему на компьютере пользователя создается файл, в который записывается созданная пара ключей. Сам файл шифруется на основе симметричного блочного шифра 3DES. При этом в качестве ключа для шифрования используется хэш от пароля, который был введен пользователем при входе в систему.

Когда пользователь входит в систему, он указывает свое имя (ник) и пароль. Если пароль оказывается верным, то файл с хранящимися в нем ключами расшифровывается на время сеанса. Иначе пользователю отказывается в доступе.

При подключении к какому-либо компьютеру сети происходит отсылка имени и открытого ключа. Если пользователь с таким именем и открытым ключом имеется в базе, хранящейся на компьютере, к которому осуществляется подключение, то подключаемому пользователю со стороны подключающего пользователя отсылается шифрованное системное сообщение, с целью выяснить является ли пользователь действительно тем, за кого он себя выдает. После этого на машине пользователя, который желает осуществить подключение, полученное системное сообщение должно быть расшифровано с помощью закрытого ключа пользователя. Далее результат расшифровки отправляется на сторону подключающего пользователя. Если сообщение было расшифровано верно, то производится подключение нового узла к сети. При этом новый пользователь отображается в качестве друга (с меткой friend), т.е. является именно тем, за кого он себя выдает. После этого новый пользователь устанавливает связь со всеми остальными участниками сети аналогичным образом.

Если пользователь с таким именем и открытым ключом не имеется в базе, хранящейся на компьютере, к которому осуществляется подключение, то этот пользователь не получает никаких системных сообщений, он получает метку unknown (неизвестный), его имя хранится в памяти только на время сеанса и не заносится в базу. При этом нет уверенности в том, что этот человек является именно тем, за кого он себя выдает. Далее новый пользователь устанавливает связь со всеми остальными участниками сети аналогичным образом.

Если пользователь не является другом (т.е. имеет метку unknown), то при добавлении в друзья с этим пользователем осуществляется обмен системными сообщениями. В случае если пользователь успешно прошел проверку, то информация об этом пользователе (имя и открытый ключ) из памяти заносится в файл, в котором хранятся сведения

о других друзьях. Однако в списках у других участников сети, у которых этот пользователь отображался с пометкой unknown (неизвестный), он будет также отображаться как неизвестный.

Таким образом, пользователи сети делятся на два типа: друзья, которые успешно прошли процедуру аутентификации, и неизвестные пользователи, которые могут не являться теми, за кого они себя выдают.

Использование данной системы аутентификации позволяет без особых трудностей синхронизировать базы, имеющиеся у разных пользователей. При этом у каждого участника обмена сообщениями имеется свой список друзей. В базах хранятся открытые ключи, по которым невозможно подобрать закрытый ключ. Поэтому открытый ключ можно сообщать кому угодно и даже публиковать. К тому же в данной системе используется алгоритм RSA, стойкость которого основана на сложности разложения модуля на два больших простых множителя. До настоящего времени не найдены практически реализуемые общие способы решения этой задачи при длине модуля 512 бит и более [2].

ЛИТЕРАТУРА

1. Мещеряков Р.В., Праскурин Г.А. Теоретические основы компьютерной безопасности. Томск: В-Спектр, 2007. 344 с.

2. Мещеряков Р.В., Шелупанов А.А. Комплексное обеспечение информационной безопасности автоматизированных систем. Томск: В-Спектр, 2007. 350 с.

ЗАЩИТА ЛОКАЛЬНОЙ СЕТИ ОТ ВНЕШНИХ УГРОЗ

В.А. Довбыш, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, dvaenkin@sibmail.com

В настоящее время количество локальных сетей с каждым годом увеличивается, так как растет количество организаций, в которых они просто необходимы. Как правило, в них хранится и обрабатывается коммерческая тайна или конфиденциальная информация. Поэтому остро встает вопрос их защиты от внешних угроз, т.е. конкурентов или просто злоумышленников. Целью данной работы является разработка методики защиты локальной сети от внешних угроз.

В защиту локальной сети от внешних угроз входят организационные, правовые, программно-аппаратные, криптографические, а также инженерно-технические средства. Для того чтобы выбрать, какие именно средства и как будут использоваться, необходимо создать концептуальный план защиты сети. А для того чтобы его создать, необходимо провести:

1. Анализ бизнес-требований.

2. Оценку влияния общих бизнес-факторов на проект защиты.

3. Снижение затрат на защиту.

4. Разработку правовых требований к информационной безопасности.

5. Оценку влияния проекта защиты на конечных пользователей.

6. Разработку мер по снижению риска в проектах защиты.

7. Снижение влияния несовместимости систем на их защиту.

8. Анализ угроз из-за проблем с сопровождением системы безопасности.

9. Анализ существующих политик и мер безопасности.

10. Классификацию информации в целях защиты (почему необходимо защищать информацию, принципы классификации информации).

11. Анализ уязвимости данных на разных этапах их обработки.

12. Анализ рисков для администрирования ИТ-инфраструктуры.

После того как все это будет выполнено, можно приступать к следующему шагу: разработке концептуального плана защиты. В разработку концептуального плана защиты входят:

1. Моделирование угроз.
2. Планирование действий при нарушении безопасности.
3. Изоляция сегментов сети.
4. Планирование процедуры восстановления.

Также необходимо провести анализ технических ограничений (определение технических ограничений, анализ ограничений по совместимости).

После того как все вышеперечисленные процедуры будут выполнены, можно приступать к практической реализации разработанных методов защиты локальной сети от внешних угроз.

Так как количество локальных сетей в обозримом будущем будет расти, актуальность данная проблема не потеряет.

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО КАНАЛА ПЕРЕДАЧИ ИНФОРМАЦИИ МЕЖДУ WEB-СЛУЖБАМИ. PHP-РЕАЛИЗАЦИЯ

В.Н. Елисеев, аспирант каф. КИБЭВС

г. Томск, ТУСУР, vne@security.tomsk.ru

В современном мире информатизация общества, развитие сетевых технологий и сети Internet подталкивают мировое бизнес-сообщество к переходу на уровень экономического взаимодействия, отвечающий высочайшим стандартам научно-технического прогресса.

Как в публичных, так и корпоративных системах все большее распространение находят WEB-службы, которые повышают эффективность работы компаний на B2B-рынке за счет снижения затрат на подготовку торговых процедур и расширения географии бизнеса до масштаба всего мира. Как правило, такие системы требуют идентификации и аутентификации клиента, а также криптозащиту передаваемых данных.

Но у конечного пользователя, может и не быть возможности организовать обмен данных по SSL-каналу. А в некоторых случаях выбор в пользу SSL будет являться далеко не лучшим решением. В этом случае защиту WEB-служб можно построить в соответствии со спецификацией WS-Security.

Спецификация WS-Security разработана совместно фирмами Microsoft Corp., IBM Corp. и VeriSign Inc. и направлена на то, чтобы помочь организациям разрабатывать защищенные, совместимые приложения для Web-служб.

К сожалению, при разработке группы спецификаций Web-служб консорциум W3C ориентировался прежде всего на их публичное использование, и по этой причине вопросы безопасности Web-служб изначально не рассматривались как приоритетные.

Традиционный подход к защите передаваемых данных в Web предполагает организацию защищенного SSL-канала, и доступ к Web-службе организуется по протоколу HTTPS. Специфика этого протокола требует наличия на сервере специального SSL-сертификата, который фактически привязан к одному конкретному IP-адресу. Такое решение не всегда удобно. Например, если необходимо реализовать несколько различных защищенных каналов на одном Web-ресурсе. Также SSL имеет еще ряд недостатков: только транспортный уровень взаимодействия, шифрование полностью всего трафика, увеличение трафика в 2,5 раза, увеличение времени отклика, также не решены некоторые вопросы ЭЦП.

Поэтому предлагается реализовать более гибкую систему обмена сообщениями, которая бы предоставляла удобный WEB-интерфейс взаимодействия по протоколу HTTP, а также обеспечивала бы все необходимые защитные механизмы при передаче данных.

Спецификация WS-Security позволяет организовать защиту SOAP-сообщения, вне зависимости от транспортного протокола. В основе WS-Security в свою очередь лежат следующие спецификации:

– XML Signature;
– XML Encryption;
– SOAP.

Удобство протокола SOAP, основанного на XML, позволяет свободно использовать закрытые теги, помещая туда зашифрованную информацию, при этом необходимая служебная информация помещается в заголовок SOAP-сообщения.

Отправленный запрос представляет собой XML-документ, сгенерированный в соответствии со спецификацией WS-security.

Заголовок документа отражает некоторый аспект общей обработки тела SOAP-сообщения. Дочерние элементы вовлечены в обмен информацией между начальным отправителем SOAP-сообщения и SOAP-узлом.

Язык PHP является № 1 в области разработки Web-приложений (по опубликованным рейтингам языков программирования сообщества разработчиков TIOBE Software), поэтому актуальность защищенного взаимодействия Web-служб на базе php-интерфейса будет только возрастать.

ЛИТЕРАТУРА

1. SOAP Версия 1.2 Часть 0: Учебник для начинающих, Рекомендация W3C от 24 июня 2003 года – http://www.w3.org/2002/07/soap-translation/russian/part0.html

2. WS-security – http://en.wikipedia.org/wiki/WS-Security

3. WS-Security – Краткий обзор – http://www.rsi.ru/news/news.asp?id=1343

МОДЕЛЬ НАРУШИТЕЛЕЙ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ЭЛЕКТРОННОЙ КОММЕРЦИИ

С.С. Ерохин, инженер каф. КИБЭВС

г. Томск, ТУСУР, т. 420-191, ess@nalog.fisb.ru

Оценка защищенности информационной системы включает в себя этап формирования контрмер угрозам ИБ [1]. Контрмеры должны быть адекватны дестабилизирующим факторам, которые порождают нарушители. В зависимости от уровня компетенции, технической оснащенности и т.д. нарушители делятся на классы, которые в совокупности образуют модель нарушителей. Модель нарушителей используется в комплексе с классификацией угроз ИБ.

Модели нарушителей, рассматриваемые различными авторами [2–4], не отражают в полной степени все возможные навыки и способности нарушителей. Одни авторы приводят только классификацию внешних нарушителей, другие – внутренних, а комплексной модели нарушителей не приводится. Было принято решение разработать модель нарушителей для информационных систем электронной коммерции.

В соответствии с правом доступа в контролируемую зону были выделены два типа нарушителей: внутренние и внешние. Внутренние нарушители делятся на уровни в соответствии с их правами доступа в ИС организации. Классификация внутренних нарушителей приведена в табл. 1.

Таблица 1

Классификация внутренних нарушителей (сотрудников) ИБ по уровням

Идентификатор	Наименование	Уровень	Описание возможностей
P1	Внутренний пользователь системы	Низкий	Пользователю предоставляется доступ на запуск программ только из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации
P2	Внутренний пользователь системы	Средний	Пользователю предоставляется доступ на создание и запуск собственных программ с новыми функциями по обработке информации
P3	Внутренний пользователь системы	Высокий	Пользователю предоставляется доступ на управление функционированием информационной системой и системой защиты информации

Наряду с внутренними нарушителями – сотрудниками, также могут быть внутренние нарушители – партнеры, клиенты и т.д. Классификация внутренних нарушителей – партнеров приведена в табл. 2.

Таблица 2

Классификация внутренних нарушителей (партнеров, конкурентов) ИБ по уровням

Идентификатор	Наименование	Уровень	Описание возможностей
R1	Партнеры, конкуренты	Низкий	Обладает общедоступной информацией об объекте атаки. Отсутствуют знания в области информационно-телекоммуникационных систем

Внешние нарушители ИБ делятся в соответствии с их уровнем знания, технической оснащенностью и программной составляющей. Классификация внешних нарушителей приведена в табл. 3.

Таблица 3

Классификация внешних нарушителей ИБ по уровням

Идентификатор	Наименование	Уровень	Описание возможностей
Q1	Внешний нелегальный пользователь системы	Любитель	Отсутствуют достаточные знания об объекте атаки. Отсутствуют знания в области компьютерных технологий для идентификации и использования уязвимости ИС
Q2	Внешний нелегальный пользователь системы	Специалист	Обладает общедоступными знаниями об объекте атаки. Обладает расширенными знаниями в компьютерных технологиях. Идентифицирует и использует уязвимости с помощью стандартного программного обеспечения
Q3	Внешний нелегальный пользователь системы	Эксперт	Обладает конфиденциальными знаниями об объекте атаки. Профессионально обладает знаниями в области построения компьютерных систем. Идентифицирует и использует уязвимости с помощью специализированного программного обеспечения и специализированного оборудования

Предложенная модель нарушителей направлена на снижение вычислительной сложности оценки защищенности информационных систем электронной коммерции, так как позволяет оценивать состояние системы под воздействием определенного нарушителя. Класс нарушителей, с учетом которого проводится оценка защищенности ИС, определяется руководством организации и может включать в себя как один класс, так и несколько.

ЛИТЕРАТУРА

1. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТИ; ДМК Пресс, 2005. 384 с.

2. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб.: БХВ-Петербург, 2003. 752 с.

3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия Телеком, 2004. 280 с.

4. Домарев В.В. Безопасность информационных технологий. Системный подход. К.: ООО «ТИД ДС», 2004. 992 с.

ОЦЕНКА ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ЭЛЕКТРОННОЙ КОММЕРЦИИ

С.С. Ерохин, инженер каф. КИБЭВС

г. Томск, ТУСУР, т. 420-191, ess@nalog.fisb.ru

В настоящее время существует множество различных методик оценки защищенности:

– качественные с применением стандартов в области информационной безопасности (NIST 800-30, ISO 27001, Cobit 3rd);

– количественные с применением инструментальных средств оценки защищенности (ГРИФ, АванГард, Cobit).

Все методики имеют общий недостаток. Оценка защищенности проводится по субъективным факторам, воздействующим на информацию, а также во временном срезе, что не позволяет оценить защищенность в интервале времени, а также предусмотреть объективные факторы воздействия на информацию. К объективным факторам воздействия на информацию относятся технические отказы оборудования. Автором предложена методика оценки защищенности с использованием Марковских процессов и учетом субъективных [1] и объективных факторов воздействия на информацию.

Методика оценки защищенности с учетом объективных факторов:

а) построение графа информационной системы [2];

б) построение матрицы переходных вероятностей информационной системы размером [*m*; *n*], $m \in 0...i$ и $n \in 0...j$, где *i*, *j* – количество объектов информационной системы;

в) составляем систему линейных дифференциальных уравнений [3] по формуле

$$\frac{dp_i(t)}{dt} = \sum_{j=1}^{n} p_j(t)\lambda_{ji}(t) - p_i(t)\sum_{j=1}^{n}\lambda_{ij}(t),$$

где $p_j(t)$ – вероятность нахождения системы в состоянии *j*; $p_i(t)$ – вероятность нахождения системы в состоянии *i*; $\lambda_{ji}(t)$ – интенсивность перехода из состояния *j* в состояние *i*; $\lambda_{ij}(t)$ – интенсивность перехода из состояния *i* в состояние *j*;

г) решаем систему линейных дифференциальных уравнений методом преобразования Лапласа и определяем вероятностей состояния системы $p_i(t)$ и функцию готовности $K_\Gamma(t)$:

– преобразуем систему дифференциальных уравнений, подставляя вместо $p_i(t)$ изображение $\hat{p}_i(z)$, а вместо $p_i'(t)$ – выражение $z\hat{p}_i(z) - p_i(0)$;

– составляем по системе дифференциальных уравнений дробно рациональную функцию и находим корни знаменателя:

$$\hat{K}_{\Gamma}(z)=\frac{M(z)}{N(z)}=\frac{z^m+a_1z^{m-1}+\ldots+a_m}{z^n+b_1z^{n-1}+\ldots+b_n};$$

– преобразуем операторную форму функции готовности в оригинал:

$$\hat{K}_{\Gamma}(z)=\sum_{i=1}^{n}\frac{M(z)}{N(z)}e^{z_it};$$

д) определяем функцию простоя и строим график данной функции.

На основании полученных результатов можно будет прогнозировать поведение технических объектов системы. Совместное использование двух методов оценки защищенности, под воздействием объективных и субъективных факторов, позволяет адекватно и своевременно принимать решение по устранению угроз ИБ.

ЛИТЕРАТУРА

1. Мещеряков Р.В., Бондарчук С.С., Ерохин С.С. Модели и методы оценки защищенности информации и информационной безопасности объекта // Безопасность информационных технологий. 2007. № 2. С. 39–46.

2. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М.: Наука. Гл. ред. физ.-мат. лит., 1991. 384 с.

3. Половко А.М., Гуров С.В. Теория надежности. 2-е изд. СПб.: БХВ-Петербург, 2006. 704 с.

ИДЕНТИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ЭЛЕКТРОННОЙ КОММЕРЦИИ

С.С. Ерохин, инженер каф. КИБЭВС

г. Томск, ТУСУР, т. 420-191, ess@nalog.fisb.ru

Идентификация угроз информационной безопасности (ИБ) является одним из наиболее значимых процессов при проведении оценки защищенности информационной системы (ИС). В качестве основы процесса применяют различные формальные модели. Но в большинстве случаев идентификация угроз проводится в соответствии с принятой классификацией угроз, так как выделить все угрозы ИБ практически не представляется возможным.

Различные авторы [1–4] предлагают различные классификации угроз ИБ, но на практике адаптировать их классификации к системам электронной коммерции и отнести угрозу к определенному классу не всегда возможно. Поэтому было принято разработать собственную классификацию угроз ИБ на основе российского ГОСТ Р 51275 –

«Объект информатизации. Факторы, воздействующие на информацию» [5].

В соответствии с данным документом выделяются две основные категории угроз – субъективные и объективные, далее идет разделение на угрозы внутренние и внешние и т.д.

1. Объективные угрозы ИБ.

Внутренние:

1.1. Дефекты, сбои и отказы, аварии технических средств и систем объекта информатизации.

1.2. Дефекты, сбои и отказы программного обеспечения объекта информатизации.

Внешние:

1.3. Явления техногенного характера:

а) непреднамеренные электромагнитные облучения объекта информатизации;

б) радиационное облучение объекта информатизации.

1.4. Природные явления, стихийные бедствия:

а) термические угрозы;

б) климатические угрозы и т.д.

2. Субъективные угрозы ИБ.

Внутренние:

2.1. Разглашение защищаемой информации лицам, имеющим к ней право доступа, через:

а) лиц, не имеющих права доступа к защищаемой информации;

б) передачу информации по открытым линиям связи;

в) обработку информации на незащищенных технических средствах обработки информации и т.д.

2.2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации путем:

а) несанкционированного изменения информации;

б) несанкционированного копирования защищаемой информации.

2.3. Несанкционированный доступ путем:

а) подключения к техническим средствам и системам обработки защищаемой информации;

б) использования закладочных средств;

в) использования программного обеспечения технических средств обработки информации через:

1) маскировку под зарегистрированного пользователя;

2) дефекты и уязвимости программного обеспечения и т.д.;

г) хищения носителя защищаемой информации и т.д.

2.4. Недостатки организационного обеспечения защиты информации при:

а) задании требований по обеспечению безопасности;

б) несоблюдении требований по обеспечению безопасности;

в) контроле эффективности защиты информации.

2.5. Ошибки обслуживающего персонала при:

а) эксплуатации технических средств;

б) эксплуатации программных средств;

в) эксплуатации средств и систем защиты информации.

Внешние:

2.6. Доступ к защищаемой информации с применением технических средств:

а) разведки:

1) радиоэлектронной;

2) оптико-электронной;

3) фотографической;

4) визуально-оптической и т.д.

2.7. Несанкционированный доступ к защищаемой информации путем:

а) подключения к техническим средствам и системам объекта информатизации;

б) использования закладочных средств;

в) использования программного обеспечения технических средств через:

1) маскировку под зарегистрированного пользователя;

2) дефекты и уязвимости программного обеспечения и т.д.;

г) несанкционированного физического доступа к объекту информатизации и т.д.

2.8. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

2.9. Действия криминальных групп и отдельных преступных субъектов:

а) диверсия в отношении объекта информатизации;

б) диверсия в отношении элементов объекта информатизации.

2.10. Искажение, уничтожение или блокирование информации с применением технических средств путем:

а) преднамеренного силового электромагнитного воздействия:

1) по сети электропитания на порты электропитания постоянного и переменного тока;

2) по проводным линиям связи на порты ввода-вывода сигналов и порты связи и т.д.;

б) преднамеренного силового воздействия различной физической среды;

в) использования программных или программно-аппаратных средств при осуществлении:

1) компьютерной атаки;

2) сетевой атаки;

г) воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.

Данная классификация является исчерпывающей для угроз ИБ в информационных системах электронной коммерции.

ЛИТЕРАТУРА

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия – Телеком, 2004. 280 с.

2. Ярочкин В.И. Информационная безопасность. 2-е изд. М.: Академический Проект; Гаудеаемус, 2004. 544 с.

3. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. М.: Горячая линия – Телеком, 2006. 544 с.

4. Домарев В.В. Безопасность информационных технологий. Системный подход: К.: ООО «ТИД ДС», 2004. 992 с.

5. ГОСТ Р 51275 – 2006. Объект информатизации. Факторы, воздействующие на информацию.

ШИФР CA1

С.К. Росошек, к.ф.-м.н., доцент,
О.О. Евсютин, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-403-09-21, korvin@ms.tusur.ru

В данной статье приведены описание шифра CA1, построенного на основе обратимого клеточного автомата на разбиении [1], и некоторые результаты исследования данного шифра.

CA1 – это симметричный блочный шифр на основе обратимого клеточного автомата на разбиении. Ключ составляет 128 бит. Размер блока данных – 144 бита.

Процесс шифрования заключается в следующем: блок данных заполняет решетку клеточного автомата, представляющую собой двумерный битовый массив размером 12×12 бит; из ключа формируется таблица правил, управляющая развитием клеточного автомата; клеточный автомат развивается в течение 32 шагов.

Таблица правил определяет схему разбиения на каждом шаге развития клеточного автомата и таблицу замен. Таблица замен состоит из двух столбцов. В первом столбце перечислены все возможные состояния блока разбиения, второй столбец представляет собой перестановку

первого столбца. Перестановка получается с помощью циклического сдвига первого столбца на p позиций. Значение p постоянно для всех шагов развития клеточного автомата. Схема разбиения на i-м шаге задается парой чисел $\{a_i, b_i\}$.

Блоки разбиения имеют постоянный размер 3×3 клетки. Поэтому схема разбиения на каждом шаге задается парой чисел $\{a_i, b_i\}$, $0 \le a_i \le 2$ и $0 \le b_i \le 2$, а для записи параметра p, определяющего таблицу замен, нужно 9 бит.

Схема разбиения меняется на каждом шаге. Ключ шифрования делится на 32 части по 4 бита. Тогда a_i определяется как сумма 1-го и 3-го битов, а b_i – как сумма 2-го и 4-го. Значение p также определяется из ключа. Ключ делится на 8 частей по 16 бит, биты каждой части складываются друг с другом по модулю 2, результат будет соответствующим битом числа p. Девятый бит p определяется как результат сложения по модулю 2 первых 8 бит.

Для исследования клеточных автоматов на разбиении была разработана программа «Машина клеточных автоматов». Роль данной программы заключается в выборе тех клеточных автоматов или тех групп клеточных автоматов, которые наиболее подходят для построения на их основе шифра. Критериями отбора являются надежность шифрования и скорость обработки информации. Распределение бит в решетке клеточного автомата должно удовлетворять требованиям статистической безопасности, т.е. быть равномерным или приближенным к равномерному. При этом такое распределение бит должно быть достигнуто за число шагов, не превышающее заданное.

Одно из требований, предъявляемых к хорошему блочному шифру, заключается в том, что изменение незначительной части блока открытого текста должно значительно изменить соответствующий блок шифртекста [2]. В идеале каждый бит блока открытого текста должен влиять на весь блок шифртекста полностью. Поэтому число шагов развития клеточного автомата должно выбираться таким, чтобы каждый бит решетки в начальном ее состоянии распространил свое влияние на все остальные биты решетки в процессе развития клеточного автомата.

В процессе исследования шифра CA1 основное внимание было направлено на оценку статистической безопасности. Оценка статистической безопасности шифра проводилась с помощью батареи статистических тестов, описанных в стандарте FIPS PUB 140-1 [3].

По результатам исследования был сделан вывод, что шифр CA1 обладает хорошими показателями перемешивания и рассеивания битов при шифровании. Но также было обнаружено, что для данного шифра существует достаточно большое количество «плохих» ключей. Этот

недостаток должен быть устранен, для чего, в частности, необходимо изменить процедуру развертывания секретного ключа.

ЛИТЕРАТУРА

1. Тоффоли Т., Марголус Н. Машины клеточных автоматов. М.: Мир, 1991. 284 с.
2. Смарт Н. Криптография. М.: Техносфера, 2005. 525 с.
3. FIPS PUB 140-1, Security requirements for cryptographic modules, US DOC/NBS, January 11, 1994.

ПРОГРАММА «СТРАЖ» ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS

И.В. Фролов, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-407-77-62, ivanfr@rambler.ru

В настоящее время существует огромное количество программного обеспечения, такого как: антивирусы, брандмауэры, программы резервного копирования, шифрования данных и т.д. Обычному пользователю трудно ориентироваться в таком разнообразии, а именно в подборе программного обеспечения, необходимого для защиты информации, хранящейся на компьютере.

В операционной системе «Windows XP», начиная со второго обновления (SP2), реализована функция «Центр обеспечения безопасности Windows». Данная функция предназначена для защиты компьютера и облегчает работу с основными возможностями обеспечения безопасности, к которым относятся: определение функционирования брандмауэра, службы автоматического обновления, антивирусного приложения и его версии [1].

Целью данной работы является реализация программы, которая будет не только определять наличие средств защиты информации, но и реализовывать другие возможности по улучшению защищенности информации на компьютере. Программа позволит определять наличие установленного программного обеспечения, осуществляющего защиту компьютера (антивирусов, брандмауэров и др.).

Продукт реализуется таким образом, чтобы он мог расширять свои функциональные возможности за счет модульности. Для разработки программы используется технология динамически подключаемых библиотек DLL (Dynamic Link Library), которые представляют собой универсальный механизм интеграции в программы процедур и функций, написанных другими программистами на различных языках программирования, что позволяет согласовывать программы [2].

Выделяются следующие этапы работы программы, изображенные на рис. 1.

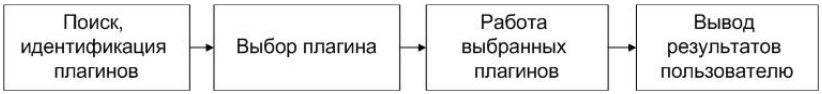


Рис. 1. Этапы работы программы

Программа работает следующим образом. Из главной программы пользователь выбирает и запускает необходимые ему плагины. После запуска программы происходит инициализация переменных, далее идет поиск и идентификация плагинов. Идентифицированные плагины можно запустить двумя вариантами: ручным и автоматическим режимом. При автоматическом режиме запускаются все идентифицированные плагины; используя ручной режим, пользователь выбирает плагины на свое усмотрение. Выбрав необходимые плагины, можно приступать к их запуску. Далее программа выполняет выбранные плагины в порядке очереди. Вызвав плагин, программа передает ему управление, который выполняет и передает результат работы в основную программу.

Поступившие данные из плагина программа отображает в наглядном виде, как это показано на рис. 3. Просмотрев результаты работы приложения, пользователь может увидеть наличие или отсутствие у него, например, антивируса.

На рис. 2 приведена структура программы, состоящей из «Главного блока» и подключаемых плагинов блоков проверки средств защиты информации. Главный блок отвечает за следующие функции: поиск и опрос плагинов, выбор необходимых плагинов, запуск плагинов, выгрузка выполненных плагинов, вывод рекомендаций и результатов работы плагинов.

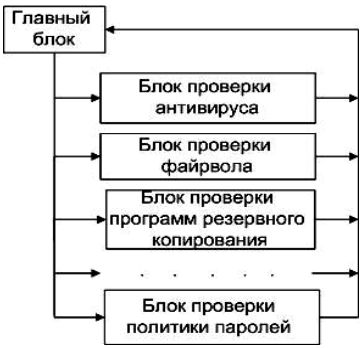


Рис. 2. Структура программы

Блоки проверки реализуют проверку данных и возвращают результат плагина в главный блок. При запуске блока, отвечающего за проверку антивируса, определяется его название, состояние (работает или не работает), а также состояние баз данных антивируса. Собранная

информация передается в главный блок и отображается в наглядной форме, как это показано на рис. 3.

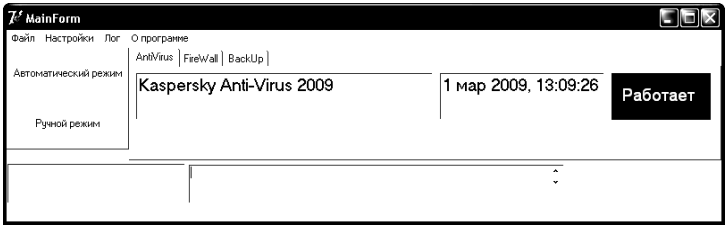


Рис. 3. Программа в действии

Использование технологии динамически подключаемых библиотек для реализации программы «Страж» для операционной системы Windows дает широкие возможности для пользователей. Например, позволяет пользователю писать собственные плагины, реализующие самые разные функции, и при этом использовать любой удобный для него язык программирования. Динамически подключаемые библиотеки позволяют не ограничивать возможность программы несколькими функциями, например, как в «Центре обеспечения безопасности Windows», который ограничен проверкой антивируса, брандмауэра, степени обновления операционной системы. Реализуемые плагины позволяют проверять программы резервного копирования, антивирусы, брандмауэры и давать рекомендации пользователю. В конечном итоге это может привести к увеличению защищенности операционной системы, предоставляя информацию о текущих настройках и их изменении.

В дальнейшем планируется реализация проверки «локальной политики безопасности», а именно параметров безопасности, что позволит пользователю настроить их на максимальную защищенность. Также существует возможность реализовать специальные тесты по проверке установленных продуктов, что позволит пользователю определить, функционирует ли его антивирус, брандмауэр.

ЛИТЕРАТУРА

1. Microsoft Corporation Microsoft Windows XP Professional: учеб. курс MCSA/MCSE/. 2-е изд. 2003. 1008 с.

2. Фаронов В.В. Delphi 6: учеб. курс. М.: Издатель Молгачева С.В., 2001. 672 с.

ЭНТРОПИЙНЫЙ ПОДХОД К ИНДЕНТИФИКАЦИИ АВТОРА И ЯЗЫКА КОРОТКОГО ЭЛЕКТРОННОГО СООБЩЕНИЯ

С.В. Голубев, студент 5-го курса, каф. КИБЭВС,
А.С. Романов, аспирант каф. КИБЭВС,
Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС
г. Томск, ТУСУР, cmisas@sibmail.com

Популярность средств коммуникации посредством обмена короткими электронными сообщениями с возможностью изменения степени анонимности автора и использования их в криминальных целях ставит актуальную задачу идентификации автора.

Целью настоящей работы является исследование возможности применения энтропийного метода идентификации авторов, применительно к коротким электронным сообщениям.

В ходе экспериментов обрабатывались короткие электронные сообщения двух типов: Интернет-пейджера (ИП) и форума.

В ходе первой серии экспериментов оценивалась возможность идентификации автора при помощи вычисления энтропии. Было установлено, что значение энтропии является нестабильной характеристикой. Так, для одного автора на протяжении 30 различных текстов, при объеме выборки в 1000 символов энтропия принимала значения в диапазоне для униграмм 3,149–3,757, для биграмм 4,991–5,583, для триграмм 5,837–6,392 (рис. 1).

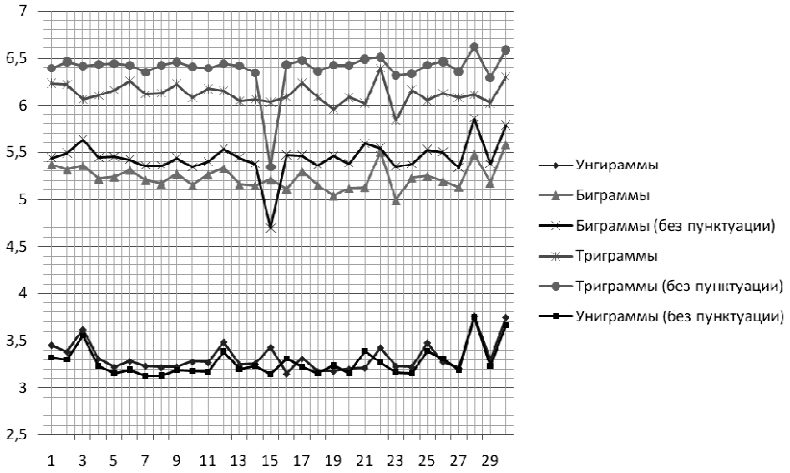


Рис. 1. График энтропий *n*-грамм для 30 различных текстов одного автора объемом выборки 1000 символов каждый

Результаты анализа сообщений Интернет-пейджера разных авторов представлены на рис. 2.

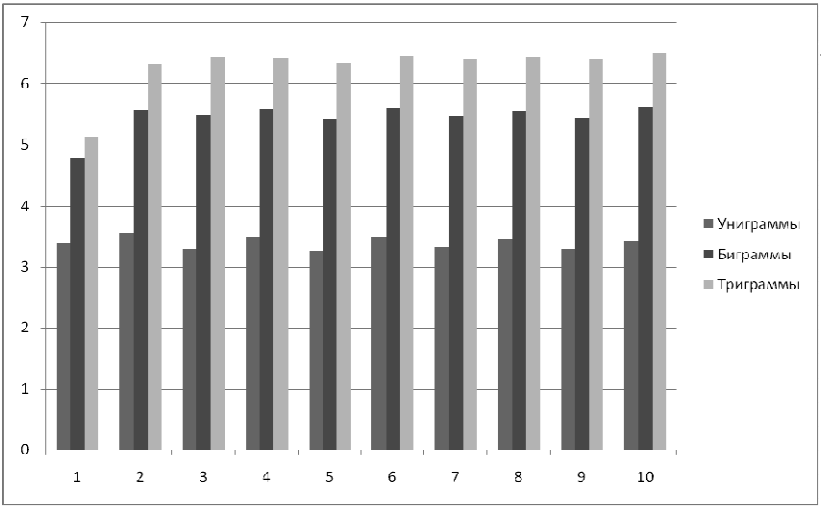


Рис. 2. Гистограмма средних значений энтропий *n*-грамм
для 10 текстов 10 авторов объемом выборки 1000 символов каждый

Исключение знаков препинания незначительно изменяет значение энтропий (табл. 1).

Таблица 1

Средние значения энтропий

Тип сообщения		С учетом знаков пунктуации			Без учета знаков пунктуации		
		Униграммы	Биграммы	Триграммы	Униграммы	Биграммы	Триграммы
ИП	Один автор	3,324	5,237	6,120	3,269	5,441	6,389
	10 авторов	3,396	5,450	6,284	3,325	5,489	6,392
Форум, 10 авторов		3,759	5,608	6,292	3,640	5,593	6,325

Проанализировав полученные данные, можно сделать вывод, что значения энтропии в целом характерны для языка, на котором написан текст, и не являются инвариантом автора.

Для оценки возможности идентификации языка текста были рассчитаны средние значения энтропии 20 текстов разных авторов для четырех языков: русского, английского, немецкого и французского.

Таблица 2

Средние значения энтропий текстов форумов различных языков

Язык	Униграммы	Биграммы	Триграммы
Русский	3,640	5,593	6,325
Английский	2,897	5,027	6,063
Немецкий	2,897	4,884	5,893
Французский	2,870	4,963	6,234

Из табл. 2 видно, что среднее значение энтропии униграмм позволяет классифицировать сообщения различных языковых групп, в данном случае славянской и романской группы. Средние значения энтропии биграмм и триграмм позволяет провести языковую классификацию не только по группам, но и определить конкретный язык автора.

Следующим этапом была оценка возможности идентификации автора вычислением дивергенции *n*-грамм символов.

Вычисление дивергенции *n*-грамм проводились в два этапа для сообщений Интернет-пейджера (ИП) и форума, объем выборки для каждого из типов сообщений принимался равным 1000 и 5000 символов. При этом отдельно рассматривались случаи с учетом и без учета пунктуации. В каждом из экспериментов участвовало по 2 текста для 10 авторов. Данные представлены в табл. 3. В скобках указано количество случаев, в которых истинный автор оказывался в тройке наиболее вероятных претендентов на авторство собственного текста. Общее количество экспериментов 20.

Таблица 3

Количество правильно идентифицированных авторов методом вычисления *n*-грамм

Объем выборки в символах	Тип сообщения	С учетом пунктуации			Без учета пунктуации		
		Униграммы	Биграммы	Триграммы	Униграммы	Биграммы	Триграммы
1000	ИП	0	3(2)	0(5)	0(3)	3(4)	2(3)
	Форум	–	1(4)	1(3)	–	0(3)	1(2)
5000	ИП	2(3)	3(3)	3(1)	0(2)	2(2)	2(4)
	Форум	–	2(4)	2(2)	–	0(4)	2(2)

Проанализировав результаты, можно сделать вывод, что наибольшую эффективность представляет метод, основанный на вычислении дивергенции биграмм символов с учетом знаков пунктуации. Но и его точность следует признать недостаточной.

ЛИТЕРАТУРА

1. Шеннон К. Работы по теории информации и кибернетике. М., 1963. 829 с.

ВЫДЕЛЕНИЕ КЛЮЧЕВЫХ СЛОВ ПРИМЕНИТЕЛЬНО К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.С. Хлебников, Д.В. Черных, студенты 3-го курса, каф. КИБЭВС
г. Томск, ТУСУР, vovka_x@sibmail.com

Целью работы является создание программного комплекса, позволяющего выделять ключевые слова в слитной речи. Актуальность создания данного комплекса очевидна, так как в настоящий момент не существует каких-либо аналогов, а использование этого комплекса возможно и полезно во многих сферах человеческой жизнедеятельности. Возможные области применения создаваемого продукта:

– системы безопасности;
– речевые фильтры;
– телефонные сервисы;
– голосовые меню;
– управление компьютером людей с дисфункцией рук;
– голосовое управление бытовыми роботами.

Помимо вышеперечисленного, программный комплекс такого уровня позволил бы решить ряд фундаментальных и прикладных задач, в том числе задачу сегментации и составления параметрического описания фонем русского языка.

Для реализации проекта необходимо создать речевую базу, позволяющую изучить основные параметры минимальных звуковых единиц языка. В ходе работы были описаны требования к речевому корпусу. Основные и наиболее принципиальные требования:

– необходимость записи голосов различных дикторов (людей разных возрастных категорий, мужского и женского пола);

– наличие всех возможных звуковых единиц русской речи (не слов, а именно единиц-элементов звукового алфавита);

– большое количество различных реализаций этих единиц (голоса разных дикторов, отличный друг от друга эмоциональный окрас сказанных фраз).

Также необходимо описать алфавит минимальных единиц русского языка, позволяющий сегментировать речевую базу на множество элементов.

Все звуковые единицы разделены на классы: гласные и согласные. Гласные, в свою очередь, делятся на подклассы: ударные и безударные. Следует отметить, что и внутри этих подклассов существует градация. Так, согласные подразделяются на твердые и мягкие. Их различие связано с движением средней части спинки языка. Например: _т_уча – _т_елпо, _к_арась – оч_к_и, _б_ык – _б_изон. Существенную роль в звучании ударного гласного играют звуковые единицы, окружающие

его. В связи с этим данный подкласс разбит на четыре группы: 1 – между твердыми (т_а_нк, к_о_т); 2 – между твердым и мягким (п_о_ни, к_о_нь, дет_а_ль); 3 – между мягким и твердым (п_и_р, п_е_карь); 4 – между мягкими (п_е_чь, вес_е_лье). Важным фактором для безударных гласных являются тип согласного перед ним и положение относительно ударного гласного. В связи с этим была использована так называемая формула Потебни: гласные ударного слога – 3 единицы, первого предударного – 2, второго предударного и заударного – 1 единица. По этой формуле безударные гласные разбиваются на следующие группы: силой в 2 ед. после твердого (п_о_дкова), силой в 1 ед. после твердого (половин_а_), силой в 2 ед. после мягкого (пел_и_кан), силой в 1 ед. после мягкого (полнолун_и_е) [1].

На данный момент создан окончательный вариант алфавита. Всего 77 элементов. Это позволяет перейти на следующий этап – сегментацию. Различные русскоязычные фразы из речевой базы будут сегментироваться на множество минимальных элементов. Результаты ручной сегментации будут использоваться для поиска параметров речевого сигнала, характеризующих выделенные минимальные единицы языка.

ЛИТЕРАТУРА

1. Буланин Л.Л. Фонетика современного русского языка. М.: Высшая школа, 1970. 207 с.

КЛАССИФИКАЦИЯ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ ДЛЯ ОПРЕДЕЛЕНИЯ СТРАТЕГИИ ЗАЩИТЫ ИНФОРМАЦИИ

М.А. Хурсевич, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-906-198-80-01, revelator@kvadro.net

Образовательные ресурсы входят в четверку самых востребованных ресурсов Internet. Они необходимы любому человеку, поскольку он должен повышать свои знания на протяжении всего трудоспособного возраста. В России образовательные ресурсы представлены в Internet весьма широко, однако они мало структурированы.

Распределение сайтов по видам ресурсов отображается на рис. 1 гистограммой.

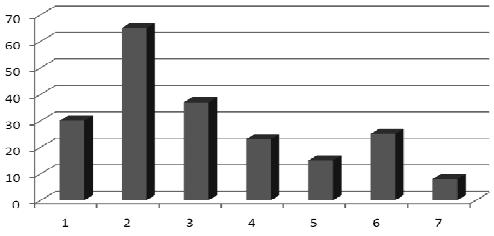


Рис. 1. Распределение основных видов ресурсов по сайтам

Основные виды ресурсов, которые представлены на гистограмме:

1 – образовательные стандарты;

2 – учебные планы, программы учебных дисциплин;

3 – электронные учебные пособия;

4 – тесты;

5 – справочники, классификаторы, архивы, базы данных (БД);

6 – электронные библиотеки;

7 – периодические издания.

Результаты проведенных исследований показали, что ни одна из универсальных информационно-поисковых систем и специализированных информационных систем по проблемам образования не представляет исчерпывающе полный сервис.

При проведении анализа был изучен ряд поисковых систем с точки зрения удобства нахождения образовательной информации, таких как: www.yandex.ru, www.google.ru, www.rambler.ru, www.aport.ru, ruscience.newmail.ru, www.list.ru, http://www.students.ru/.

Оказалось, что Интернет-системы не содержат полного объема информации по сайтам образовательного направления. Выявлена недостаточная структурированность разделов по теме «Образование» как в общих, так и в специализированных поисковых системах.

Аннотирование в половине случаев осуществляется владельцем информационно-образовательного ресурса, в 15% случаев – редактором поисковой системы. При наличии ограничения на количество символов в аннотирование ресурса необходимо либо вводить рекомендации по описанию сайта, либо установить функцию предварительного просмотра аннотации, так как в ином случае она может оказаться неполной или неожиданно обрываться.

Специалисты указывают на такую «болезнь» российского Интернета как «рейтингомания», т.е. ориентация на существующие рейтинги и на существующие системы подсчета посетителей. Однако цифры, показывающие только количество людей, которые обратились к сайту, не отвечают на вопросы о том, как эти ресурсы используются.

Проблемой Интернет-ресурсов остается их незащищенность. На многих сайтах нет даже систем регистрации пользователей, не говоря уже о защите ресурсов данного сайта.

В последние годы в России получили активное развитие различные образовательные ресурсы, доступные через Интернет. Этот процесс энергично продолжается.

Стоит отметить, что в Томске сложилась достаточно уникальная ситуация, связанная с развитием Интернет-технологий. Динамичное развитие внутригородской интрасети позволило подключать к Интернету очень большое количество людей, а буквально за последние пол-

года провайдеры значительно снизили цены на трафик вне Томска и Томской области, что сделало крупные образовательные порталы еще доступнее.

Создание системы российских образовательных порталов направлено на расширение и упорядочение образовательной информации и существенное упрощение ее поиска [1].

Одной из актуальных задач информатизации образования является проблема классификации информационных ресурсов – образовательных электронных изданий (ОЭИ). Также классификация информационных ресурсов является одной из задач при определении защищаемых объектов. Подобная классификация может быть проведена на основе нескольких различных критериев. По выполняемым функциям ОЭИ можно отнести к традиционным учебным изданиям и соответственно, использовать принципы классификации, используемые для учебной книги [2].

Прежде чем переходить к классификации ОЭИ, необходимо выделить основные параметры, характеризующие ОЭИ, которые впоследствии могли бы лечь в основу критериев для классификации. При этом возможные значения подобных параметров требуют как можно более четкой и заранее фиксированной рубрикации.

Универсальную классификацию предметных и образовательных областей, фиксируемых для каждого ОЭИ, определить однозначно невозможно. Это связано, в первую очередь, с многовариативностью тематических направлений. На практике могут быть использованы несколько подходов к классификации образовательных областей. Одной из наиболее общих, универсальных и распространенных с точки зрения практического использования классификаций образовательных областей является классификация, построенная по тематическим направлениям общего и профессионального образования.

Классификации возможных уровней, типов и форм образовательного процесса, для которых могут разрабатываться образовательные электронные издания, достаточно четко фиксированы в существующей системе образования Российской Федерации. Выбор уровня, типа или формы образования для ОЭИ должен осуществляться в строгом соответствии с классификацией.

Следует отметить, что фиксация автором ОЭИ уровня, типа и формы образования носит рекомендательный характер, поскольку конкретные ОЭИ, разработанные для одного уровня, типа или формы, могут быть достаточно эффективно использованы в учебном процессе, характеризуемом другим набором параметров.

Преимущества использования современных информационных технологий при разработке и эксплуатации ОЭИ позволяют адаптиро-

вать функционирование таких изданий к индивидуальным особенностям каждого участника образовательного процесса, а также к специфике целой аудитории обучающихся, что дает разработчикам ОЭИ дополнительные возможности по рубрикации и классификации. В связи с этим система параметров ОЭИ должна быть расширена с помощью одного из возможных значений типа аудитории: абитуриенты, исследователи, менеджеры, преподаватели, учащиеся.

Исходя из указанных выше возможных параметров-критериев можно выстроить многоуровневую классификацию образовательных электронных изданий и ресурсов.

ЛИТЕРАТУРА

1. Домрачеев В.Г., Иванников А.Д., Ретинская И.В., Скуратов А.К. Обзор российских образовательных ресурсов – http://nit.miem.edu.ru/2003/domrachev.htm.
2. Общероссийский классификатор продуктов ОК 005-93.

МЕТОД ЗАЩИТЫ ОТ КОПИРОВАНИЯ РАСПРЕДЕЛЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д.А. Иванов, студент 5-го курса ЭФ, каф. ЭМИС,
И.Г. Боровской, науч. рук., д.ф.-м.н., зав. каф. ЭМИС
г. Томск, ТУСУР, т. 8-903-954-24-21, dima.ivanov@sibmail.com

В связи с ростом количества пользователей имеющих непрерывный доступ в сеть Интернет, в последнее время растет популярность использования программных продуктов, располагающихся не на локальной машине пользователя, а на удаленном сервере в сети Интернет. Это подтверждает К. Манди – шеф Microsoft по исследованиям и стратегии, говорящий о переходе программных продуктов к смешанной схеме – локальной и серверной (Интернет-сервисы). В том числе подобный переход позволит более жестко отслеживать несанкционированный доступ и незаконное копирование программных систем.

Целью данного исследования являются анализ существующего инструментария для создания распределенного программного обеспечения и анализ методов защиты от несанкционированного копирования и распространения программного продукта.

Любое распределенное программное обеспечение состоит из двух частей:

1. Серверная часть. Располагается на удаленной машине и осуществляет все вычислительные операции. Также серверная часть отвечает за разграничение прав доступа пользователей.

2. Клиентская часть. Настольное приложение, с помощью которого пользователь взаимодействует с серверной частью.

Исходя из того, что информационными ресурсами, возвращаемыми сервером, будут гипертекст (HTML/CSS) и интерпретируемый язык Java Script, в качестве клиентской части может выступить Интернет-браузер. Автором были проанализированы пять популярных браузеров: Internet Explorer, Mozilla FireFox, Opera, Safari, Google Chrome. Наибольшую производительность обработки гипертекста и более быструю интерпретацию Java Script кода показал браузер Google Chrome, работающий на свободной технологии для отображения веб-страниц – WebKit. Для полноценной работы программе-клиенту также необходим доступ к системным ресурсам локальной машины (такие как файловая система, системный реестр, буфер обмена и др.). Проанализированные браузеры доступа к системным ресурсам не имеют по причине обеспечения безопасности. В связи с этим автором была проанализирована технология Adobe Integrated Runtime (AIR) – это платформонезависимая среда для запуска приложений, позволяющая использовать HTML/CSS, Java Script, Adobe Flash и Adobe Flex для переноса веб-приложений (Rich Internet Applications, RIA) на настольные ПК. AIR использует технологию WebKit и имеет высокую скорость обработки гипертекста и Java Script. AIR приложения могут функционировать без подключения к Интернет, отправляя накопленные в процессе работы данные в момент появления соединения с сервером.

К преимуществам относится возможность легко перенести готовое HTML- или Adobe Flash\Flex-приложение на компьютер пользователя и осуществить взаимодействие с сервером. AIR-приложения имеют доступ к файловой системе, буферу обмена, имеется поддержка нескольких окон, поддерживается технология drag and drop и др.

К недостаткам относятся ограниченный доступ к SQLite. Приложения, написанные на AIR, являются однопоточными. AIR-приложения – это проприетарное программное обеспечение, т.е. они зависят от среды выполнения Adobe.

Ряд крупных компаний используют в своей деятельности решения на базе Adobe AIR, такие как America Online, NASDAQ, CleVR, Pownce. В Российской Федерации Adobe AIR использовала компания Rambler для разработки приложения «Рамблер-Друзья».

Для защиты программного продукта от несанкционированного копирования автором предложен следующий порядок действий:

1. При регистрации пользователя на сервере ему высылается программа-клиент, в которой спрятан уникальный идентификационный номер зарегистрированного пользователя.

2. При запуске программы-клиента происходит авторизация идентификационного номера на сервере и в случае верного совпадения предоставляется доступ к программному продукту.

3. В случае одномоментного подключения двух и более клиентов с одинаковыми идентификационными номерами клиенты получают отказ в доступе, а зарегистрированному пользователю приходит сообщение о необходимости обновления программы-клиента с новым идентификационным номером.

Таким образом, проведенный в работе анализ позволил определить необходимый инструментарий для создания распределенного программного обеспечения с повышенным уровнем защиты от несанкционированного копирования.

ЛИТЕРАТУРА

1. Таненбаум Э., Стен М. Распределенные системы. Принципы и парадигмы. СПб.: Питер, 2003. 880 с.

2. Уллман Л., Adobe AIR. Разработка приложений с помощью Ajax. СПб.: БХВ-Петербург, 2009. 560 с.

3. Торопков С.С. Альтернативные браузеры. М.: ДМК Пресс, 2006. 320 с.

АТТЕСТАЦИЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Р.К. Измайлов, студент 5-го курса ФВС,
А.П. Зайцев, науч. рук., проф. каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-411-04-34, izmailov@ms.tusur.ru

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» – подтверждается, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации.

Порядок проведения аттестации объектов информатизации на соответствие требованиям безопасности информации включает следующие действия:

– подачу заявки на рассмотрение и проведение аттестации;

– анализ исходных данных по аттестуемому объекту информатизации;

– проведение предварительного специального обследования аттестуемого объекта информатизации;

– разработку программы и методики аттестационных испытаний;

– заключение договоров на аттестацию;

– испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);

– проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации;

– проведение аттестационных испытаний объекта информатизации;

– оформление, регистрацию и выдачу «Аттестата соответствия»;

– осуществление государственного контроля и надзора, инспекционного контроля над проведением аттестации и эксплуатацией аттестованных объектов информатизации;

– рассмотрение апелляций.

Мероприятия по выявлению и оценке каналов утечки информации. Наличие каналов утечки информации определяется физическими свойствами среды распространения сигналов и характеристиками источников информации. Каналы утечки информации на объектах существуют всегда, но опасность они представляют только тогда, когда их информационные сигналы могут быть зафиксированы за пределами контролируемой зоны и расшифрованы. Для безопасности информации необходимо, чтобы уровень сигналов в каналах утечки был ниже воспринимаемого средствами технической разведки или же позволял маскирование сигналов.

Методики и порядок проведения мероприятий по выявлению и исследованию каналов утечки информации определены нормативно-методическими документами. В документах приведен перечень работ по выявлению каналов утечки информации, который предусматривает:

– специальные проверки (СП);

– специальные обследования (СО).

Специальные проверки. Специальные проверки представляют собой проверки технических средств и систем (ТСС) объекта защиты с целью выявления и изъятия специально установленных закладных устройств съема информации непосредственно с ТСС, выявления технических доработок по изменению свойств ТСС, облегчающих умышленный или неумышленный съем информации, выявления различного рода программных закладок съема информации. При проведении специальных проверок применяются специализированные технические средства.

Специальные обследования. Под специальными обследованиями выделенных помещений понимают комплекс мероприятий по выявлению возможно установленных электронных устройств съема информации в ограждающих конструкциях, предметах интерьера, бытовых приборах и проводных коммуникациях выделенного помещения. Специальные обследования, как правило, проводятся с применением специальных технических средств.

Акустические и виброакустические каналы утечки информации. Технический контроль состояния акустической защищенности выделенного помещения проводится в целях документального подтверждения реальной возможности утечки акустической информации из проверяемого помещения во время проведения в нем мероприятий, связанных с обсуждением секретных вопросов.

Побочное электромагнитное излучение (ПЭМИ) технических средств – одна из главных причин существования проблемы электромагнитной совместимости технических средств. Поэтому выявление и инструментальный контроль ПЭМИ всегда входили в число важных задач органов радиоконтроля и лиц, связанных с разработкой и эксплуатацией этих средств.

В случаях, когда технические средства применяются для обработки информации ограниченного доступа, наибольшую актуальность имеют вопросы, связанные с информативными ПЭМИ и наводками информативных сигналов на токопроводящие цепи. Под ними понимают ПЭМИ и наводки, которые содержат сведения об обрабатываемой информации и могут быть перехвачены заинтересованными лицами.

Для проведения аттестационных испытаний при аттестации объектов информатизации необходимо специализированное оборудование.

Программно-аппаратный комплекс «Навигатор» – предназначен для автоматического, автоматизированного и экспертного поиска сигналов ПЭМИН от проверяемых технических средств, измерения частоты и пикового значения амплитуды найденных сигналов, хранения, обработки и представления результатов поиска и измерений в удобном для оператора виде и применяется на объектах сферы обороны и безопасности.

Программно-аппаратный комплекс «Спрут-7» – предназначен для проведения акустических и виброакустических измерений, для проверки выполнения норм эффективности защиты речевой информации от ее утечки по акустическому и виброакустическому каналам, а также утечки за счет низкочастотных наводок на токопроводящие элементы ограждающих конструкций зданий и сооружений и наводок от технических средств в речевом диапазоне частот, образованных за счет акустоэлектрических преобразований.

ЛИТЕРАТУРА

1. Шелупанов А.А., Зайцев А.П., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Томск, 2008.

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.

3. www.nelk.ru – Холдинг предприятий безопасности.

КОМПЛЕКС ПРАКТИЧЕСКИХ РАБОТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Э.Р. Хайретдинов, Р.А. Хусаенов, студенты 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, wooferr@rambler.ru

Дисциплины «Безопасность операционных систем» и «Организационное обеспечение информационной безопасности» являются одними из базовых для специальности 090105 («Комплексное обеспечение информационной безопасности автоматизированных систем»). В связи с этим необходимо приближать курс практических занятий к решению задач, возникающих при создании системы защиты информации какого-либо объекта.

Основными направлениями построения систем защиты информации являются ограничение и обнаружение утечек конфиденциальной информации. Целью представленной работы является разработка комплекса практических работ, приближенных к решению практических задач защиты информации.

В рамках упомянутых дисциплин создается комплекс практических работ, включающих:

– аудит событий безопасности Windows XP Pro;

– ограничение использования программ с помощью встроенных средств Windows XP;

– разграничение доступа к устройствам с использованием DeviceLock;

– ограничение использования цифровых документов при помощи Windows Right Management Service;

– разграничение доступа к файловым объектам с использованием SecrecyKeeper;

– разграничение доступа к файловым объектам при помощи встроенных средств Windows XP Pro.

Основными задачами при построении комплекса практических работ являются:

– составление теоретической части;

– практическое применение программных средств для создания систем защиты информации;

– создание банка заданий для студентов с целью закрепления пройденного материала.

Для создания и проведения аудита событий в Windows XP Pro будут использоваться встроенный редактор групповой политики и журнал событий безопасности. Путем определения параметров аудита для различных категорий событий можно создавать политику аудита [1].

Возможен аудит следующих категорий событий: вход-выход из системы, управление учетными записями, доступ к службе каталогов, доступ к объектам, изменение политики, использование привилегий, отслеживание процессов, системных событий [2].

Для ограничения запуска программ используются политики ограниченного использования программ, встроенные в Windows XP. Можно определить уровень безопасности по умолчанию «неограниченный» или «не разрешено», чтобы разрешить или не разрешить выполнение всех программ. Исключения в уровень безопасности могут быть внесены с помощью следующих правил: правила для хеша, для сертификатов, для пути и для зоны Интернета. С их помощью можно определить программы, разрешенные или запрещенные для запуска [2].

Для разграничения доступа к устройствам используется программный продукт DeviceLock. Данный продукт состоит из приложений и консолей, позволяющих администратору компьютера контролировать доступ пользователей к портам ввода-вывода, устройствам хранения информации, устройствам печати информации и обмена информации. Для обеспечения разграничения доступа DeviceLock встраивается в виде службы ОС. Контроль доступа может выполняться на двух уровнях: уровне интерфейса (порта) и уровне типа (съемное устройство, принтеры, жесткие диски и т.д.). Контроль на уровне типа осуществляется за счет идентификации устройств по комбинации идентификатора производителя (VID), продукта (PID) и серийного номера [3].

Служба управления правами Windows Rights Management Services (далее RMS) предоставляет средства, позволяющие в совместимых приложениях (MS Office, MS Outlook, Internet Explorer) контролировать использование и распространение данных, а именно:

– защищать данные и документы организации в интрасети компании, а также от пользователей, для которых они не предназначены;

– гарантировать безопасность и защиту от подделки;

– ограничивать срок хранения содержимого в соответствии с имеющимися требованиями, даже если это содержимое передается через внешнюю сеть в другие организации;

– требовать журнал аудита, который позволяет отследить, кто получил доступ и использовал содержимое.

Ограничения, которые можно установить к приложению, поддерживающему RMS, следующие: просмотр, печать, сохранение, экспорт, операции с буфером обмена, редактирование, использование макросов, относительные и абсолютные сроки устаревания, требование соединения с сервером RMS для подтверждения разрешений пользователя, ограничение пересылки и возможности ответа [4].

Для разграничения доступа к файловым объектам с применением SecrecyKeeper используется механизм, реализующий контроль действий пользователя по перемещению информации на основе уровня секретности информации, уровней допуска пользователя и уровней безопасности Компьютера, которые могут принимать значения (метки доступа) общедоступно, конфиденциально и секретно. В соответствии с этими принятыми определениями реализуется многоуровневая (мандатная) модель управления доступом. Разграничение доступа осуществляется с использованием серверной части, на которой задаются метки доступа для пользователей, компьютеров и объектов, а также за счет клиентской части, встраиваемой в ОС, на которой производится управление доступом [5].

Дискреционная модель управления доступом реализуется с помощью встроенных средств обеспечения безопасности Windows XP Pro. Для этого применяются возможности файловой системы NTFS. Система NTFS позволяет предоставлять особые разрешения, которые точно определяют, каким образом пользователь может обращаться к тому или иному файлу либо папке. В NTFS все разрешения сводятся к пяти стандартным разрешениям (изменить, чтение и выполнение, список содержимого папки, чтение, запись).

Комплекс разрабатываемых практических работ охватывает основную часть методов борьбы с утечками информации при работе на локальной рабочей станции под управлением ОС Windows. Это позволит при изучении рассматриваемых дисциплин получить комплексное представление о защите информации на локальной рабочей станции.

ЛИТЕРАТУРА

1. http://technet.microsoft.com/ru-ru/library/cc776394.aspx
2. Документация по Microsoft Windows XP Professional
3. http://www.devicelock.com/ru
4. http://technet.microsoft.com/ru-ru/library/cc706990.aspx
5. http://www.secrecykeeper.com

ПРОБЛЕМЫ ПОСТРОЕНИЯ ДЕЦЕНТРАЛИЗОВАННОЙ СЕТИ ПЕРЕДАЧИ СООБЩЕНИЙ

М.М. Хандорин, студент 4-го курса, каф. КИБЭВ

г. Томск, ТУСУР, M.Khandorin@gmail.com

Удобным средством передачи информации в сети Интернет являются децентрализованные логические сети. Они позволяют обмениваться данными, минуя главный узел или сервер, что позволяет увели-

чить скорость передачи данных и надежность сети в целом. Однако при построении такой сети приходится решать серьезные проблемы:

– подключение пользователя к сети, в которой отсутствует центр;

– передачу сообщения по сети;

– обеспечение нормального функционирования сети при выходе одного из пользователей.

Решение первой проблемы – тривиально: для подключения новый пользователь должен любым способом выяснить IP-адрес какого-либо другого пользователя уже вошедшего в сеть, если сеть только создается то первого пользователя. Однако в сети Интернет существуют пользователи, не имеющие реального IP-адреса, – как правило, это те пользователи, которые используют proxy-серверы или выходят в Интернет из локальной сети через роутер, этих пользователей назовем «пассивными». Они не могут вводить новых пользователей в сеть. Кроме того, между двумя «пассивными» пользователями не существует возможности установить прямое соединение, следовательно, доставка сообщений им возможна только через других пользователей. По той же причине при появлении нового «пассивного» пользователя ранее присутствовавшие в сети пассивные пользователи могут узнать о его появлении только из служебного сообщения, рассылаемого пользователем, подключающим нового.

Проблема передачи сообщений в децентрализованной сети лежит за рамками данной статьи, однако для ее решения был избран способ передачи сообщения «по цепочке» от одного пользователя к другому.

Проблема обеспечения нормального функционирования сети при выходе одного из пользователей возникает из-за того, что сообщения в сети передаются по цепочке – возникает необходимость постоянно проверять наличие всех пользователей в сети, и в случае ухода одного из них перестраивать маршрут передачи. Так как для построения сети применялся протокол TCP, для проверки наличия пользователя в сети достаточно отправить ему любое сообщение – наличие отчета о доставке пакета, который является обязательным для протокола TCP, будет означать присутствие пользователя. Так как пассивные пользователи не имеют прямой связи друг с другом, при обнаружении отсутствия одного из «пассивных» пользователей по сети рассылается сообщение о выходе этого пользователя, чтобы другие «пассивные» пользователи могли исключить его из списков пользователей.

Построенная по изложенным выше принципам сеть решает поставленные проблемы.

Среди достоинств сети стоит отметить:

– высокую скорость распространения сообщений;

– низкие затраты трафика у отдельного пользователя.

Недостатками построенной сети являются:
– большое количество служебного трафика;
– сложность построения.

АВТОМАТИЧЕСКАЯ СЕГМЕНТАЦИЯ РЕЧЕВОГО СИГНАЛА НА ВОКАЛИЗОВАННЫЕ ЗВУКИ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

В.В. Компанец, студент 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, memfis_tm@mail.ru

В рамках группового проектного обучения была реализована нейронная сеть по распознаванию вокализованных звуков. В качестве нейронной сети использовался двухслойный перцептрон прямого распространения с промежуточным слоем в 200 нейронов. На вход нейронной сети подавались выходные значения трех параметров:

– medi30 – медиана спектра в каждой из 30 мс;

– assym – асимметрия спектра в каждой из 30 мс;

– maxch30_128 – максимальное значение спектра за 30 мс при 128 каналах.

К вокализованным звукам относятся все гласные звуки, а также согласные звуки, при произношении которых задействованы голосовые связки. В данной работе звуки не подразделялись на мягкие или твердые, также не разделялись согласные относительно их положения в слове. Вместо этого мягкие и твердые варианты произношения одного согласного звука объединялись в одну группу, которой присваивалось название звука. Аналогично объединялись и гласные звуки [1].

В качестве объекта анализа использовались две нейронные сети с объемом обучающей выборки в пять и десять сигналов соответственно. В качестве контрольной выборки использовались 25 сигналов одного диктора, в число которых входили и обучающие выборки (ОВ) каждой сети. В табл. 1 приведен выход нейронной сети для каждого варианта объема выборки по каждой группе звуков.

Таблица 1

Количество вокализованных звуков в контрольной выборке и их распознавание нейронной сетью

Вокализованные звуки в контрольной выборке								
А	О	У	И	Ы	Э	Б, Б’	В, В’	М, М’
105	26	15	49	8	22	9	18	16
Д, Д’	Ж	Й	Л, Л’	Г, Г’	Н, Н’	Р, Р’	З, З’	Итого
17	3	11	53	8	28	26	4	418

Распознанные вокализованные звуки при объеме обучающей выборки в 5 сигналов								
А	О	У	И	Ы	Э	Б, Б’	В, В’	М, М’
105	26	15	48	8	20	9	18	15
Д, Д’	Ж	Й	Л, Л’	Г, Г’	Н, Н’	Р, Р’	З, З’	Итого
12	3	10	52	7	26	24	4	400
Распознанные вокализованные звуки при объеме обучающей выборки в 10 сигналов								
А	О	У	И	Ы	Э	Б, Б’	В, В’	М, М’
105	26	15	48	7	22	9	18	15
Д, Д’	Ж	Й	Л, Л’	Г, Г’	Н, Н’	Р, Р’	З, З’	Итого
16	3	10	52	7	27	24	4	408

В данной работе также были поставлены задачи определения ошибок первого и второго рода нейронной сети и влияния обучающей выборки на эти ошибки. Количество невокализованных звуков для контрольной выборки равно 114. В табл. 2 приведены результаты работы нейронных сетей, количество распознанных звуков и количество ошибок.

Таблица 2

Результаты анализа статистики

ОВ	Ошибка I рода	Ошибка II рода	Количество распознанных звуков		Количество ложных срабатываний
			вокализованных	невокализованных	
5	18 (4%)	26 (23%)	400 (96%)	88 (77%)	14
10	10 (2%)	28 (25%)	408 (98)	86 (75%)	15

Из табл. 2 видно, что ошибка первого рода в 22 раза меньше количества распознанных вокализованных звуков, а следовательно, нейронная сеть может использоваться для выделения вокализованных звуков в речевом сигнале. Ошибка второго рода в три раза меньше количества распознанных невокализованных звуков.

Также из табл. 2 видно, что существенной разницы при изменении объема обучающей выборки не было достигнуто. Таким образом, можно сделать вывод о том, что увеличение объема обучающей выборки не оказывает существенного влияния на улучшение работоспособности нейронной сети.

ЛИТЕРАТУРА

1. Буланин Л.Л. Фонетика современного русского языка. М.: Высшая школа, 1970. 206 с.

ПРОЕКТИРОВАНИЕ, РАЗРАБОТКА И ВНЕДРЕНИЕ WEB-РЕСУРСА, ПОСВЯЩЕННОГО КАФЕДРЕ КИБЭВС

К.О. Изотов, А.В. Меркульев, В.Г. Кондратьева,
студенты 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, МоНСТрuk@ms.tusur.ru

Обмен информацией с помощью сети Интернет стал неотъемлемой частью любой компании, предприятия или же любого учебного заведения.

В сети Интернет организаторы располагают ресурс, где находится необходимая информация. Различные пользователи обладают различными правами на получение информации о данной фирме, предприятии или же учебном заведении. Информация, которая располагается на сайте, может быть доступна только сотрудникам или же студентам, то есть каждый из них может получить информацию, предназначенную для организации внутренней деятельности предприятия, например, о расписании занятий для студентов, об учебной литературе в электронном виде и т.д. Также существует информация, к которой любой пользователь может получить доступ, эта информация является общей и предназначена для общей характеристики предприятия, фирмы или же учебного заведения. Если рассматривать учебное заведение, в данном случае кафедры, то в этом случае общей информацией будет являться информация для абитуриентов, история создания кафедры, контактная информация, информация о преподавателях кафедры (фамилия, имя, отчество, ученые степени, дисциплины, которые преподает данный преподаватель, фотографии), новости кафедры, фотографии и т.д.

Поэтому для любого университета важно иметь свой собственный Интернет-ресурс, который будет предоставлять необходимую информацию не только студентам и преподавателям, но и абитуриентам, желающим получить информацию о данном высшем учебном заведении. Также не менее важно иметь собственный файловый портал, который необходим для упрощения учебного процесса, для более оперативного взаимодействия преподавателей и студентов кафедры КИБЭВС.

Целью проекта является проектирование, разработка и внедрение Web-ресурса, посвященного кафедре Комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС).

Прежде всего на начальных этапах проектирования сайта необходимо определится с системой, которая будет контролировать сайт, а также будет способствовать его управлению.

CMS – Content Management System – это система управления сайтом. Системы CMS позволяют вносить изменения и дополнения на

сайт через удобный редактор. Системы управления сайтами не требуют специальных знаний.

CMS обычно включают в себя различные разделы, которые приведены ниже:

1. Управление структурой сайта.
2. Создание и удаление разделов и подразделов, пунктов меню.
3. Внесение товаров в каталог продукции.
4. Добавление иллюстраций с возможностью загрузки их в базу с локального диска.
5. Редактирование титулов страниц и метатегов.
6. Редактирование текстов страниц.
7. Раздел для новостей.
8. Статистику посещаемости.
9. По желанию – опросы, анкетирование, онлайн-консультации, доски объявлений, страницы отзывов, файловый менеджер.

Если авторская система пишется с нуля, то сначала определяется, какие функции в ней необходимы и как все будет структурировано. Важно сразу продумать названия таблиц, каталогов и файлов. Каждый из компонентов движка разрабатывается и тестируется отдельно и только после успешного тестирования интегрируется в общий проект. Авторские движки сайтов и системы CMS требуют достаточного времени и бюджета для разработки, но бывают случаи, когда такие расходы вполне оправданы.

После выбора или написания CMS, а также разработки графического макета сайта следующим этапом для создания сайта является «верстка».

Верстка Web-страниц представляет собой процесс преобразования графического макета в HTML-код, набор картинок и стилей. В свою очередь, правила преобразования определяются стандартами w3c (World Wide Web Consortium, Консорциум Всемирной паутины). Впрочем, в связи с тем, что большинство производителей браузеров в той или иной степени игнорируют рекомендации w3c, процесс верстки существенно усложняется.

Большинство верстальщиков оптимизирует код под три браузера: Internet Explorer, Firefox и Opera. Иногда к этому списку добавляют еще Safari, основной браузер Mac OS.

Процесс верстки начинается с разделения макета на структурные блоки. Именно это разделение и будет в дальнейшем диктовать основной «скелет» страницы. Чаще всего выделяют такие блоки как header (верхний колонтитул, «шапка»), который включает в себя логотип, меню навигации и иногда баннер (рекламное изображение), content (блок, в котором отображается непосредственно информация)

и footer (верхний колонтитул). Впрочем, верстальщики редко ограничиваются именно такой структурой. Для нашего сайта характерно, что три верхних блока являются header'ом, левый средний блок – content'ом, нижний блок – footer'ом. Назначение правого среднего блока пока неопределенно. Возможно, в дальнейшем он будет использоваться для вывода служебной информации в режиме администрирования.

В дальнейшем каждый из полученных блоков также делится на элементы до тех пор, пока каждый из них нельзя будет отобразить отдельным HTML-тегом. Теги собираются в иерархическую структуру и для каждого из них прописывается стиль, отвечающий за их позиционирование, цвет, шрифт и пр.

После того как организовали правильное отображение страницы в одном из выбранных браузеров, проводится процесс оптимизации для остальных. Существует большое количество разнообразных статей, руководств, советов по оптимизации страниц, таблиц, иллюстрирующих работу тех или иных тегов и стилей в разных браузерах.

В результате пошагового выполнения предложенных действий и в рамках «Группового проектного обучения» внедрили Web-ресурс, посвященный кафедре комплексного обеспечения информационной безопасности электронно-вычислительных систем (КИБЭВС), который в настоящее время находится в рабочем состоянии и преподносит информацию для заинтересованных пользователей (преподавателей, студентов, абитуриентов и их родителей).

ЛИТЕРАТУРА

1. Инструмент сравнения CMS – http://www.cmsmatrix.org/matrix/cms-matrix.

2. TOMSKNET Banner Exchange.http://tbe.tom.ru.

3. Руководство Артемия Лебедева – http://www.artlebedev.ru/ kovodstvo/paragraphs.

4. Habrahabr – http://habrahabr.ru.

РАСПОЗНАВАНИЕ ЗВУКОВ К', С', Т' ПРИ ПОМОЩИ НЕЙРОННОЙ СЕТИ MATLAB

Ю.И. Конькова, студентка 4-го курса, каф. КИБЭВС

г. Томск, ТУСУР, skave@ms.tusur.ru

Одной из важнейших проблем распознавания речи является выделение из слитного потока элементарных лингвистических частиц – фонем. Фонемы обладают многочисленными признаками, которые можно использовать для их классификации и распознавания. Например, звонкость или глухость, мягкость или твердость.

После выделения информативных признаков речевого сигнала можно представить эти признаки в виде некоторого набора числовых параметров (т.е. в виде вектора в некотором числовом пространстве). Далее задача распознавания фонем сводится к их классификации при помощи обучаемой нейронной сети [1]. В данном исследовании для построения нейронных сетей используется пакет Neural Networks (Нейронные Сети) системы MATLAB.

В ходе работы были проанализированы динамические спектрограммы [2] реальных сигналов на предмет нахождения общих особенностей спектра мягких глухих согласных. Спектрограммы строились для 128 частотных каналов. Если разбить их диапазон на три равные части, то в пределах каждого интервала спектр звука носит приблизительно одинаковый характер. Особенности спектра на каждом интервале совпадают у фонем *к'*, *с'*, *т'* (объединим эти звуки в класс для распознавания нейронной сетью): первый интервал характеризуется средней интенсивностью и небольшим разбросом значений спектра, а на втором и третьем интервалах составляющие сигнала имеют низкую интенсивность.

На основе этих наблюдений был создан параметр для нейронной сети, представляющий собой математическое ожидание и дисперсию спектра на каждом частотном интервале. Нейронная сеть прошла обучение на реальных сигналах двух дикторов (первые 25 тестовых фраз для оценки качества речи и узнаваемости голоса диктора из ГОСТ Р 50840-95 «Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости») [3]. Для иллюстрации работы сети были выбраны тестовые фразы тех же дикторов. На рис. 1–3 представлены спектрограммы сигналов и соответствующие выходы нейронной сети. Синим цветом сеть отмечает согласные рассматриваемого класса (*к'*, *с'*, *т'*).

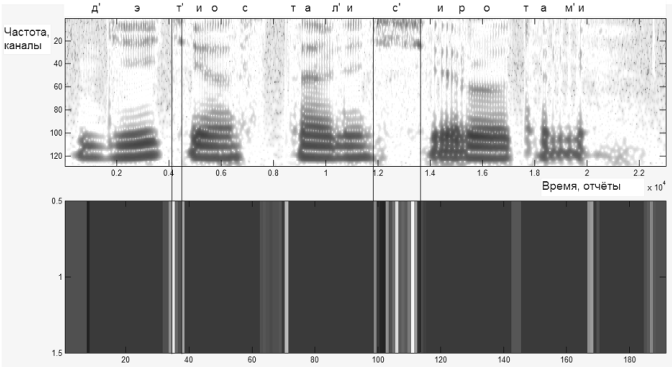


Рис. 1. Спектрограмма и выход нейронной сети для фразы «Дети остались сиротами»

Предварительная оценка эффективности сети дала следующие результаты. Ошибки первого рода (когда сеть не распознает нужную фонему): 23,7% звуков исследуемого класса не распознаются. Не распознаются 40% к’, 7% с’ и 29% т’. Ошибки второго рода (когда сеть выдает «лишний» результат): в среднем 1 ошибка на 35 фонем.

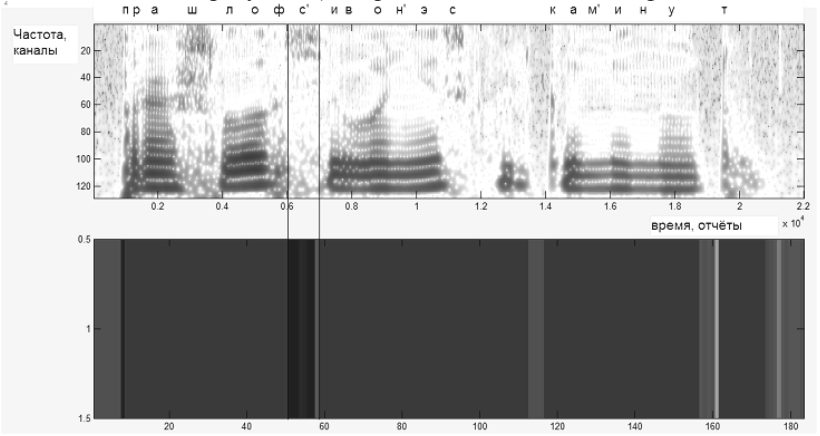


Рис. 2. Спектрограмма и выход нейронной сети для фразы «Прошло всего несколько минут»

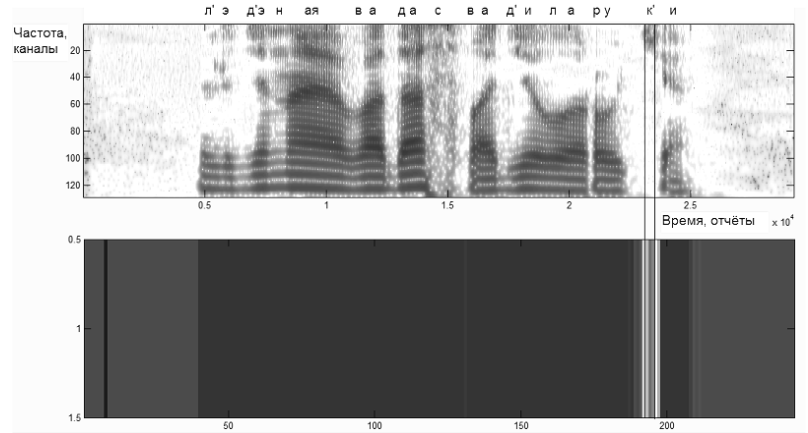


Рис. 3. Спектрограмма и выход нейронной сети для фразы «Ледяная вода сводила руки»

В данном случае множества тестовой и обучающей выборок совпадают. Для получения более достоверных статистических данных требуется расширить тестовую выборку. Планируется дальнейшая ра-

бота по улучшению результатов нейронной сети. Возможно изменение состава звуков распознаваемого класса.

ЛИТЕРАТУРА

1. Фролов А.В., Фролов Г.В. Синтез и распознавание речи. Современные решения. М., 2003.

2. Бондарко Л.В. Звуковой строй современного русского языка. М.: Просвещение, 1977.

3. ГОСТ Р 50840–95 «Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости». М., 1995.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИИ

А.В. Космачев, аспирант каф. РЗИ

г. Томск, ТУСУР, т. 8-913-116-33-06, kosmachev@ms.tusur.ru

Информационное общество, в котором живет сегодня человек, с одной стороны, может стать благоприятной средой для развития личности. Но это же самое общество может стать агрессивной средой, разрушающей личность. Поэтому частная жизнь личности, равно как и жизнь общества в целом, должно быть защищена от разрушительного информационного воздействия [1].

Особым институтом права на неприкосновенность частной жизни в условиях автоматизации и развития новых информационных технологий является институт персональных данных.

В целом ситуация с персональными данными в России по сравнению с другими европейскими странами оставляет желать лучшего. Постоянно происходит воровство БД, содержащих персональные данные. Предприятия же разводят руками, ведь на них не накладывается ответственность, все списывается на недовольных, обиженных сотрудников или хакеров. Поэтому в свободном обращении можно всегда найти базы не только коммерческих фирм, но даже и государственных организаций.

В современном мире к защите конфиденциальных сведений предъявляют все большие требования. В связи с этим нормативные акты, регулирующие обеспечение сохранности персональных данных вообще и работников в частности, предусмотрены не только национальным законодательством, но и международными актами [2].

В России в 2007 г. вступил в силу Закон № 152-ФЗ «О персональных данных». В сферу действия этого нормативного акта попадают все юридические и физические лица, на попечении которых находятся сведения о других граждан. Закон требует, чтобы каждая организация, владеющая персональными данными своих сотрудников, клиентов,

партнеров и т.д., обеспечила конфиденциальность всей этой информации. Хотя для организаций, обрабатывающих персональные данные граждан, предусмотрена отсрочка в выполнении требований ФЗ до 1 января 2010 г., бизнесу и госструктурам необходимо вовсю готовиться к реализации положений закона. Взаимосвязь законодательства изображена на рис. 1.

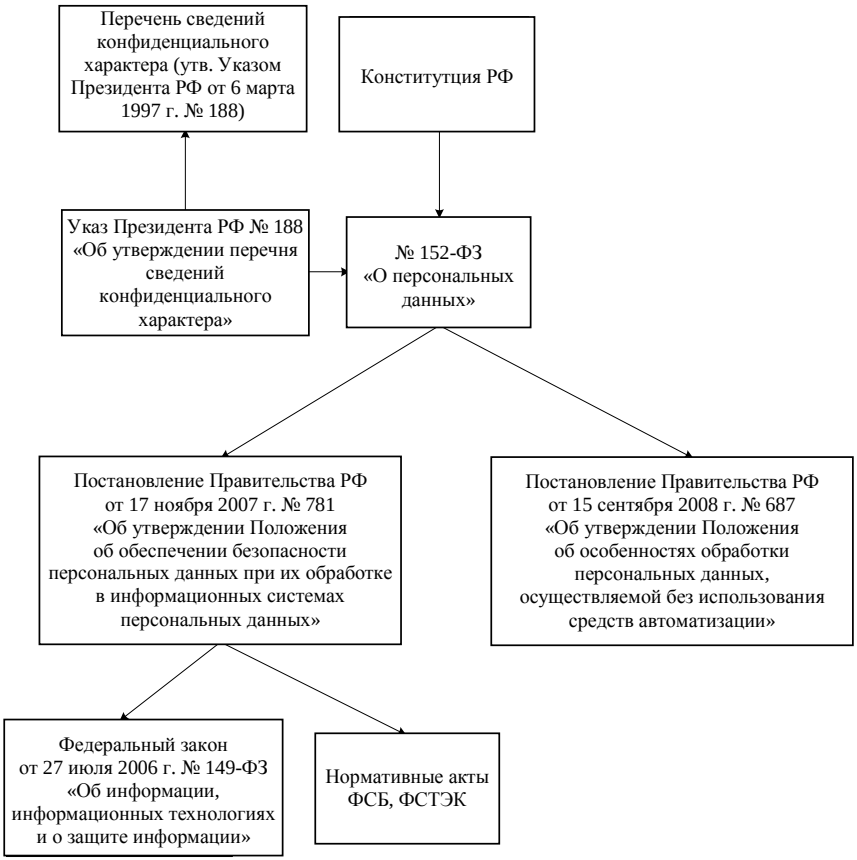


Рис. 1. Правовое регулирование защиты персональных данных

Несмотря на такое большое количество нормативных актов, до сих пор не понятно, как же организовать защиту персональных данных. Существующие нормативные акты ФСБ и ФСТЭК, которые должны были устранить эти недопонимания, изображены на рис. 2 [3].

Но вместо этого методики ФСТЭК закрыли грифом для служебного использования, разделили полномочия ФСБ и ФСТЭК по контролю защиты персональных данных [4]. Учитывая, что к 2010 г. все операторы должны привести свои информационные системы в соответствие требованиям законодательства, должна вестись активная работа по защите персональных данных. Но вместо этого организации положились на русское «авось», а специалисты по защите информации не могут разобраться в дебрях нашего законодательства.

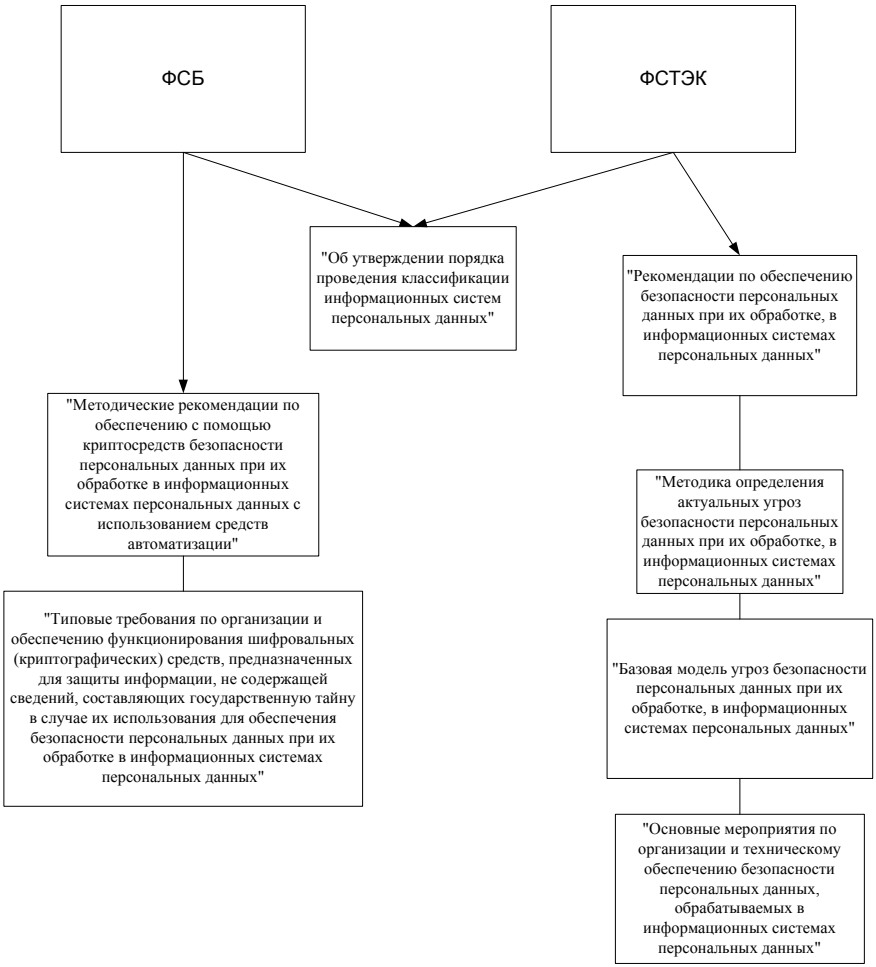


Рис. 2. Нормативные акты ФСБ и ФСТЭК

К сожалению, Закон «О персональных данных» был переписан с зарубежных стандартов, без адаптации к России. Отсюда и данная ситуация непонимания, разделения полномочий на ведомства, издание большого количества нормативных актов, которые еще больше усугубляют положение.

ЛИТЕРАТУРА

1. Охрименко С.А., Черней Г.А. Информатизация общества и права человека – http://www.ase.md/~osa/publ/ru/pubru18.html.

2. Защита персональных данных: Опыт правового регулирования. М.: Галерия, 2001 – http://www.gdf.ru/books/ books/defence/003shtml.

3. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Постановлением Правительства РФ от 17 ноября 2007 г. № 781).

4. Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития. М.: Изд-о Моск. ун-та, 1999. 133 с.

РАСПОЗНАВАНИЕ ПЕЧАТНЫХ СИМВОЛОВ МЕТОДОМ СКЕЛЕТИЗАЦИИ ИЗОБРАЖЕНИЯ

А.В. Ковалев, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, maniagl@rambler.ru

В последние годы распознавание образов находит все большее применение в повседневной жизни. Распознавание речи и рукописного текста значительно упрощает взаимодействие человека с компьютером, распознавание печатного текста используется для перевода документов в электронную форму. Во многих областях техники используются различные автоматы и устройства, более или менее удачно решающие задачу распознавания. Это и автомат для сортировки почтовых конвертов по индексу, и зенитная ракета, захватывающая горячее сопло самолетного двигателя, но игнорирующая солнце, и различные системы анализа спутниковых снимков, и голосовой вызов мобильного телефона, и многое другое.

Программа распознавания занимается тем, что на основе небольшого набора примеров начертаний каждой буквы определяет, какую из них символизирует введенный знак.

Существует множество сложных методов распознавания образов, и теоретические работы по данной теме могут повергнуть в трепет своей монументальностью, но и программы на элементарных алгоритмах, толково реализованные, могут выдавать неплохие практические результаты.

Требуется создать продукт в виде программного обеспечения, решающего задачу распознавания образов печатных символов из растро-

вого изображения и выдающего результат распознавания в виде файла текстового формата. В продукте должен быть применен метод скелетизации исходного изображения.

Задача распознавания включает следующие подзадачи:

– приведение исходного растрового изображения к бинарному виду, т.е. к двумерной матрице черных и белых точек, где объект задается черными точками растра, а фон – белыми;

– сегментация;

– скелетизация полученных образов;

– оптимизация полученных скелетов;

– сопоставление с базой эталонов;

– вывод результатов распознавания.

Все алгоритмы распознавания образов работают с единственным видимым образом. Для разбиения изображения на части, каждая из которых содержит свой уникальный объект, используется сегментация.

Алгоритм скелетизации – это метод распознавания одинарных бинарных образов, основанный на построении скелетов этих образов и выделения из скелетов ребер и узлов. Далее по соотношению ребер, их числу и числу узлов строится таблица соответствия образам. Так, например, скелетом круга будет один узел, скелетом буквы «П» – три ребра и два узла.

Полученный скелет изображения не является оптимальным. Это связано, прежде всего, с тем, что скелет, получаемый из изображения, имеет искажения тем большие, чем меньше размер изображения в пикселях. Другими словами, качество исходного материала, который был подвергнут оцифровке с целью ввода в ЭВМ, сильно проявляет себя в виде дефектов получаемого скелета. Для уменьшения влияния искажений на получаемый скелет необходимо произвести оптимизацию скелета. В оптимизированном скелете возможно представление некоторой последовательности ребер одним отрезком.

В результате создано программное обеспечение, решающее задачу распознавания печатного текста из растрового изображения. Также проведено сравнение результатов распознавания разработанного продукта и программы FineReader 9.0 компании ABBYY. Вследствие сравнения получены данные о «плюсах» и «минусах» обоих продуктов, в зависимости от качества и содержания тестовых исходных изображений.

МОДУЛЬ ИДЕНТИФИКАЦИИ И КРИПТОГРАФИИ БИЛЛИНГОВОЙ СИСТЕМЫ

Б.М. Козлов, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, kbm@admin.tomsk.ru

Человечество в своей повседневной жизни использует все большее количество различного вида услуг. И, как следствие всего этого, возникает потребность в их оплате. Способов оплаты услуг также стало больше. Это связано с развитием технологий и заинтересованности поставщиков в максимальном сборе средств. Наибольшей популярностью на сегодня пользуется оплата посредством электронных терминалов и платежных систем. Масштаб распределенности этих систем огромен. При этом остро встает вопрос об организации защиты информации, передаваемой между сборщиком платежей и поставщиком услуг, посредством различных каналов связи. Информация, таким образом, становится уникальным продуктом, имеющим огромную ценность. Поэтому защита информации является отдельной организационной и технической задачей, связанной с шифрацией передаваемых данных, созданием территориально разделенных резервных серверных мощностей с постоянно актуальной базой данных. Сфера жилищно-коммунального хозяйства – один из наиболее перспективных и динамично развивающихся рынков. Вопросы организации безопасного финансового расчета для нее весьма актуальны. Разрабатываемое программное решение – модуль идентификации и криптографии, используемый в составе биллинговой системы УМП «Единый расчетно-кассовый центр» (далее – ЕРКЦ), – призвано решить эту часть вопросов, используя в себе технологию шифрования передаваемых данных и их цифровой подписи.

Требуется создать продукт для информационной защиты пакетов данных, передаваемых по открытым каналам связи.

Разработка модуля идентификации и криптографии (далее – МИиК) состоит из следующих частей:

1. Анализ предметной области. Изучение архитектуры построения вычислительной сети ЕРКЦ. Анализ используемых аппаратных и программных средств. Изучение схем информационных потоков.
2. Постановка вопросов защиты информации, стоящих перед ЕРКЦ. Выбор объектов защиты.
3. Сравнительный анализ аналогов разрабатываемого МИиК.
4. Постановка задач перед разрабатываемым МИиК.
5. Выбор класса требований разрабатываемого продукта. Анализ правовой части данного вопроса.

6. Сравнительный анализ всех составных критериев разрабатываемого продукта. Выбор оптимальных решений на базе поставленных задач.

7. Разработка продукта.

8. Интеграция МИиК в биллинговую систему. Тестирование.

9. Разработка документации на созданный продукт.

Особенности продукта:

1. Модульный принцип построения.

2. Кроссплатформенность.

3. Производительность. Обработка многопоточности транзакций.

4. Бесплатность ПО при разработки МИиК, что сильно влияет на конечную себестоимость продукта.

В результате работы выполнен сравнительный анализ существующих подходов к организации защиты финансовых данных при обмене ими по открытым каналам связи между УМП «ЕРКЦ» и его клиентами. На основе анализа предложен ряд мер, позволяющий повысить защищенность биллинговой системы ЕРКЦ. Разработан МИиК с целью защиты данных при использовании их вне доверенной вычислительной среды. Созданный МИиК был интегрирован в уже существующий комплекс биллинговой системы ЕРКЦ.

КОМПЛЕКСНАЯ СИСТЕМА КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ДЛЯ СРЕДНЕГО И МАЛОГО БИЗНЕСА

И.А. Кукало, студент 4-го курса РТФ (РЗИ),
Е.Ю. Агеев, к.т.н., доцент
г. Томск, ТУСУР, т. 413-884, i@kukalo.ru

Унификация захватывает самые различные области ИТ, и отрасль ИБ не является исключением. Многие эксперты предсказывают комплексным устройствам управления защитой от угроз большое будущее [1]. Главная цель данной работы – создание системы UTM (унифицированного управления защитой от угроз) на базе свободного программного обеспечения (СПО) [2] с открытым исходным кодом, а также оценка и сравнение системы с ее коммерческими аналогами. Данное устройство ориентировано на потребителей из сегмента малого и среднего бизнеса, где особо важно использование устройств с минимальной стоимостью, простыми и гибкими механизмами внедрения и эксплуатации.

В настоящее время системы UTM включают следующие механизмы защиты [3]:

1) межсетевой экран (МСЭ);

2) систему обнаружения/предотвращения атак;

3) средство построения VPN;

4) систему контроля доступа к Интернет-сайтам (фильтрация URL);

5) антивирус и подсистему защиты от шпионского ПО.

В качестве дополнительных опций в таких системах часто используются:

1. Система контроля электронной почты.
2. Антиспам.

На начальном этапе разработки особое внимание было уделено анализу рынка систем UTM, который позволил выявить следующее:

1. Коммерческие производители систем UTM повсеместно используют СПО.

2. На рынке СПО не существует успешных реализаций систем UTM, сравнимых по функциональности с коммерческими аналогами, хотя стоит отметить наличие большого количества успешных реализаций отдельных составляющих систем UTM.

3. Высокая стоимость коммерческих реализаций систем UTM затрудняет использование продукции в сфере малого и среднего бизнеса, которые обладают ограниченным бюджетом на ИБ.

Таким образом, было принято решение об использовании наиболее удачных реализаций продуктов СПО в собственной реализации системы UTM. Главными требованиями к используемому ПО были выдвинуты его стабильность, функциональность, а также техническая поддержка. Реализованное комплексное устройство включает в себя лучшие наработки рынка СПО и является максимально совместимым с ПО сторонних производителей за счет использования стандартных протоколов IPSec, PPTP, ICAP, X.509, LDAP и т.д. Использование криптографических средств ограничено зарубежными, но наиболее распространенными алгоритмами шифрования – DES, 3DES, Blowfish, AES, алгоритмами хеширования – MD5, MD4, SHA-1, SHA-2, а также алгоритмами реализации ЭЦП – RSA, DH, DSA. Использование российских криптографических алгоритмов присутствует на экспериментальном уровне и не является необходимым для целевой аудитории системы UTM.

Формальные требования по уровню защиты от НСД в соответствии с нормативной документацией: до 1Г, соответствие применяемого МСЭ требованиям четвертого класса защищенности, соответствие применяемых СВТ требованиям шестого класса защищенности.

Итогом работы стала СБ, состоящая из комплекса бесплатного и свободно распространяемого ПО, позволяющая обеспечить следующую функциональность:

1. Защита внутреннего периметра от вредоносного и шпионского трафика.

2. Объединение филиальной сети территориально разрозненной организации в единую ЛВС.

3. Защита внутреннего периметра от НСД со стороны злоумышленников.

4. Контроль целостности системы UTM, расположенной удаленно территориально.

5. Оптимизация и контроль использования ресурсов сети Интернет.

6.Генерирование и обслуживание криптографических сертификатов.

В дальнейших планах – интеграция в проект модуля по борьбе со спамом, а также создание упрощенного интерфейса управления, для этого в состав СБ включена поддержка разработок на языке Java (ПО Apache+Tomcat).

Управление системой UTM осуществляется с помощью командной строки (по протоколу SSH) и большого количества документированных конфигурационных файлов, реализующих различные сценарии применения СБ. Распространение ПО осуществляется посредством использования мультиплатформенных загрузочных дистрибутивов, а также посредством установки дистрибутива на ОС FreeBSD. Предусмотрена сетевая версия установки системы.

Для оценки эффективности предложенной СБ было произведено категорирование информации, подлежащей защите, для типовой организации, и методом экспертной оценки [4] произведен анализ рисков до и после внедрения СБ. В качестве экспертов привлекались начальник отдела ИТ и главный специалист службы безопасности филиала ГПБ (ОАО) в г. Томске. Применение спроектированной системы защиты позволило снизить рассчитанные информационные риски до уровня приемлемых. Снижение уровней высоких и средних рисков составило:

- для информации, составляющей коммерческую тайну, – 78%;
- для информации служебного пользования – 69%.

ЛИТЕРАТУРА

1. Орлов С. Один за всех // LAN, журнал сетевых решений. 2006. № 7.

2. Концепция развития разработки и использования свободного программного обеспечения в Российской Федерации [Электронный ресурс]. Электрон. дан.: Нормативные документы Министерства информационных технологий и связи – Режим доступа:
http://www.minkomsvjaz.ru/upload/docs/20080314101749lP.rtf

3. Лукацкий А.В. Системы защиты «все в одном»: как объять необъятное/ А.В. Лукацкий // Connect! Мир связи. 2006. № 7.

4. Покровский П. Анализ рисков / П. Покровский // LAN, журнал сетевых решений. 2004. № 10.

ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ И ТАБЛИЦЫ ЗАМЕН АЛГОРИТМА ГОСТ 28147–89

И.А. Кукало, студент 4-го курса РТФ (РЗИ)
г. Томск, ТУСУР, т. 413-884, i@kukalo.ru

Отечественный алгоритм шифрования ГОСТ 28147–89 определен в стандарте [2]. Алгоритм шифрует данные 64-битными блоками с использованием 256-битного ключа шифрования. Использование данного алгоритма шифрования подкрепляется законодательством РФ. Государственные организации, а также некоторые коммерческие обязаны использовать для защиты информации только сертифицированные ФСБ и ФСТЭК средства криптографической защиты информации. Получение данных сертификатов подразумевает, что «в указанных криптосредствах реализованы криптографические алгоритмы, объявленные государственными или отраслевыми стандартами Российской Федерации...» [1].

С момента опубликования ГОСТа на нем стоял ограничительный гриф «Для служебного пользования», и формально шифр был объявлен «полностью открытым» только в мае 1994 г. Именно после этого стали появляться результаты криптоанализа, использующие слабые места данного алгоритма шифрования.

Одним из самых известных методов атаки на алгоритмы симметричного шифрования, основанные на сети Файстеля, является дифференциальный криптоанализ, предложенный Э. Бихамом и А. Шамиром [3] в 1990 г. Дифференциальный криптоанализ использует множество пар текстов с определенной разностью, анализ которых позволяет выделить некий ключ (или его фрагмент), который является искомым ключом либо однозначно, либо с наибольшей (по сравнению с другими возможными ключами) вероятностью [4].

Данный метод основан на анализе пар открытых и зашифрованных текстов, между которыми существует определенная разность. При анализе различных алгоритмов разность текстов может быть определена различным образом. Для ГОСТ 28147–89 разность текстов $a1$ и $a2$ определяется как операция XOR между данными текстами:

$$D(a)=a1\oplus a2\,, \qquad (1)$$

где D – разность текстов.

Предположим, имеется два открытых текста $b1$ и $b2$, которые на входе какого-либо раунда алгоритма имеют разность $D(b)$.

Наложение фрагмента ключа операцией XOR не меняет разность текстов, так как

$$D(b)=D(bk)\,, \qquad (2)$$

где $D(bk)$ – разность текстов после наложения ключа шифрования.

Результат побитового сдвига на 11 позиций для разности текстов определяется следующим образом:

$$D(be) = shl(bs1) \oplus shl(bs2) = shl(bs1 \oplus bs2) = shl(bs), \quad (3)$$

где $shl()$ – операция побитового сдвига влево; $bs1$, $bs2$ – значения текстов на выходе таблиц замен.

Таким образом, единственной операцией, существенно влияющей на значение разности текстов, остается табличная замена, и здесь дифференциальный криптоанализ эксплуатирует следующие факты:

- Каждое конкретное значение $D(bk)$ приводит не ко всем возможным значениям $D(bs)$.
- Данные значения $D(bs)$ имеют различную вероятность.

Зная $D(bs)$ и $D(bk)$, можно с определенной вероятностью выделить ключи, используемые в алгоритме шифрования. Для атаки на 32-раундовый ГОСТ необходимо большое количество пар разностей открытых и зашифрованных текстов. На практике такими парами могут служить служебные заголовки файлов, содержащие постоянную, не изменяющуюся информацию и их зашифрованные аналоги.

Поскольку таблицы замен в стандарте [2] не приведены, то очевидно, что криптостойкость алгоритма во многом зависит от свойств используемых таблиц замен, соответственно, существуют слабые таблицы замен (пример таковой приведен в [5]), применение которых может упростить вскрытие алгоритма.

Целью данной работы является создание средства анализа таблиц замен, используемых в алгоритме ГОСТ 28147–89. Главным объектом исследования выступают таблицы замен, используемые Центральным банком (ЦБ) РФ. Значения этих таблиц приведены в [4].

Результатом работы является разработанное программное обеспечение, способное анализировать таблицы замен, используемые в ГОСТ 28147–89. Это достигается путем использования дифференциалов, которые представляет собой пары разностей Δx, Δy над полем двоичных чисел, где x, y – векторы входа и выхода таблицы замен. Для вероятностной оценки возможных значений дифференциалов на входе таблицы замен составляется матрица дифференциалов, которая состоит из всех возможных значений Δx и Δy, т.е. имеет размерность 16*16 значений в соответствии с размером таблицы замен, заданной стандартом [2]. Исходя из этой матрицы, опираясь на известные значения Δy, вычисляются наиболее вероятные значения Δx, что позволяет вычислить x, x' – пары входных векторов. С помощью этих векторов, путем операции XOR со значениями соответствующих открытых текстов, возможно определить значение ключа с определенной долей вероятности (методика описана в [6]).

Анализ таблиц замен, используемых ЦБ РФ, показал что все восемь *S*-блоков имеют достаточно равновероятностные характеристики матрицы дифференциалов. Максимум значения вероятности дифференциала в *S*-блоках равен 0,375, что не является минимумом, но пригодно для практического использования. Наилучшими вероятностными характеристиками обладают второй и пятый S-блоки (таблица).

Количество максимальных значений вероятности дифференциалов

*S*1	*S*2	*S*3	*S*4	*S*5	*S*6	*S*7	*S*8
2	0	5	5	0	2	2	4

Для учебных целей удалось вывести ряд «слабых» таблиц замен, обладающих плохими вероятностными характеристиками, снижающими криптостойкость алгоритма.

ЛИТЕРАТУРА

1. Лукацкий А.В. Особенности использования VPN в России – Режим доступа: http://bugtraq.ru/library/crypto/vpn1.html – своб. Заглавие с экрана.

2. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

3. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems – http://citeseer.ist.psu.edu – The Weizmann Institute of Science – July 19, 1990.

4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си: Пер. с англ. М.: Триумф, 2002. 816 с.

5. Петров А.А. Компьютерная безопасность: криптографические методы защиты. М.: ДМК, 2000. 448 с.

6. Ростовцев А.Г. Теоретическая криптография / А. Ростовцев, Е. Маховенко. СПб. [и др.]: Профессионал, 2004. 485 с.

ЦИФРОВАЯ ПОДПИСЬ НА МАТРИЧНОМ КОЛЬЦЕ

В.В. Летахов, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-521-66-78, letahovvv@sibmail.com

Представьте себе ситуацию: вам отправили по электронной почте документ с конфиденциальной информацией по финансированию на будущий год. Вам необходима абсолютная уверенность в том, что полученный файл совершено идентичен оригиналу и содержащиеся в нем цифры не были изменены «в пути». Подозрение, что документ «в пути» был подделан, появляется, если некоторые цифры не сходятся, а электронная передача велась через внешнюю почтовую систему.

Как убедиться в том, что полученный вами документ – абсолютная копия отправленного вам оригинала [1]?

Для этого существуют алгоритмы идентификации цифровой информации. Здесь стоит уточнить, что алгоритмы работают только с цифровой информацией. Если необходимо идентифицировать текстовый документ или изображение, то путем кодирования нужно получить цифровой аналог данной информации.

Различают несколько алгоритмов идентификации. Контрольные суммы, контроль CRC, хэширование и цифровая подпись – базовые средства аутентификации при цифровой передаче данных.

Контрольные суммы – наиболее простой способ проверки целостности данных, передаваемых в цифровом виде. Вычисляется контрольная сумма (определенное значение, которое идентифицирует цифровую информацию).

Контроль CRC – более совершенный способ цифровой идентификации некоторой последовательности данных. Это вычисление контрольного значения ее циклического избыточного кода (cyclic redundancy check – CRC) [2].

Алгоритмы цифровой подписи – наиболее надежный способ идентификации цифровой информации. Система цифровой подписи заключается в следующем.

Сэм обрабатывает по специальному алгоритму документ, который собирается отправить Тому, в результате получает некоторый параметр, рассчитанный на основании содержимого документа. Обычно это занимает значительно меньше места, чем исходный документ, – параметр 128 или 256 двоичных разрядов. Затем Сэм с помощью своего личного ключа шифрует полученный параметр. Итоговое значение служит цифровой подписью Сэма. Сэм отправляет Тому документ и свою цифровую подпись. Том пропускает документ, полученный от Тома, через тот же алгоритм, которым пользовался Том. Затем Том дешифрует цифровую подпись, полученную от Сэма, пользуясь предоставленным Сэмом ключом общего пользования. Том сравнивает значение параметра, полученного при выполнении, с расшифрованным значением цифровой подписи. Если эти значения совпадают, значит, подпись подлинная и документ «в пути» не подвергся изменениям. В противном случае, либо документ искажен, либо подпись подделана, либо и то и другое [4].

Вероятнее всего, именно по такой или подобной схеме будут вестись дела через Internet или любую другую информационную службу. Этот алгоритм послужил основой проекта государственного стандарта США – Digital Signature Standard (DSS) [5]. В нем применяются: алгоритм Secure Hash Algorithm для расчета параметров хэширования

и криптосистема с ключом общего пользования, известная под названием Digital Signature Algorithm (DSA) и предназначенная для получения цифровой подписи по параметрам хэширования.

Цифровая подпись на матричном кольце – алгоритм, который работает с кольцом квадратных матриц второго порядка. Порядок кольца может быть выбран произвольно. На данном этапе исследования алгоритма берется порядок 2^{64}. Каждый элемент матрицы имеет длину 64 бит. Суммарный размер матрицы 64*4 = 256 бит. Открытым и закрытым ключами являются матрицы по 256 бит. Подпись формируется из двух матриц и имеет размер 512 бит.

Главные параметры алгоритма подписи криптостойкость, быстродействие, длины ключей, длина подписи. Главной задачей на данном этапе исследования алгоритма является его оптимизация путем выбора оптимальных параметров алгоритма подписи. Длина закрытого ключа может быть уменьшена до длины 128 бит, при этом стойкость ключа к перебору уменьшается не существенно. Что касается быстродействия, то в алгоритме будет реализован алгоритм быстрого возведения матрицы в натуральную степень, а также ряд других изменений [6].

Время покажет, будет ли данный метод создания цифровой подписи эффективным. Однако вне зависимости от результата важно другое: действительно существует возможность совершенно безопасно осуществлять цифровые торговые операции.

ЛИТЕРАТУРА

1. http://www.ronl.ru/programirovanie/4712.htm
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2001. 376 с.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.
4. http://student.km.ru/ref_show_frame.asp?id=A9BB5041D847412C90336AD4866CEF0B
5. http://www.security.ase.md/publ/ru/pubru86/
6. http://evgenius.nightmail.ru/publ4.htm

ЗАЩИЩЕННЫЙ ДОКУМЕНТООБОРОТ В UNIX-СИСТЕМАХ

И.В. Маренков, студент 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-906-958-84-90, some_x@inbox.ru

Чтобы электронный документ мог использоваться вместо бумажного, необходимо также обеспечить доверие пользователя к его содержанию, предотвратить несанкционированные изменения и возможность утери (разрушения), организовать упорядоченный доступ поль-

зователей к документам. Как правило, современные системы защищенного электронного документооборота строятся на базе компьютеров под управлением операционных системы семейства Windows фирмы Microsoft, зачастую с применением офисного пакета этого же поставщика. Однако порой не вполне оправданно из поля зрения упускаются UNIX подобные операционные системы, такие как Linux, FreeBSD, Solaris и OpenSolaris, готовые предложить адекватную замену для большинства (или всех) компонентов систем защищенного электронного оборота, применяющихся в операционных семействах Windows. В данной статье будут рассмотрены эти компоненты и варианты их замещения в рассматриваемых операционных системах.

Электронная цифровая подпись обеспечивает такие важные свойства, как удостоверение источника документа и невозможность отказа от авторства. В соответствии с Федеральным законом «Об электронной цифровой подписи» средства электронной цифровой подписи должны быть сертифицированы. Примером сертифицированного средства электронной цифровой подписи работающего в рассматриваемых операционных системах является программное обеспечение CryptoPro CSP [1]. Производитель гарантирует его работоспособность в операционных системах Solaris 9, Red Hat Linux и FreeBSD 5.x.

Использование сертифицированного программного обеспечения в соответствии с упомянутым Федеральным законом позволяет владельцу сертификата ключа подписи подписывать созданные им документы электронной цифровой подписью, которые с точки зрения Российского государства будут равнозначны собственноручно подписанным документам.

Однако многие пользователи операционных систем семейства Windows в нашей стране для подписи электронных документов используют программное обеспечение, соответствующее стандартам OpenPGP [2] и GnuPG [3], являющимся не совместимыми с российскими стандартами ГОСТ Р 34.10–2001 и ГОСТ Р 34.11–94. Причины такого поведения кроются либо в незнании законов, либо в том, что пользователю не критична ничтожность правового статуса подписанного им документа, либо пользователь попросту не является резидентом РФ. В любом случае очевидно, что при построении систем защищенного электронного документооборота возможны случаи, когда поддержка упомянутых стандартов была бы полезна или необходима. И такие средства имеются.

В частности, для всех рассматриваемых UNIX подобных операционных систем доступен почтовый клиент Mozilla Thunderbird, для этого почтового клиента доступны подключаемые модули для поддержки стандартов шифрования OpenPGP и GnuPG. Аналогичные подключаемые модули доступны для почтовых клиентов Kmail и Sylpheed.

В ряде случаев для организации защищенного электронного документооборота вполне достаточно обойтись развертыванием в организации виртуальной частной сети (vpn). Обмен документами через такую сеть позволяет обмениваться документацией по незащищенным каналам, не опасаясь попадания внутренних документов в руки посторонних лиц, что особенно ценно в случае, если организация не имеет собственного помещения или часть ее сотрудников часто бывает в командировках.

Хорошим выбором для организации рассматриваемой сети будет свободный программный продукт под названием OpenVPN [4]. Он позволяет организовать частную сеть поверх протокола TCP или UDP, а также через часть proxy серверов. Причем OpenVPN способен функционировать в качестве сервера или клиента не только в UNIX подобных операционных системах, но и в системах семейства Windows и Mac OS X.

Еще одним простейшим приемом, позволяющим увеличить защищенность документооборота, является шифрование файлов. Microsoft Office (офисный пакет – широко распространенный на системах семейства Windows) имеет встроенные средства шифрования создаваемых им файлов. Этой возможностью нередко пользуются как мерой предосторожности от несанкционированного доступа к документам в небольших организациях. К счастью, при переходе к офисной работе на базе UNIX подобных систем пользователям не нужно отказываться от старых привычек. Доступный на всех рассматриваемых UNIX системах офисный пакет OpenOffice.org полностью поддерживает создание и открытие шифрованных файлов как родного формата – Open Document, так и формата Microsoft Office. Но стоит отметить, что оба офисных пакета по умолчанию создают документы, совместимые с Microsoft Word 2000, что означает применение некриптостойких параметров шифрования [5].

Системы защищенного документооборота, работающие на системах семейства Windows (такие как Docs Vision [6]), зачастую применяются в крупных организациях. Как правило, они интегрируют в себе рассмотренные средства защиты документооборота, такие как шифрование файлов и наложение ЭЦП, дополняя их средствами для хранения сертификатов и закрытых ключей пользователя, журналирования и разграничения прав пользователей. Развертывание подобных систем возможно и на UNIX системах. В частности, компания ЭЛВИС-ПЛЮС разработала [7] систему электронного документооборота в интересах Федеральной службы по техническому и экспортному контролю. Система строится на программно-аппаратной платформе Sun Microsystems и для реализации функций документооборота использует программное

обеспечение Documentum [8]. Решение обеспечивает разграничение прав пользователей, шифрование данных, наложение ЭЦП и журналирование. Кроме того, пользователю доступен не только основной офисный пакет – Star Office, но и унаследованное программное обеспечение фирмы Microsoft за счет терминального доступа к выделенному Windows серверу.

Таким образом, можно заключить, что на данный момент на базе рассмотренных UNIX подобных операционных систем возможна организация защищенного документооборота любого уровня сложности. Руководствуясь этим знанием, руководители больших и малых предприятий, другие ответственные лица могут более гибко строить системы защищенного документооборота, что в конечном счете выльется в минимизацию затрат и повышение эффектности работы.

ЛИТЕРАТУРА

1. http://www.uc-em.ru/services_spo_cryptopro.html
2. https://www.pgpru.com/biblioteka/specifikacii/files?get=rfc4880.txt
3. http://www.gnupp.org/
4. http://openvpn.net/
5. Скляров Д.В. Искусство защиты и взлома информации. СПб.: БХВ-Петербург, 2004. 288 с.
6. http://www.docsvision.com/
7. http://ru.sun.com/solutions/success/government/fstec.html
8. http://www.documentum.ru/

МОДЕЛИРОВАНИЕ ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ

Е.П. Матченко, студент 4-го курса, каф. КИБЭВС,
Ю.М. Филимонов, науч. рук., к.ф.-м.н., доцент каф. КИБЭВС
г. Томск, ТУСУР, fym@keva.tusur.ru

Люди во все времена хотели знать будущее, читать мысли окружающих, быть готовыми к любым ситуациям, возникающим в ответ на их действия. Попробовать заглянуть за грань пространства и времени уже сейчас позволяют новые технологии и методики моделирования сложных систем: узнать, как быстро распространится дезинформация в рядах воинской части, как много людей умрет от чумы за месяц, какие будут последствия от стихийных бедствий, ущерб компьютерной системе от вирусов и многое другое.

Можно ли создать систему, которая помогла бы ответить на интересующие нас вопросы? Для реализации этой программы на первом

шаге мы решили провести моделирование системы аналогично [1], но состоящей из взаимодействующих субъектов двух сортов. Дополнительный атрибут субъектов определял «силу» взаимодействия субъектов.

Взяв миллион особей, для имитации конфликта поделили их на два лагеря, условно назвав одну половину «добрыми», а другую (ту, которая, возможно, заражена или имеет дезинформацию, или же выступает в качестве агрессора) назовем «злыми» (Далее «добрых» назовем «Д», а «злых» – «З»).

Таким образом, пробуя при одинаковых условиях запускать нашу модель вновь и вновь, мы будем получать разные результаты, получать более полную картину происходящего и множество возможных вариантов, которые могут произойти. Наш же миллион особей имеет ряд характеристик. Прежде всего, это лояльность, в нашей системе не запрещен переход особей из категории «Д» в категорию «З» и обратно, сколь угодно раз. Эта лояльность меняется от общения особей друг с другом. В данной работе представлены результаты моделирования при следующих условиях.

Злые особи являются таковыми и другими стать не могут. В отличие от злых, добрые имеют уровень лояльности, от которого зависит, станут они злыми при общении со злыми или останутся добрыми. Уровень лояльности стать злым, после каждой встречи со злым возрастает.

На рис. 1 показано, как особи взаимодействуют друг с другом.

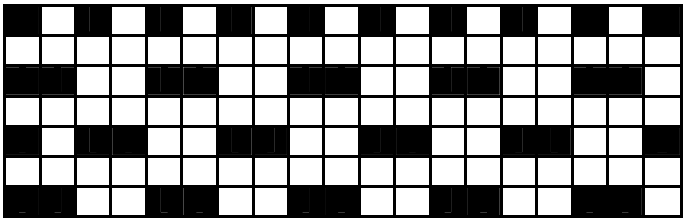


Рис. 1. Взаимодействие субъектов системы

Строка 1 показывает наличие 10 особей, строка 2 показывает попарные встречи особей i и $i + 1$. Строка 3 показывает попарные встречи особей $i + 1$ и $i + 2$ (но в этом случае крайние особи под № 1 и № 10 останутся без партнера для взаимодействия). Остальные строчки аналогичны. Под лояльностью подразумевается вероятность восприятия информации, это вероятность того, что при общении доброй особи со злой особью добрая станет злой, то есть примет информацию злой особи. Для этого было решено взять следующее правило.

Если уровень лояльности (всего уровень может быть от 0 до 9) меньше или равен 5, то особь не воспринимает информацию, но ее лояльность повышается на единицу, если же более единицы лояльность, то особь воспринимает информацию. Результаты моделирования приведены на графике (рис. 2).

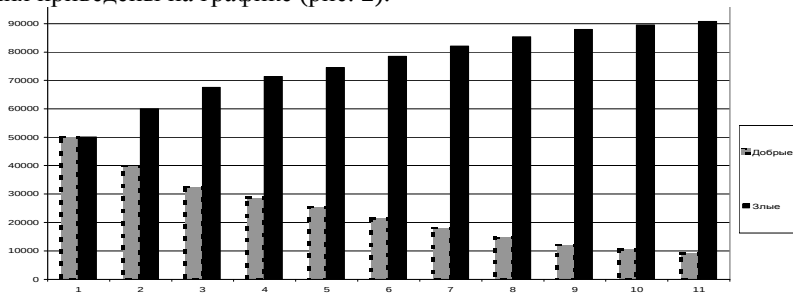


Рис. 2. Число особей в зависимости от количества встреч

График отображает первые 10 встреч (на оси *X* отображается порядковый номер встречи, на оси *Y* – количество особей разного рода). График на рис. 3 показывает поведение особей при одинаковых условиях и правилах поведения.

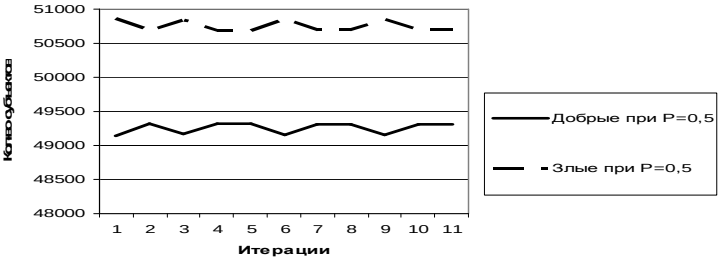


Рис. 3. Число особей в зависимости от количества встреч

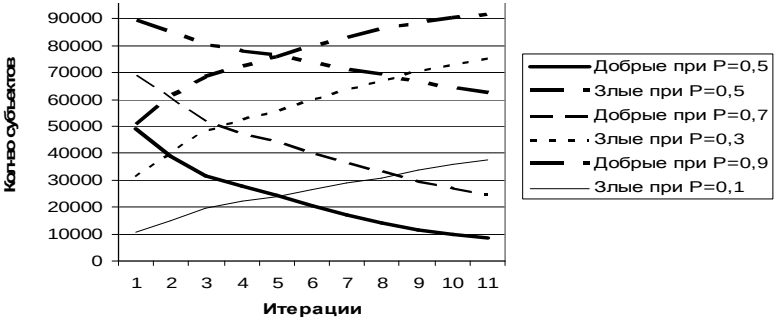


Рис. 4. Зависимость числа субъектов от итераций
для разных начальных условий

На графике рис. 4 представлен результат расчетов, когда особи категории «Д» и «З» имеют прежние правила поведения, но разные условия. В данном примере P – это вероятностное количество особей в разных категориях, то есть $P = 0{,}3$ и $P = 0{,}7$ соответствует процентному соотношению особей в системе примерно 30% к 70% (±3% в среднем из-за вероятностного распределения особей).

ЛИТЕРАТУРА

1. Филимонов Ю.М. Вычисление энтропии системы на основе моделирования субъектов методом Монте-Карло // Доклады ТУСУР. 2008. Т. 2(18). Ч. 1. С. 65.

МЕТОД ПОЛУЧЕНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ ХУКОВ

Ю.С. Михайлова, студентка 5-го курса, каф. ЭМИС,
И.Г. Боровской, науч. рук.
г. Томск, ТУСУР, т. 8-923-408-57-78, charm1234567@yandex.ru

В настоящее время возрос интерес к обучающим системам, системам моделирования, интерактивным программам. Для различных систем и потребностей существует необходимость получения текстовой информации для ее дальнейшей обработки.

Целью данного исследования является разработка метода получения текстовой информации из любого окна приложения, что в дальнейшем позволяет предоставить пользователю необходимую информацию, основываясь на полученных данных.

Операционная система Microsoft Windows уже содержит механизмы, позволяющие получить текстовую информацию, такие как Clipboard, Data Copy, DDE, File Mapping, Mailslots и т.д. Но каждый из способов обладает определенного рода недостатками. В связи с этим был разработан универсальный метод получения текстовой информации из любого окна, основанный на предлагаемых автором «графических» хуках.

В Windows хуком называется механизм перехвата особой функцией событий до того, как они дойдут до приложения. Эта функция может затем реагировать на события и в некоторых случаях изменять или отменять их [1].

В операционной системе существует определенный набор хуков, но все они реализованы лишь для стандартных операций. Нет ни одного системного хука, который мог бы удовлетворить следующей цели –

перехвату графического отображения текстовой информации и последующей замены ее на свою информацию. В связи с этим была разработана методика получения графической информации с помощью создания собственного хука – механизма, позволяющего изъять текстовую информацию из любого окна приложения. Эта методика состоит в том, что происходит установка графического хука, после чего приложение подвергается принудительной перерисовке. Затем происходит изъятие информации из функции TextOut.

Перехват функций чужого процесса удобнее всего осуществлять внедрением собственной DLL с функцией-двойником. Для того чтобы подгрузить нашу DLL в атакуемый процесс, необходимо создать обычный хук WH_GETMESSAGE с пустым обработчиком, после этого DLL подгрузится во все GUI-процессы. Подмена функции осуществляется с помощью непосредственной записи кода перехода в начало перехватываемой функции, используя определенный набор функций записи кода в памяти. Затем с помощью команды jump происходит передача управления на свою «подмененную» функцию, которая может выполнять необходимые нам операции. Следующей трудностью является захват памяти из другого приложения. Получение текста осуществляется изъятием информации из параметра *str, который необходимо поместить в разделяемую между всеми DLL память, используя определенные директивы препроцессора. Затем эту информацию можно редактировать, изменять по своему усмотрению [2, 3].

Данная методика дает следующие преимущества: при выделении определенного слова или при наведении на него курсора мыши в любом окне, в сочетании с нажатием определенной клавиши можно получить определение термина, подсказку, расшифровку, перевод слова или более подробное значение данного термина. Окну лишь необходимо перерисоваться. К тому же, часто Web-страницы защищены от копирования, так, данный механизм дает универсальную возможность получения текстовой информации из страницы. Таким образом, предложенная методика является расширением возможностей операционной системы Windows, поскольку стандартных хуков, выполняющих подобные операции, в системе нет.

ЛИТЕРАТУРА

1. Kyle Marsh, перевод О. Быков «Хуки в Win 32» http://www.rsdn.ru/article/baseserv/winhooks.xml

2. Dr. Joseph M. Newcomer: Пер. А.Остапенко «Хуки и DLL». 2001.

3. Тихомиров В.А. Перехват API-функций в Windows NT/2000/XP – http://www.rsdn.ru/article/basesev/IntercetionAPI.xml

ДЕЦЕНТРАЛИЗОВАННАЯ СИСТЕМА ОБМЕНА СООБЩЕНИЯМИ В СЕТИ ИНТЕРНЕТ

Н.С. Михайлов, студент 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, dem@ms.tusur.ru

В этой статье дан обзор системе обмена сообщениями, которая была спроектирована и разработана в рамках группового проектного обучения по теме «Децентрализованная система обмена сообщениями в сети Интернет».

В настоящее время систем обмена сообщениями в Интернет огромное множество. Самые известные примеры: ICQ, IRC [1] и др. Однако без серверов такая архитектура не имеет никакого смысла. В таких системах именно центральные звенья (серверы) являются наиболее уязвимыми, и в первую очередь подвержены атакам со стороны злоумышленников. Независимо от наличия в сети клиентов сеть будет существовать исключительно при условии существования серверов. Это и является основным недостатком данной архитектуры. Рост клиент-серверной сети, которая тем больше, чем клиентов в нее добавлено, приводит к росту нагрузок на сервер. С каждым новым клиентом нагрузка на центральный узел увеличивается. Таким образом, сеть может становиться перегруженной. Для создания таких систем требуются как дорогие аппаратные средства, так и очень хороший канал связи для сервера.

Целью создания данной системы является отказ от традиционной, использующейся во многих ныне известных программах, централизованной (серверной) схемы обмена сообщениями. При этом значительно затрудняется перехват сообщения в сети, так как заранее не известна траектория передачи этого сообщения. И чем больше пользователей в данной сети, тем сложнее отследить пути передачи сообщения. В данной системе если один пользователь вышел из сети, то это не скажется на работоспособности всей сети. Один высоконадежный и дорогостоящий элемент клиент-серверной сети заменяется множеством менее надежных элементов в децентрализованной сети. Причем надежность децентрализованной сети выше. С каждым новым элементом сети надежность увеличивается, а не уменьшается.

В процессе реализации проектная группа столкнулась с некоторыми трудностями. Например, построение системы, передача сообщений в ней, аутентификация. Из-за того, что не все пользователи могут принимать входящие подключения, передачу сообщений было решено осуществить случайным образом. То есть очередное сообщение доставлялось пользователям почти всегда по новому маршруту. Аутентификацию в децентрализованной системе обмена сообщениями было

решено осуществить на основе асимметричного алгоритма RSA [1]. Осуществленная схема работы системы аутентификации напоминает схему в PGP [1].

Разработанная децентрализованная система обмена сообщениями имеет большие перспективы. Ведь на ее основе можно создать децентрализованный голосовой чат и децентрализованную видеоконференцию. Именно в видеоконференциях нагрузка на аппаратные средства сервера и канала его связи чрезмерно высоки и зачастую серверы не справляются с большим количеством пользователей. Именно в таких ситуациях децентрализованная система может прийти на помощь. Правда, придется решать другие проблемы, такие как оценка канала связи каждого пользователя.

ЛИТЕРАТУРА

1. http://ru.wikipedia.org Википедия. Свободная энциклопедия. Статьи: ICQ, IRC, RSA, PGP.

ТИПОВОЙ КОМПЛЕКТ ДОКУМЕНТОВ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

А.Л. Навойников, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-401-94-52, Frozer@sibmail.com

Основой для разработки «Типового комплекта документов для защиты персональных данных в высшем учебном заведении» явился Федеральный закон № 152 «О персональных данных», принятый 8 июля 2006 г. Данный закон регулирует отношения, связанные со сбором, хранением, обработкой, распространением персональных данных, и касается государственных и муниципальных органов, физических и юридических лиц, обрабатывающих персональные данные с использованием средств автоматизации [1].

Рассмотрим этапы работы создания типового комплекта документов.

1. *Введение в нормативно-правовую базу*.

В настоящее время существует 3 основных общедоступных документа, которые регламентируют отношения, связанные с обработкой персональных данных:

- Федеральный закон №152 «О персональных данных»;
- Постановление Правительства РФ № 781 об утверждении положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

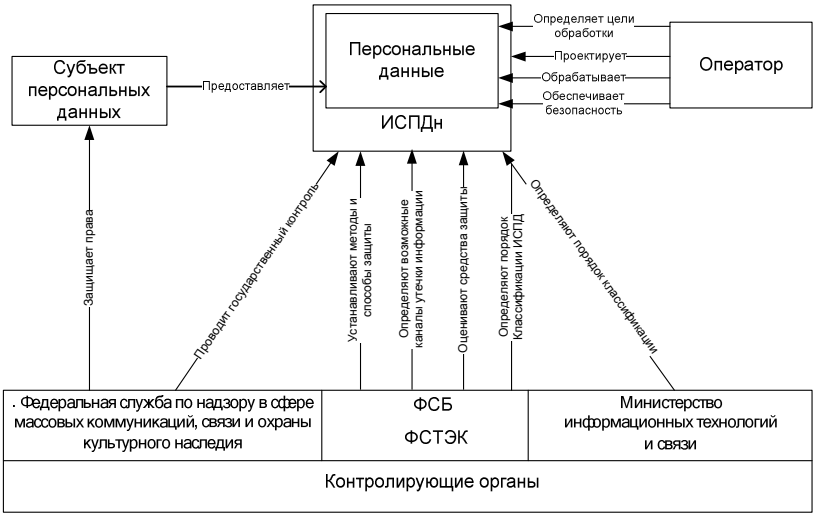


Рис. 1. Отношения при обработке персональных данных

2. *Разработка типовой схемы высшего учебного заведения.*

Разработка типовой схемы производится с целью:

- Определить, в каких отделах и подразделениях циркулируют персональные данные.
- Определить масштабы исследуемых информационных систем.
- Определить классы информационных систем.
- Получить оценку информационной системы для построения модели угроз.

В ходе работы было выделено три основных направления деятельности вуза, где обрабатываются персональные данные.

Учебное: обработка персональных данных на факультетах, кафедрах, в библиотеках.

Административно-хозяйственное: обработка персональных данных в отделе кадров (студенческом, сотрудников), студгородках.

Экономическое: обработка персональных данных в бухгалтерии и планово-финансовом отделе.

3. *Классификация информационных систем персональных данных.*

По степени важности определяют четыре категории персональных данных (Хпд).

По объему (Хнпд) выделяют три категории систем.

Класс типовой информационной системы определяется в соответствии с таблицей [2].

Хпд \ Хнпд	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

4. *Составление перечня угроз и уязвимостей.*

Перечень должен содержать данные по угрозам безопасности персональных данных, обрабатываемых в информационной системе, связанных:

- с перехватом персональных данных по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в информационную систему персональных данных с целью изменения, копирования, неправомерного распространения персональных данных или деструктивных воздействий на элементы информационной системы [3].

5. *Выбор методики оценки актуальных угроз, рекомендаций по устранению угроз.*

В настоящее время существует несколько хорошо известных проработанных методик оценки. В качестве основной можно взять методику оценки, разработанную ФСТЭК. После оценки актуальности каждой угрозы требуется выработать защитные меры против наиболее актуальных угроз.

ЛИТЕРАТУРА

1. «О персональных данных»: Федеральный закон № 152-ФЗ, утв. Президентом Российской Федерации 27 июля 2006 г.

2. «Об утверждении порядка проведения классификации информационных систем персональных данных»: Приказ ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20 от 13 февраля 2008 г.

3. «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»: Постановление Правительства РФ № 781 от 17 ноября 2007 г.

ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ

Н.Ю. Омланд, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, omland@bk.ru

Основными функциями системы анализа информационных рисков будет проведение анализа потенциальных угроз, оценка возможных потерь, а также выбор оптимальных по цене мер по защите, сокращающих риски до приемлемого уровня.

Оценка рисков будет проводиться в следующих направлениях:

− объекты информационной системы;

− программы обработки информации;

− каналы связи;

− механизмы управления системой защиты.

Сначала система производит анализ информационных рисков, который включает в себя следующие этапы:

− выбор информационных ресурсов и объектов, для которых будет проведен анализ;

− разработка методологии оценки риска;

− анализ угроз и определение слабых мест в защите;

− идентификация угроз и формирование списка угроз;

− формирование детального списка угроз.

Чтобы обеспечить надежную защиту, нужно определить возможные угрозы для обеспечения защиты информации и оценить последствия осуществления тех или иных угроз, а также определить меры и средства защиты информации. В связи с тем, что анализ всей системы может быть неоправданным с финансовой точки зрения, в некоторых случаях следует сосредоточиться на наиболее значимых угрозах и последствиях. Также существует вероятность столкнуться с проблемами, связанными с большим разнообразием потенциальных угроз. В этом случае мы не можем рассмотреть каждую из них, поэтому выбор должен происходить, не заходя за рамки здравого смысла, выявляя не только вероятность и масштаб угрозы, но и их источники.

При разработке методологии оценки рисков должны быть получены оценки предельно допустимого и существующего риска осуществления угрозы в течение определенного момента времени. В лучшем случае каждая из угроз должна получить значение вероятности ее осуществления в течение определенного промежутка времени. На практике для большинства угроз невозможно получить достоверные данные о вероятности реализации угрозы и приходится ограничиваться качественными оценками. При разработке методики оценки риска возможно использование методов системного анализа.

Производится оценка ущерба от реализации угроз безопасности, способных нарушить доступность, конфиденциальность, целостность защищаемой информации. Наряду с этим производится оценка затрат на защитные мероприятия и остаточного риска. Также производится предварительная оценка прямых затрат по каждому мероприятию, причем затраты на мероприятия, носящие комплексный характер, не учитываются.

Анализ стоимости и эффективности системы определяется путем определения расходов на систему защиты информации, которую необ-

ходимо соотнести с ценностью информации и ресурсов, использующихся в системе и подвергающихся риску, а также с ущербом, нанесенным организации в результате реализации угроз. После окончания анализа требуется уточнение допустимых остаточных рисков и расходов по мероприятиям, связанным с защитой информации.

В итоге после проведения оценки создается отчетный документ, который должен содержать следующие пункты:

− перечни угроз и рекомендации по снижению вероятности их возникновения;

− защитные меры, необходимые для нейтрализации угроз;

− анализ стоимости и эффективности;

− создание выводов о допустимых уровнях остаточного риска и целесообразности применения конкретных вариантов защиты.

Существует несколько групп оценки риска:

− администраторы информационной системы;

− руководство организацией;

− служба безопасности;

− пользователи системой;

− владельцы данных и приложений.

Администраторы информационной системы несут ответственность за работу данной системы, а также обеспечивают группу оценки риска информацией о конфигурации системы, в которую входят:

− аппаратные средства ЭВМ;

− программное обеспечение;

− данные;

− распределение функций ИС по ее компонентам.

Администраторы могут также указывать на случившиеся воздействия при реализации угрозы.

Руководство организацией ответственно за поддержку политики безопасности системы. Руководство обеспечивает финансирование требуемых служб, а также занимается разработкой руководящих документов, гарантирующих достижение целей политики безопасности. Руководство ответственно за правильную оценку долгосрочных последствий для организации.

Служба безопасности обеспечивает разработку и поддержку политики безопасности, а также контролируют соблюдение правил политики безопасности.

Пользователи системой ответственны за корректное представление точной информации относительно используемых ими данных, ресурсов и приложений.

Владельцы данных и приложений ответственны за то, что их данные (или приложения) адекватно защищены и доступны только уполномоченным пользователям.

При оценке защищенности системы должны быть решены следующие пункты:

1. Ценности.
2. Угрозы.
3. Воздействия.
4. Последствия.
5. Меры защиты.
6. Риск.

Основная цель оценки рисков состоит в определении рисков для системы. Процесс оценки риска проводится в два шага.

Первый шаг:

- определение границ системы для анализа;
- определение степени детализации описания системы;
- определение методологии.

Второй шаг (проведение анализа рисков):

- идентификация ценностей;
- оценка вероятностей;
- измерение риска.

ЛИТЕРАТУРА

1. http://www.fstec.ru/

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОБЪЕКТ

П.Б. Первушин, студент 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-913-881-15-92, pperveshin@sibmail.com

Физические средства представляют собой первую линию защиты информации и элементов вычислительных систем, и поэтому обеспечение физической целостности таких систем и их устройств является непременным условием защищенности информации. Системы контроля и управления доступом являются неотъемлемой частью физических средств охраны объекта. Системой контроля и управления доступом называется совокупность программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещения отдельных помещений, а также оперативный контроль перемещения персонала и времени его нахождения на территории объекта. Система контроля и управления доступом предназначена для выполнения комплекса мероприятий, направленных на ограничение и санкционирование доступа сотрудников на территорию предприятия, в помещения и зоны ограниченного доступа. Система контроля и управления доступом обеспечивает [1]:

1) автоматизацию работы проходной предприятия;

2) регистрацию и учет посетителей предприятия;

3) создание архива с объемом памяти, обеспечивающим регистрацию всех фактов посещения предприятия сотрудниками и посетителями с указанием даты и времени посещения, их фотографий и иных данных с возможностью хранения и использования в течение одного года;

4) возможность ежедневного архивирования базы данных разовых посетителей в конце рабочего дня, ведение протоколов, электронных журналов;

5) многоуровневую организацию доступа с возможностью корректировки базы данных администратором в соответствии с решаемыми задачами;

6) оформление карт доступа в виде пропусков с фотографией и различными данными сотрудника;

7) защиту от несанкционированного проникновения на территорию посторонних лиц;

8) защиту от проникновения во внутренние помещения сотрудников, гостей предприятия и иных посторонних лиц, у которых нет полномочий для доступа в данные помещения;

9) постоянную регистрацию и мониторинг событий в системе контроля доступа (СКД);

10) дистанционное управление замками, а также изменение статуса карт доступа;

11) постоянное наблюдение за состоянием оборудования СКД на мониторе диспетчера;

12) возможность развития за счет расширения программно-аппаратных частей без нарушения работоспособности смонтированного оборудования, а также возможность модернизации в случае изменения или расширения функций, выполняемых системой.

Целью работы является анализ и исследование существующих систем контроля и управления доступом, обеспечивающих контроль и санкционированный доступ на охраняемый объект. В общем случае, представленном на рис. 1, за всеми процессами следит управляющий сервер. Управляющий сервер по сети связан с сервером баз данных, пультами управления и периферийным оборудованием. С другой стороны, управляющий сервер следит за состоянием всех контроллеров, а следовательно, и всего оборудования идентификации. Контроллеры связаны с исполнительными устройствами (шлагбаумами, турникетами, электрозамками и т.п.) и устройствами идентификации (proximity считывателями, ключами touch memory, биометрическими идентификаторами).

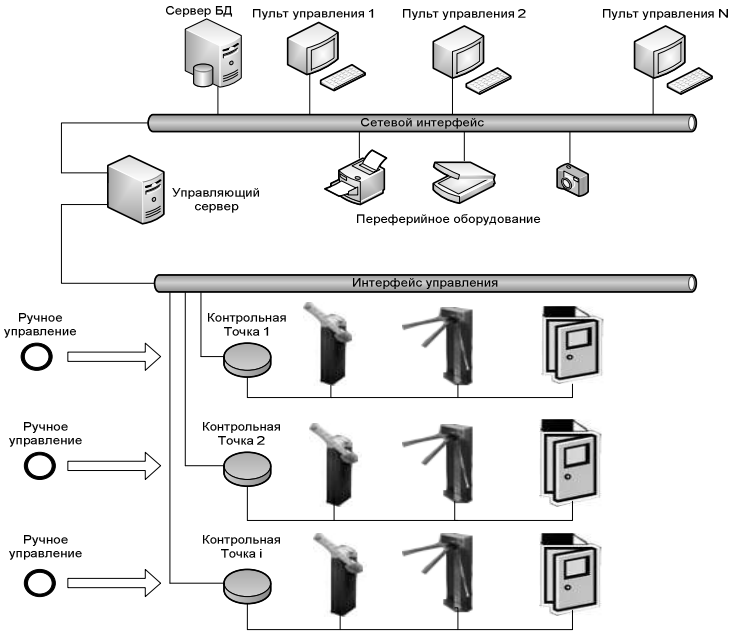


Рис. 1. Общая схема системы контроля и управления доступом

В результате анализа существующих систем контроля и управления доступом было принято решение использовать систему «Кронверк», производителем которой является ЗАО «Системы контроля доступа». Важную роль в принятии решения сыграла возможность предварительного ознакомления со свободно распространяемым программным обеспечением «Кронверк Профессионал». Система контроля «Кронверк» может служить основой для создания интегрированной системы безопасности объекта, работая в едином комплексе средств и систем управления доступом, видеонаблюдения, пожарной автоматики и охранной сигнализации [2].

Возможности системы контроля и управления доступом «Кронверк» позволяют решить одну из задач организации проходных на охраняемом объекте, а именно – исключение утрат бесконтактных карт доступа, выдаваемых посетителям организации. Автоматический сбор гостевых карт доступа производится с помощью специальных картоприемников. Особенностью предлагаемого решения по сравнению с традиционно используемыми является совмещение пропускного пункта для постоянных сотрудников с пропускным пунктом для посетителей, что обеспечивает значительную экономию средств.

В современных условиях система контроля и управления доступом – это не просто набор пропускных устройств, контроллеров, считывателей и т.д., а сложный комплекс организационных и технических мероприятий, процесс управления доступом в котором автоматизирован и практически не требует участия оперативного персонала.

Проанализировав возможности системы контроля и управления доступом «Кронверк», можно сделать вывод о том, что данная система позволяет полностью решить задачу контроля доступа на охраняемый объект персонала и посетителей, контроль перемещения и времени его нахождения на территории объекта, контроль за перемещением грузов, а также совмещать системы видеонаблюдения, пожарной автоматики и охранной сигнализации.

ЛИТЕРАТУРА

1. Зайцев А.П., Шелупанов А.А. Техническая защита информации: учеб. пособие. М.: Горячая линия-Телеком, 2007. 616 с.

2. http://kronwerk.ru – ЗАО «Системы контроля доступа».

ОЦЕНКА КАЧЕСТВА СИСТЕМЫ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ПРЕДПРИЯТИЯ

И.А. Петроченко, студентка 5-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-905-990-79-87, pia87@yandex.ru

Основная цель работы состоит в предложении методов и способов оценки качества системы организационной защиты предприятия. Организационный элемент системы защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы. Эти меры связаны с установлением режима конфиденциальности в фирме. Элемент организационной защиты является стержнем, основной частью рассматриваемой комплексной системы. По мнению большинства специалистов, меры организационной защиты информации составляют 50–60% в структуре большинства систем защиты информации. Это связано с рядом факторов и также с тем, что важной составной частью организационной защиты информации являются подбор, расстановка и обучение персонала, который будет реализовывать на практике систему защиты информации. Организационные меры защиты отражаются в нормативно-методических документах службы безопасности, службы конфиденциальной документации предприятия [1]. Термин «организация» можно рассматривать с двух точек зрения. С одной точки зрения, «организация» – это

существительное, описывающее характеристики текущего состояния системы. С другой точки зрения, «организация» – это отглагольное прилагательное от глагола «организовывать», т.е. «организация» есть процесс управления. Существует множество теорий управления. Одна из них – бюрократическая теория Макса Вебера. Под указанным термином в бюрократической теории понимается форма правления с жестко отработанными (формальными, заранее предопределенными) процедурами. По мнению М. Вебера, такая схема построения организации гарантирует предсказуемость поведения персонала, а значит, возможность достоверного планирования, дисциплину и стабильность.

В данной работе рассмотрена организационная защита с точки зрения этой теории. Для этого выделяются все процессы и регламентируются. Для снижения нагрузки разрабатываются субъектно-объектные модели нормативных документов: выделяются все субъекты и все объекты, определяются «существенные» связи, прописываются все требования, предъявляемые к этим связям, получившаяся модель сравнивается с эталоном. В качестве примера рассмотрен нормативный документ – Положение «О порядке доступа работников к файловой подсистеме автоматизированной системы ООО «Газпром трансгаз Томск» (далее – «Матрица доступа»), который был сравнен с эталонной моделью (рис. 1).

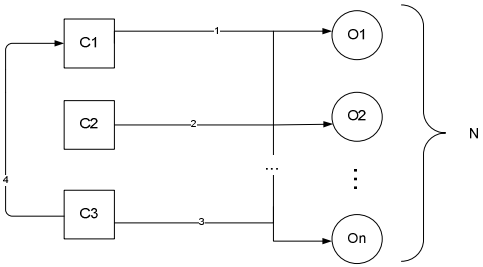


Рис. 1. Эталонная модель матрицы доступа

Объекты: O1 – папка для хранения информации, необходимой для работы 1; O2 – папка для хранения информации, необходимой для работы 2; On – папка для хранения информации, необходимой для работы N. Субъекты: C1 – работник; C2 – начальник структурного подразделения; C3 – администратор информационного ресурса. Связи: 1 – осуществляет доступ; 2 – осуществляет доступ; 3 – осуществляет доступ; 4 – создает персональную папку. Требования: I класс (обязанности): C2-2-O (1, n): Определяет перечень папок, необходимых работнику; C1-1-O (1, n): Следит за правильностью хранения данных в пап-

ках; С3-3-О (1, n): Контроль создания папок, распределение прав доступа между работниками. II класс (права): С2-2-О (1, n): Имеет право на просмотр содержимого папок работника. III класс (ответственность): С1-1-О (1, n): Персональная ответственность за правильность хранения сведений; С2-2-О (1, n): Персональная ответственность за организацию работы своих подчиненных со сведениями; С3-3-О (1, n): Персональная ответственность за создание папок и распределение к ним прав доступа.

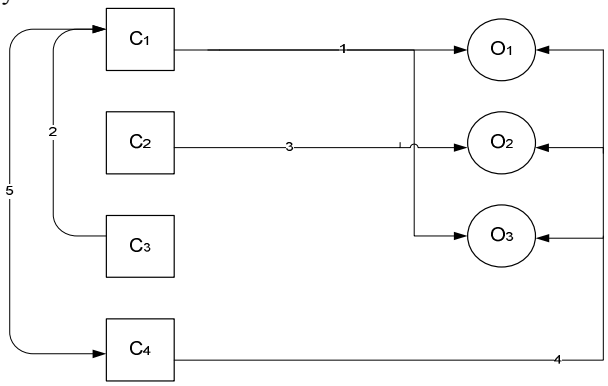


Рис. 2. Матрица доступа

Объекты: О1 – папка «Открытые сведения»; О2 – папка «Конфиденциальные сведения»; О3 – папка «Архив». Субъекты: С1 – работник; С2 – начальник структурного подразделения; С3 – администратор информационного ресурса; С4 – куратор работ. Связи: 1 – осуществляет доступ; 2 – создает персональную папку; 3 – осуществляет доступ; 4 – осуществляет доступ; 5 – С1 может выполнять функции С4. Требования, предъявляемые к взаимодействиям (связям): I класс (обязанности): С2-3-О1, С2-3-О2, С2-3-О3: Определяет перечень папок, необходимых работнику; С1-1-О2, С1-1-О3: После завершения оперативной работы информацию необходимо переместить из О2 в О3; С4-4-О1, С4-4-О2, С4-4-О3: После завершения оперативной работы информацию необходимо переместить из О2 в О3. II класс (права): не указаны. III класс (ответственность): С1-1-О1, С1-1-О2, С1-1-О3: Персональная ответственность за правильность хранения сведений; С2-3-О1, С2-3-О2, С2-3-О3: Персональная ответственность за организацию работы своих подчиненных со сведениями; С3-2-С1: Персональная ответственность за создание папок и распределение к ним прав доступа. В результате сравнения был сделан вывод о возможной доработке этого нормативного документа по ряду пунктов.

Такое представление нормативно-правовой базы дает возможность оценить все взаимодействия, их зрелость и, следовательно, в дальнейшем произвести ряд действий, способных улучшить организационную защиту предприятия.

ЛИТЕРАТУРА

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов. М.: Горячая линия – Телеком, 2004. 280 с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ЗАЩИТЫ САЙТА, РАЗРАБОТАННОГО НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ PHP С ИСПОЛЬЗОВАНИЕМ СЕРВЕРА БАЗ ДАННЫХ MYSQL, ОТ АТАК ТИПА SQL-ИНЪЕКЦИЯ, PHP-ИНЪЕКЦИЯ И МЕЖСАЙТОВЫЙ СКРИПТИНГ

М.А. Приходько, доцент

г. Москва, Институт государственного управления, права и инновационных технологий, т. +7-903-107-83-45, spex19@mail.ru

Язык web-программирования PHP и сервер баз данных MySQL – чаще всего используемая на сегодня «связка» технологий для разработки Web-сайтов. Как и в любой другой сфере, у такой распространенности есть обратная сторона – Web-сайты, разработанные по схеме PHP+MySQL, привлекают наибольшее внимание злоумышленников, а методы их взлома совершенствуются каждый день.

Web-сайты, разработанные на языке PHP с использованием СУБД MySQL, уязвимы для атак типа **SQL-инъекция**, **PHP-инъекция** и **межсайтовый скриптинг**. Эти атаки затрагивают **все** аспекты работы с Web-сайтом – сервер СУБД, файловый сервер, на котором выполняется интерпретатор PHP, и даже клиентскую машину, на которой выполняются Javascript-скрипты. **Децентрализованная** проверка переменных в условиях бурно развивающегося или просто очень крупного проекта неизбежно приводит к возникновению «дыр» в коде, которые незамедлительно атакуются. Поэтому необходима проверка переменных **не в каждом конкретном случае**, а **в самом начале каждой PHP-страницы**, причем проверка автоматизированная и унифицированная. Эта проверка должна осуществляться специальной системой безопасности, которая будет не только обнаруживать и блокировать атаки, но и уведомлять о них администратора Web-сайта, а также протоколировать все несанкционированные действия посетителей Web-сайта.

Система безопасности **geneGuard** построена на основе интеллектуального механизма фильтрации по принципу «черного списка», когда запрещается использование определенного набора слов. При формировании HTML-текста страницы модуль безопасности производит проверку переменных, передаваемых методами **GET** и **POST**, – в тексте значения переменной ведется поиск одного из запрещенных слов. Если атака не была обнаружена, используется оригинальное значение переменной. **Если атака была обнаружена, переменная аннулируется**, а вся информация об атакующем и самой атаке протоколируется в базе данных.

Для борьбы с *PHP-инъекцией* **в начале параметра** (первые 4 символа) выявляется наличие слова *http*, которое трактуется как **подозрение** на выполнение *PHP-инъекции*. В этом случае в начало значения автоматически добавляется слово «*ссылка»:* а администратор получает предупреждение о **возможной** попытке атаки типа PHP-инъекции.

Добавляемое слово «*ссылка»* позволяет, во-первых, в случае **реальной атаки** ее нейтрализовать, а во-вторых, в случае **корректной** (а значит, безопасной) ссылки ее сохранить, не нарушив при этом смыслового содержания значения параметра.

Фильтрация атак типа **межсайтовый скриптинг** производится по словам <script> и </script>.

Фильтрация атак типа **SQL-инъекция** производится по целому перечню запрещенных слов, состав которого зависит от конкретного защищаемого сервера СУБД (в нашем случае – MySQL). Для обработки «пограничных» ситуаций (значений вида «**select***ion*», часть которых является командой языка SQL) после обнаружения запрещенного слова проверяются предыдущий и следующий за словом символы. Окончательное блокирование происходит в случае подтверждения обнаружения «отдельно стоящего» слова, окруженного специальными символами (пробел, скобка, * и др.). Список таких «сигнальных» символов для каждого запрещенного слова может отличаться и хранится в настройках системы безопасности. В тех случаях, когда это возможно, дополнительно производится анализ на наличие целой «структуры» SQL-запроса, например за словом *select* должно следовать слово *from*.

Для борьбы с наиболее распространенными методами «обхода» фильтров перед анализом производится унификация значений переменных. Во-первых, *значение параметра предварительно анализируется на наличие hex-кодов, которые преобразуются в кодировку ascii*. Во-вторых, *перед сравнением значения параметра и запрещенного слова принудительно переводятся в один и тот же регистр* (верхний или нижний).

Еще один способ «изменить» код атаки заключается во внедрении **комментария**, который позволит скрыть запрещенное слово от фильтра, одновременно выполнив атаку (например, ***s/*comment*/elect***). Для борьбы с ним «начало» и «конец» комментария могут быть внесены в список в качестве запрещенных слов. Вторым способом борьбы с подобными действиями может быть модификация механизма унификации значений переменных, в который добавляется этап «вырезания» подобных «комментариев».

Система безопасности geneGuard внедрена на четырех Web-сайтах различной тематики:

- электронный журнал www.elenoize.com;
- сайт научного фонда и научной конференции www.ikf2008.ru;
- сайт музыкального лейбла www.elenoize-records.com;
- сайт Автоматизированной системы интерактивного контроля знаний («Аргус-М») www.argusm.com.

Анализ работы системы на этих сайтах позволяет сделать следующие выводы:

- *система безопасности с фильтрацией по принципу «черного списка»* **не приводит** *к излишне «жесткой» фильтрации в условиях использования ее на русскоязычном сайте и может быть использована без изменений для защиты сайтов различной тематики*;
- *существующие методики обхода систем безопасности, построенных по принципу «черного списка», естественным образом предлагают механизмы защиты, которые встраиваются в единую технологию путем добавления специального вида запрещенных слов, используемых для сокрытия атак.*

Система geneGuard функционирует с мая 2008 г. по настоящее время (март 2009 г.). За этот период выявлено более 80000 (84909!) различных действий, которые были расценены как несанкционированные. Из них около 2000 приходится непосредственно на атаки типа SQL- и PHP-инъекция (остальные являются результатом работы различных «ботов»). Это еще раз подтверждает актуальность проблемы и явным образом указывает на ее важность.

Система безопасности geneGuard распространяется **свободно** и **бесплатно**. Подробнее познакомиться с системой, а также скачать базовые исходные коды можно на сайте автора:

http://www.argusm.com/article.php?id=158

КОМПЬЮТЕРНЫЙ ВИРУС КАК БАЗИС РАЗВИТИЯ СРЕДСТВ ЗАЩИТЫ БУДУЩЕГО

М.А. Приходько, доцент

г. Москва, институт государственного управления, права и инновационных технологий, т. +7-903-107-83-45, spex19@mail.ru

В медицине, где ненанесение вреда – один из основных принципов, уже давно используются опасные, а иногда и просто смертельные вирусы во благо человека. Например, при изготовлении «живых вакцин», которые по своей сути представляют **живой вирус**, ослабленный специальным образом, чтобы, будучи введенным в организм человека, дать последнему возможность выработать антитела. Так и компьютерные вирусы могут использоваться не только для **сознательного** анализа средств защиты, но и стать **прототипом** средств защиты нового поколения.

Глобальную информационную систему (совокупность всех аппаратных и программных средств) можно рассматривать как *информационный организм*. С этой точки зрения разумно защищать не каждую отдельную *информационную клетку* (неделимый программно-аппаратный комплекс – компьютер), а весь организм в целом. Для этого необходимо разработать глобальную *информационную иммунную систему*, основной составляющей которой станут *компьютерные антитела* – вирусоподобные программы, направленные на уничтожение угроз определенного характера.

По аналогии с организмом человека (и его иммунной системой) число компьютерных антител должно **контролироваться**. Компьютерные антитела не должны распространяться (размножаться) бесконтрольно, а необходимо поддерживать определенную популяцию, размер которой может быть увеличен при обнаружении очага заражения компьютерным вирусом.

При обнаружении очага заражения компьютерные антитела должны иметь возможность сообщить о нем другим компьютерным антителам, обладающим необходимыми свойствами для уничтожения найденного вируса. А последние должны иметь возможность быстрой репродукции и перемещения к очагу заражения.

Сформулируем минимальные требования к компьютерным антителам:

- возможность обмениваться сообщениями друг с другом;
- возможность размножаться;
- возможность не только хаотичного, но и целенаправленного перемещения;

- возможность самоуничтожения;
- возможность поддержания размера популяции.

Очевидно, что широкое использование компьютерных антител возможно только после решения целого ряда задач:

- реализация механизма идентификации компьютерного антитела (в том числе антивирусными программами), защищенного от возможности использования этого механизма вредоносными вирусами;
- реализация механизма коммуникации между антителами;
- реализация механизма саморегуляции численности популяции компьютерных антител определенного вида;
- реализация механизма целенаправленной репродукции и самоуничтожения;
- реализация механизма целенаправленного перемещения компьютерного антитела к очагу заражения;
- решение правовых проблем.

Второй вариант использования «хороших вирусов» – целенаправленная проверка качества средств защиты или анализ путей распространения компьютерных вирусов.

В первом случае компьютерный вирус исполняет роль «сканера на уязвимости». В его задачи входит передача информации о найденной уязвимости проверяющей структуре.

Во втором случае безопасный вирус распространяется всеми возможными способами для анализа путей перемещения компьютерных угроз и построения карты маршрутов их наиболее быстрого распространения.

Каждый экземпляр «хорошего вируса» должен снабжаться индивидуальным **уникальным** идентификатором, который от родителя, порождающего новую копию вируса, будет передаваться «ребенку» (помимо его собственного идентификатора). Это позволит не просто узнать «куда» распространяются вирусы, но и «как», в том числе – выявить очаги, порождающие самые крупные волны заражения, так как наличие иерархической связи между экземплярами вируса позволит подсчитать число порожденных копий вируса, а также построить маршруты распространения от самой первой до самой последней копии.

Второе необходимое свойство – возможность накапливать информацию о «родителе», породившем данный экземпляр вируса, а также всех его родителях, пока не будет найдена первая возможность передать эту информацию средствами электронной связи в аналитический центр.

Самая серьезная проблема использования «лакмусовых вирусов» – правовые аспекты такой деятельности. Не только сама возможность

использования доброкачественного вируса, который распространяется «скрытно» от пользователей, но и объем и характер информации, который разрешен для сбора таким вирусом. Будет ли создана юридическая база для использования подобных механизмов – от этого зависит будущее современных средств защиты.

Тем не менее пример современной медицины вселяет надежду на то, что в той или иной форме опыт, накопленный компьютерными злоумышленниками, в конце концов будет использован не только для нанесения вреда, но и для защиты от подобных действий. И однажды защищать персональный компьютер будет не только личный антивирус, но и целая информационная иммунная система.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОТДЕЛЕ КАДРОВ ОРГАНИЗАЦИИ

А.А. Пуха, студент 5-го курса РТФ
г. Томск, ТУСУР, a.a.puha@mail.ru

В XXI в., веке информационных технологий, особое место занимает информация. Общество всецело зависит от получаемых, обрабатываемых и передаваемых данных. По этой причине данные сами по себе приобретают высокую ценность.

Отдельное место занимает информация, несущая в себе данные о личной, индивидуальной или семейной жизни человека. Статья 2 Конституции Российской Федерации закрепляет основной принцип современного демократического общества: «Человек, его права и свободы являются высшей ценностью».

В 2006 г. вышел Федеральный закон «О персональных данных», который является основным документом, регулирующим отношения, связанные с обработкой персональных данных государственными и муниципальными органами власти, юридическими и физическими лицами, с использованием средств автоматизации (а в некоторых случаях и без). Законом установлен срок до 1 января 2010 г. для приведения информационных систем персональных данных (ИСПДн) в соответствие с новым законодательством, а в первую очередь – их подсистем информационной безопасности, так как именно к ним выдвигаются конкретные требования.

Целью работы является создание системы защиты персональных данных в организации, а именно в отделе кадров студентов Томского университета систем управления и радиоэлектроники.

При создании системы защиты персональных данных (ПД) в первую очередь составляется перечень персональных данных, обрабатываемых в организации. В зависимости от этого определяется категория персональных данных.

Вторым этапом является инвентаризация информационных систем. Знать, сколько и какие в системе серверы, какие приложения на них работают, кто имеет к ним доступ и кто, собственно, управляет конкретным ресурсом, необходимо, особенно с точки зрения обеспечения безопасности.

Основная цель анализа угроз информационной безопасности заключается в построении модели злоумышленника. Злоумышленник способен реализовать угрозу в определенном месте и времени, то есть осуществляет атаку на защищаемую информацию. Поэтому следующим шагом создания системы защиты является составление данной модели.

Мероприятия по обеспечению безопасности персональных данных формулируются в зависимости от класса ИСПДн с учетом возможного возникновения угроз безопасности интересам личности, общества и государства.

Классификацию оператор персональных данных осуществляет самостоятельно на основе модели угроз безопасности ПД в соответствии с методическими документами ФСТЭК. Класс ИСПДн оформляется документально соответствующим актом. Модель угроз создается на основании базовой модели, утвержденной ФСТЭК, и по методике этого же ведомства. Из общего (предварительного) перечня угроз на основании методики определения актуальных угроз безопасности ПД определяются те, которые относятся к актуальным для данной ИСПДн.

Для большинства ИСПД необходимо выполнять работы по предотвращению утечки ПД по различным техническим каналам, в том числе создающимся за счет побочных электромагнитных излучений и наводок. Для ИСПДн отдела кадров также необходимо проведение подобных исследований, в связи с чем с помощью специального оборудования были проведены измерения ПЭМИН, результаты измерений повлияли на составление перечня актуальных угроз.

Используя данные о классе ИСПДн и составленный перечень актуальных угроз, на основании рекомендаций и основных мероприятий по обеспечению безопасности ПД, утвержденных ФСТЭК, формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и выбираются программные и технические средства защиты информации, которые могут быть использованы при эксплуатации ИСПДн.

Для обеспечения безопасности ИСПДн используются средства защиты информации, которые имеют сертификат ФСТЭК.

Важным этапом организации защиты персональных данных является создание документов, регламентирующих работу с ПД в организации. Помимо акта о классификации, модели угроз и описания системы защиты, необходима разработка ряда нормативных документов, таких как положение о порядке обработки ПД, предусмотренное главой 14 Трудового кодекса, в котором оговаривается весь процесс получения, хранения, обработки, передачи и защиты ПД, назначаются ответственные за это должностные лица, описывается, кто имеет доступ к ПД, с какими правами и в каких случаях. Также в перечень документов входят заключения о возможности эксплуатации средств защиты персональных данных.

По закону все работники организации должны дать письменное разрешение на работу со своими персональными данными, поэтому целесообразно после введения «Положения…» в действие собрать с работников подписи об их согласии, а в дальнейшем включить разрешающую запись в бланк трудового договора.

После всех вышеописанных действий организация информирует уполномоченный орган по защите прав субъектов ПД (Россвязькомнадзор) об обработке ПД (о наличии ИСПДн, присвоенном ей классе и т.д.) и вводит систему защиты в эксплуатацию (приводит уже имеющуюся систему в соответствие с требованиями). На стадии ввода ИСПДн в действие необходимо оценить ее соответствие требованиям безопасности (провести аттестацию).

ЛИТЕРАТУРА

1. Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ.
2. Трудовой кодекс Российской Федерации от 30.12.2001.

МЕТОД АДДИТИВНОГО СГЛАЖИВАНИЯ В РЕШЕНИИ ЗАДАЧИ ИДЕНТИФИКАЦИИ АВТОРА ТЕКСТА

А.С. Романов, аспирант каф. КИБЭВС
г. Томск, ТУСУР, ras@ms.tusur.ru

Важность задачи идентификации автора печатного текста обуславливается повсеместным переходом от рукописного письма к печатному способу набора. При возникновении ситуации спорного авторства или при криминалистическом исследовании печатного текста развитые методы идентификации по почерку могут оказаться бесполезными. Кроме того, почерковедческая экспертиза позволяет опреде-

лить лишь исполнителя, но не автора текста. Проведение авторoведческой экспертизы в настоящее время осуществляется с привлечением экспертов, имеющих соответствующее образование в области лингвистики, филологии и т.д. Эффективных же количественных методов и инструментов автоматического определения авторства текстов для русского языка на данный момент не разработано.

Текст можно рассматривать как иерархическую структуру [1] и анализировать на любом уровне как последовательность отдельных составляющих его элементов (символов, словоформ, грамматических классов и т.д.) или групп элементов длиной N – N-грамм.

Однако при использовании частот появления в тексте N-грамм как признаков для идентификации исследователь сталкивается с проблемой «разреженных данных» (sparse data), когда в обучающем или исследуемом корпусе, в силу ограничения определенной длиной, отсутствует часть признаков. Особенно проблема актуальна для текстов небольших объемов и N-грамм высоких порядков. Решением является использование специальных техник сглаживания вероятностей (метод Лапласа, Гуда-Тьюринга, Катца, Кнезера-Нейя и др. [3]), которые по исходному распределению позволяют оценить вероятности ненаступивших событий.

Самым простым видом сглаживания является аддитивный метод, при котором к каждому элементу матрицы, содержащему количество подсчетов определенной N-граммы, перед переводом в вероятности добавляется некоторая величина δ, т.е. вместо формулы для расчета вероятностей N-грамм

$$P(w_{i-n+1}^{i-1}) = \frac{c(w_{i-n+1}^{i})}{\sum_{w_i} c(w_{i-n+1}^{i})}$$

используется выражение

$$P_{ADD}(w_{i-n+1}^{i-1}) = \frac{\delta + c(w_{i-n+1}^{i})}{\delta V + \sum_{w_i} c(w_{i-n+1}^{i})},$$

где $c(\cdot)$ – количество употреблений данной N-граммы; V – количество всех N-грамм в используемом словаре или алфавите.

Рассмотрим случай, когда $\delta = 1$ (метод сглаживания Лапласа), и последовательность элементов текста на самом низком уровне иерархии – уровне символов. Проведем исследования по идентификации автора в случае двух предполагаемых авторов (бинарная классификация) на корпусе, составленном из 47 текстов 11 русских писателей, взятых из Интернет-ресурса [3]. При этом будем использовать выбор-

ки объемом 1000–100000 символов, количество обучающих примеров для каждого автора будем брать равным 3, для тестирования использовать по 1 выборке автора. В качестве признаков для идентификации возьмем частоты встречаемости в тексте биграмм и триграмм символов и их сглаженные методом Лапласа эквиваленты.

В качестве инструмента для принятия решений воспользуемся реализацией метода опорных векторов (Support Vector Machine, SVM) [4].

Параметры обучения моделей SVM выбраны следующие:

1) ядро на основе радиальных базисных функций;
2) значение параметра гамма $\gamma = 0{,}5$;
3) значение параметра регуляризации $C = 1$.

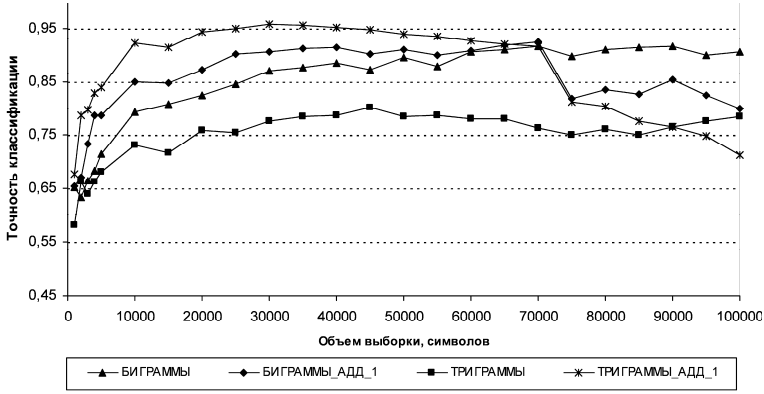


Рис. 1. Результаты исследований по биграммам и триграммам символов

Как видно из графиков (рис. 1), наиболее точной оказывается классификация с использованием в качестве признаков сглаженных методом Лапласа частот триграмм символов. Особенно четко ее преимущества проявляются на малых объемах выборки: так, уже при размере выборки 5000 символов точность классификации составляет 0,83, при 10000 символов – 0,92, максимум точности достигается при размере выборки 25000–30000 символов – 0,95.

Классификация с использованием сглаженных частот биграмм имеет меньшую точность (максимум 0,92 при объеме 65000), но также показывает лучшие результаты, чем классификация на основе несглаженных частот биграмм.

Положительные результаты по использованию аддитивного метода позволяют сделать вывод о перспективности исследования более сложных методов сглаживания.

Работа поддержана грантом ФСРМПНТ.

ЛИТЕРАТУРА

1. Романов А.С. Модель базы данных для хранения текстов и их характеристик // Доклады Томского государственного университета систем управления и радиоэлектроники. 2008. № 1(17). С. 70–73.

2. Chen S.F., Goodman J. An empirical study of smoothing techniques for language modeling // Computer Speech & Language. 1999. Vol. 13. № 4. October. P. 359–393.

3. Библиотека Максима Мошкова. Режим доступа – http://www.lib.ru, свободный.

4. Hsu C.-W., Chang C.-C., Lin C.-J. A practical guide to support vector classification. Режим доступа – http://www.csie.ntu.edu.tw/~cjlin/papers/guide/guide.pdf, свободный.

КЛАССИФИКАТОР НА ОСНОВЕ МАШИНЫ ОПОРНЫХ ВЕКТОРОВ

А.С. Романов, аспирант каф. КИБЭВС

г. Томск, ТУСУР, ras@ms.tusur.ru

Математический аппарат классификатора на основе метода «машины опорных векторов» (Support Vector Machine, SVM) был предложен В.Н. Вапником в работах [1, 2].

Пусть имеется помеченное тренировочное множество примеров $D = \{(x_i, y_i)\}_{i=1}^{\ell}$, $x_i \in X \subset R^d$, метки могут принимать значения $y_i \in Y = \{-1,+1\}$. SVM строит линейный классификатор в пространстве признаков с высокой размерностью таким образом, чтобы зазор между граничными точками двух классов, называемых опорными векторами, был максимальным. Для отображения исходных данных в пространство, в котором разделяющая их поверхность будет линейной, используются ядровые преобразования – некоторая функция

$$(\Phi(x), \Phi(x')) = k(x, x').$$

Классифицирующая функция, реализуемая SVM, записывается следующим образом:

$$f(x) = \left\{ \sum_{i=1}^{\ell} \alpha_i y_i k(x_i, x) \right\} + b.$$

Чтобы найти оптимальный коэффициент α, достаточно максимизировать функционал

$$W(\alpha) = \sum_{i=1}^{\ell} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{\ell} y_i y_j \alpha_i \alpha_j k(x_i, x_j)$$

в положительном квадранте $0 \le \alpha_i \le C$, $i = \overline{1, \ell}$. Условие максимизации:

$$\sum_{i=1}^{\ell} \alpha_i y_i = 0.$$

Параметр регуляризации C отвечает за соотношение между величиной зазора и количеством ошибок обучающего множества.

Необходимыми условиями решения задачи нелинейного программирования являются условия Каруша–Куна–Такера:

$$\alpha_i = 0 \Rightarrow y_i f(x_i) \ge 1,$$
$$0 < \alpha_i < C \Rightarrow y_i f(x_i) = 1,$$
$$\alpha_i = C \Rightarrow y_i f(x_i) \le 1.$$

Эти условия удовлетворяют множеству допустимых множителей Лагранжа $\alpha^0 = \{\alpha_1^0, \alpha_2^0, ..., \alpha_\ell^0\}$, максимизирующих целевую функцию $W(\alpha)$. Параметр смещения b выбирается, чтобы обеспечить выполнение второго условия Каруша–Куна–Такера для всех входных образцов, соответствующих множителям Лагранжа, лежащим не на границах. В общем случае только часть множителей Лагранжа α будет иметь ненулевые значения, которые и составляют опорные векторы.

Пусть I – множество индексов образцов, относящихся к множителям Лагранжа, лежащим внутри границ:

$$I = \{i : 0 < \alpha_i^0 < C\},$$

а J – множество индексов со значениями множителей Лагранжа, лежащих на верхней границе C:

$$J = \{i : \alpha_i^0 = C\},$$

тогда $f(x)$ можно переписать следующим образом:

$$f(x) = \left\{ \sum_{i \in \{I, J\}} \alpha_i^0 y_i k(x_i, x) \right\} + b .$$

Классический метод опорных векторов предназначен для решения задачи бинарной классификации. Проблему с большим количеством классов можно свести к решению нескольких бинарных задач. Для этого существуют следующие основные стратегии выбора решения [3]:

1. «Один против всех» (one-against-all). Для решения задачи строится n классификаторов таким образом, что каждый класс a_j сопоставляется с остальными $(n - 1)$ классами, т.е. в каждом из j случаев выбор осуществляется из двух вариантов: «класс a_j» и «не класс a_j». Итоговое решение по всем классам принимается по схеме «победитель забирает все» (winner takes all).

2. «Каждый против каждого» (one-against-one). Классификаторы строятся для каждой пары классов для того, чтобы можно было однозначно разделить любые два класса. Количество классификаторов в этом случае равно $n(n-1)/2$. После подачи на входы каждого из обученных классификаторов тестового образца получаем ответы, содержащие информацию о его принадлежности одному из двух классов, участвовавших в обучении. К полученному множеству ответов применяется схема мажоритарного голосования и класс, выбранный большинством классификаторов, принимается как итоговое решение.

3. Ориентированный ациклический граф (DNA). На этапе обучения работает также как стратегия «каждый против каждого». На этапе тестирования и непосредственной классификации используется корневой бинарный ориентированный ациклический граф (ориентированное дерево) с $n(n-1)/2$ внутренними узлами – обученными бинарными классификаторами и n листьями. Классифицируемый объект проходит путь от корня до одного из листьев, при этом в зависимости от результатов классификации в каждом узле один из классов отвергается и дальнейшие действия продолжаются по ветке, соответствующей второму классу. После выполнения $(n-1)$ подобных операций алгоритм достигает листа, который принимается как итоговое решение классификатора.

В отличие от искусственных нейронных сетей, применявшихся автором ранее [4], SVM лучше подходит для работы с большим признаковым пространством, что важно при использовании N-грамм элементов текста как признаков для идентификации автора. Нет необходимости в выборе количества скрытых элементов, скорость работы SVM существенно выше, чем у нейронных сетей.

Программная реализация метода SVM и стратегия «каждый против каждого» интегрированы в общую программную оболочку, структура которой описана в работе [5].

Работа поддержана грантом ФСРМПНТ.

ЛИТЕРАТУРА

1. Vapnik V.N. Statistical Learning Theory. N.Y.: Wiley, 1998. 732 p.

2. Vapnik V.N. The nature of statistical learning theory. N.Y.: Springer-Verlag, 2000. 332 p.

3. Hsu C.-W., Lin C.-J. A comparison of methods for multi-class support vector machines // IEEE Transactions on Neural Networks. 2003. № 13(2). P. 415–425.

4. Романов А.С. Подходы к идентификации авторства текста на основе n-грамм и нейронных сетей // Молодежь и современные информационные технологии: Сборник трудов VI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Томск, 26–28 февраля 2008 г. Томск: Изд-во ТПУ, 2008. С. 145–146.

5. Романов А.С. Структура программного комплекса для исследования подходов к идентификации авторства текстов // Доклады Томского государственного университета систем управления и радиоэлектроники. 2008. № 2 (18). Ч. 1. С. 106–109.

ПРОБЛЕМАТИКА РАСПОЗНАВАНИЯ ГЛАСНЫХ И СОГЛАСНЫХ ЗВУКОВ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

Е.Ф. Щипунов, студент 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, clswr@sibmail.com

Для решения задачи анализа и синтеза речи необходимо иметь соответствующие инструменты, позволяющие выделять из человеческой речи требуемые звуки. В данной работе в качестве такого инструмента, используются нейронные сети прямого распространения.

Ранее были рассмотрены подходы, предполагающие создание нейронных сетей для распознавания гласных, согласных и отдельных типов слогов. Но, как показала практика, такой подход неэффективен. Нейронные сети, обученные только на гласных или только согласных звуках, уже не могли с требуемой степенью точности определить тот же самый звук, если он находился в сочетании с другим. Поэтому данный подход не получил дальнейшего развития.

Как известно, человек никогда не произносит звуки одинаково. Даже один и тот же звук каждый раз произносится по-разному. Однако, несмотря на разницу в произношении, каждый раз произнесенный звук будет являться реализацией конкретной фонемы, которая, по сути, не изменяется [1]. Именно этот факт не позволяет получать обученные нейронные сети, способные различать конкретные типы слогов – слишком велико многообразие типов и сочетаний.

Возникает необходимость поиска новых подходов для решения поставленной задачи. Очевидно, что для решения задачи с различием звуков, слогов или даже слов необходимо иметь элементарные составляющие, из которых можно будет сложить общее решение. Такими составляющими являются нейронные сети, различающие конкретные типы звуков. В качестве примеров типов звуков можно привести следующие: вокализованные звуки, смычные взрывные звуки, аффрикаты, щелевые звуки и др.

Для создания нейронной сети, способной различать гласные и согласные звуки, была использована обучающая выборка, состоящая из 5 сигналов одного диктора. В качестве тестовой выборки использовались сигналы того же диктора, включая и те сигналы (в большинстве своем), которые нейронная сеть не встречала в обучающей выборке.

Однако, помимо наличия требуемой выборки звуков, необходимо правильно подобрать параметры самой сети. Такими параметрами являются входные значения, размер промежуточного слоя, а также активационные функции и алгоритм обучения.

В ходе подбора параметров было установлено, что размер промежуточного слоя сети напрямую влияет на качество обучения. Причем чем меньше размер промежуточного слоя, тем менее эффективно нейронная сеть реагировала на гласные звуки и наоборот.

В качестве активационной функции для каждого из слоев нейронной сети были выбраны функции гиперболического тангенса. Данная функция выбрана как наиболее часто используемая биологами в качестве математической модели активации биологической клетки [2].

В процессе исследований были получены 4 нейронных сети, способные с большей или меньшей степенью точности распознавать звуки. Однако был выбран наиболее удачный вариант сети, ошибка которой при обучении приближается к величине 10^{-8}. Данная сеть была использована в дальнейшем при наборе статистических данных на различных сигналах одного диктора. В результате из 443 согласных и гласных звуков нейронная сеть правильно определила 319 звуков и ошиблась 125 раз. Из них ошибки первого рода составили 43, ошибки второго рода – 82. В процентном соотношении нейронная сеть ошиблась в 28,2% случаев. Наибольшее число ошибок было совершено при определении гласного звука «а». Это связано с тем, что чаще всего, при произношении, этот звук «проглатывается» или же полностью сливается с последующим звуком. Ниже представлена таблица распределения ошибок нейронной сети по распознаваемым звукам. В крайнем левом столбце таблицы обозначены номера фраз из тестовой выборки. Ячейки таблицы содержат число ошибок нейронной сети, допущенных при распознавании данного звука. Например, в десятом сигнале при распознавании звука «а» в разных частях тестовой фразы было допущено 4 ошибки. Если же ошибок не было, ячейка остается пустой.

Аналогичная ситуация наблюдается и при определении звука «л», как мягкого, так и твердого. Чаще всего, если данный звук стоит в паре с гласным звуком, происходит озвончение согласного звука и нейронная сеть определяет его как гласный звук. Причем когда звук «л» находится перед гласным, в 59% случаев оба определяются как гласный звук. В обратной ситуации – в 75% случаев. Та же ситуация наблюдается не только со звуком «л». Другие звуки, например, «м», «р», «в», в сочетании с гласными звуками, оказываются в поле зрения нейронной сети лишь как единый гласный звук. Шумы, присутствующие в некоторых сигналах тестовой выборки, также увеличивают величину ошибки нейронной сети и затрудняют ее обучение.

Фрагмент таблицы, содержащий ошибки нейронной сети при распознавании звуков тестовых фраз

№	а	б	в	в'	г	г'	д	д'	ж	з	з'	и	к	к'	л	л'	м	м'
1				1														
2							1							1				
3	2											1	1					
4	1											1			1			
5	2												1		1			
6	2		1							1		1			2		1	
7	1		1					1							1			
8			1									1			1			
9	1		1												1			
10	4						1								1	1		
11			1															1
12	1				1		1							1		1		
13																		
14																		
15	1															1		1
16															2			
17	1											1	1	1	1		1	
18	1																	
19	1				1							1				1	1	
20										1					2	1		
21	1		1									1			1			
22	2	1			1		1								1			
23	3	1			1										1			

Конечно, имея одну нейронную сеть, нельзя говорить о наличии готового решения задачи анализа речи. Но, прилагая несколько нейронных сетей с требуемыми показателями качества, разложив тем самым задачу на простые составляющие, можно говорить о первых приближениях к решению данного вопроса.

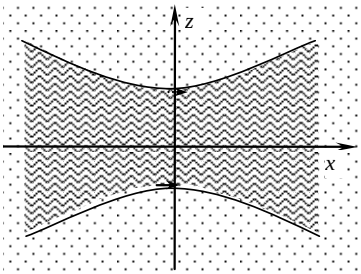


Рис. 1. Одномерный световой пучок в наноколлоидной системе

ЛИТЕРАТУРА

1. Бондарко Л.В. Звуковой строй современного русского языка. М.: Просвещение, 1997.

2. Уоссермен Ф. Нейрокомпьютерная техника: теория и практика: пер. на русский яз. Ю.А. Зуев, В.А. Точенов. М., 1992.

ОДНОМЕРНЫЕ СВЕТЛЫЕ СОЛИТОНЫ В НАНОКОЛЛОИДНЫХ СИСТЕМАХ

А.Р. Селютин, Ж.Е. Каппасов, С.А. Михнов, Л.В. Загребин, Р.В. Литвинов, канд. ф.-м.н., доцент

г. Томск, ТУСУР, т. +7-961-887-13-25, zhanik@sibmail.com

Интенсивное развитие нанотехнологий привело к созданию новых сред, обладающих нелинейным откликом на воздействие различных физических полей [1]. Нелинейный оптический отклик сред с наноразмерными включениями может быть использован для формирования динамических голограмм и оптических солитонов, обращения волнового фронта, наблюдения разнообразных коллективных явлений и др. [2–4]. Оптические солитоны в различных средах используются для создания высокоскоростных линий связи, формирования индуцированных светом оптических волноводов и в других современных приложениях нелинейной оптики [5]. В данной статье представлены результаты теоретического анализа формирования светлых пространственных оптических солитонов в коллоидных системах на основе жидкой дисперсионной среды с непоглощающими свет наночастицами в качестве дисперсной фазы.

Рассмотрим распространение монохроматического, частотой ω, одномерного светового пучка в наноколлоидной системе (рис. 1). В общем случае форма поперечной огибающей пучка изменяется вдоль направления его распространения. Огибающая солитонного пучка не изменяется при его распространении в оптически нелинейной среде [3, 5, 6]. Вектор электрической напряженности светового поля такого солитонного пучка может быть представлен в форме

$$\tilde{\mathbf{E}} = R(z)\mathbf{e}\exp\left[i(\omega t - \beta x)\right], \qquad (1)$$

где $R(z)$ и $\mathbf{e}$ – огибающая и нормированный вектор поляризации солитона соответственно; β – постоянная распространения солитона; k – волновое число в вакууме [5]. В рамках приближения Максвелла–Гарнетта показатель преломления коллоидной среды n с небольшой величиной фактора заполнения $f = NV_p << 1$ описывается следующим выражением:

$$n = \sqrt{n_b^2 + \frac{N\alpha}{\varepsilon_0}} \approx n_b + \frac{N\alpha}{2\varepsilon_0 n_b}, \qquad (2)$$

где $\alpha = 3V_p\varepsilon_0 n_b^2\left(n_p^2 - n_b^2\right)\Big/\left(n_p^2 + 2n_b^2\right)$; n_b и n_p – показатели преломления дисперсионной среды и наночастиц соответственно; N и V_p – концентрация и объем частиц, соответственно.

В работах [3, 6] показано, что концентрация наночастиц следующим образом зависит от интенсивности светового пучка $I = \mathbf{E}\cdot\mathbf{E}^*$:

$$N = N_0 \exp\left(\frac{\alpha}{4k_BT}\mathbf{E}\cdot\mathbf{E}^*\right) \approx N_0\left(1 + \frac{\alpha}{4k_BT}\mathbf{E}\cdot\mathbf{E}^*\right), \qquad (3)$$

где k_b – постоянная Больцмана; T – температура. Таким образом, диэлектрическая проницаемость наноколлоидной системы оказывается зависящей от интенсивности светового поля, что является типичным проявлением оптической нелинейности среды [7]. Стандартная процедура поиска односолитонного решения нелинейного волнового уравнения [5] приводит к следующем соотношениям для постоянной β и огибающей светлого солитона:

$$\beta = \left(n_b + \frac{3N_0\alpha^2 R^2_{\max}}{16 n_b k_b T}\right)k\,,\ R(z) = R_{\max}\,\mathrm{sech}(\gamma z), \qquad (4)$$

где $\gamma = R_{\max}\alpha k\sqrt{3N_0/8k_bT}$. Полученные соотношения (4) могут быть использованы для анализа солитонных пучков в наноколлоидных системах.

На рис. 1 показана огибающая светлого солитона, распространяющегося в коллоиде на основе воды (n_b = 1,33) с наночастицами SiO_2 (n_p = 1,553). Кривые *1*, *2*, *3* на этом рисунке отвечают исходной концентрации наночастиц $N_0 = 10^{20}$; 10^{19}; 10^{18} м$^{-3}$ соответственно. Из рисунка следует, что ширина пространственного оптического солитона уменьшается с увеличением N_0. Этот эффект обусловлен тем, что нелинейные возмущения показателя преломления наноколлоидной системы фиксированным световым пучком уве-

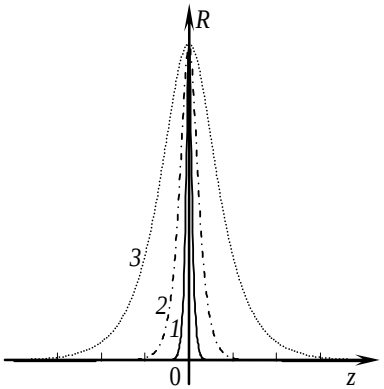


Рис. 1. Огибающая светлого солитона при различных концентрациях наночастиц: *1* – $N = 10^{20}$ м$^{-3}$; *2* –10^{19} м$^{-3}$; *3* – 10^{18} м$^{-3}$

личиваются с ростом концентрации N_0, что приводит к росту влияния нелинейной рефракции. Формирование пространственного оптического солитона становится возможным при взаимной компенсации нелинейной рефракции и дифракционного расплывания светового пучка [5, 7]. Поэтому в солитонном режиме увеличение вклада нелинейной рефракции за счет роста N_0 должно сопровождаться соответствующим увеличением вклада дифракционного расплывания, которое растет при уменьшении ширины пучка. Поэтому при фиксированной амплитуде светового поля R_{max} ширина огибающей пространственных оптических солитонов в наноколлоидных системах уменьшается с увеличением величины исходной концентрации наночастиц N_0.

Работа выполнена при частичной финансовой поддержке РФФИ (грант № 09-02-99024 р_офи).

ЛИТЕРАТУРА

1. Суздалев И.П. Физикохимия нанокластеров, наноструктур, наноматериалов. М.: КомКнига, 2006. 592 с.
2. Михнов С.А., Конкин Д.А., Агеев Е.Ю., Литвинов Р.В. // Изв. Вузов. Физика. 2008. № 9/3. С. 167–168.
3. Matuszewski M., Krolikowski W., Kivshar Y.S. // Optics express. 2008. Vol. 16. P. 1371.
4. Кульчин Ю.Н., Щербаков А.В., Дзюба В.П., Вознесенский С.С., Микаелян Г.Т. // Квантовая электроника. 2008. № 38. С. 154.
5. Кивширь Ю.С., Агравал Г.П. Оптические солитоны / Пер. с англ.; под ред. Н.Н. Розанова. М.:Физматлит, 2005. 648 с.
6. El-Gauaiuy R., Christodoulides D.N., Rotschild C., Segev M. // Optics express. 2007. Vol. 15. № 16. P. 10207–10218.
7. Шен И.Р. Принципы нелинейной оптики. М.: Наука, 1989. 558 с.

ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ АКУСТИЧЕСКОЙ (РЕЧЕВОЙ) ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

К.А. Швейдюк, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, velit@sibmail.com

Защита акустической информации достигается проведением организационных и технических мероприятий, а также выявлением электронных устройств перехвата информации.

Использование тех или иных методов и средств определяется характеристиками объекта защиты и аппаратуры разведки, условиями ее ведения, а также требованиями, предъявляемыми к эффективности защиты акустической информации, в качестве показателя оценки которой наиболее часто используют словесную разборчивость *W*. Для

оценки разборчивости речи используется инструментально-расчетный метод, при котором числовое значение словесной разборчивости рассчитывается на основе измерения отношения уровней речевого сигнала и шума в местах предполагаемого расположения датчиков аппаратуры акустической разведки. Выбор мест размещения элементов аппаратуры контроля зависит от типа аппаратуры речевой разведки, в отношении которой осуществляется защита речевой информации.

При контроле защищенности речевой информации от виброакустической аппаратуры речевой разведки контрольными точками установки измерительного виброакустического датчика являются внешние по отношению к источнику речевого сигнала поверхности различных ограждающих конструкций, инженерных коммуникаций и других предметов, которые находятся на разведопасных направлениях, а также возможные места на инженерных коммуникациях (строительных конструкциях и т.п.), доступных посторонним лицам.

Для контроля выполнения норм защищенности речевой информации от оптико-электронной аппаратуры речевой разведки используется также контактный виброакустический датчик, который крепится с помощью специальной пасты или клея на внешних поверхностях стекол окон или других отражающих пластин, колеблющихся под действием речевых акустических сигналов, и нормаль к их поверхности совпадает с разведопасным направлением.

После проведения измерений для каждой точки контроля рассчитывается словесная разборчивость речи W. Если в результате расчетов окажется, что $W > W_{\text{п}}$ (где $W_{\text{п}}$ – нормативное (пороговое) значение) производится настройка соответствующего канала системы (или увеличение уровня сигнала в соответствующем канале, или в соответствующей октавной полосе). При $W < W_{\text{п}}$ фиксируются установленные уровни сигнала в соответствующих каналах и спектральных полосах и система может приниматься в эксплуатацию.

Для оценки разборчивости речи целесообразно использовать инструментально-расчетный метод, при котором числовое значение словесной разборчивости рассчитывается на основе измерения отношения уровней речевого сигнала и шума в местах предполагаемого расположения датчиков аппаратуры акустической разведки [1]:

$$W = \begin{cases} 1{,}57 \cdot R^{0{,}25} \cdot \left[1 - \exp(-11 \cdot R)\right], & \text{если } R \le 0{,}15, \\ 1 - \exp\left(-\dfrac{11 \cdot R}{1 + 0{,}7 \cdot R}\right), & \text{если } R \ge 0{,}15, \end{cases}$$

где R – интегральный индекс артикуляции речи, рассчитываемый по формуле

$$R=\sum_{i=1}^{N}(p_i\cdot K_i),$$

где K_i – значение весового коэффициента в i-й октавной полосе;

$$p_i=\begin{cases}\dfrac{0{,}78+5{,}46\cdot\exp\left[-4{,}3\cdot10^{-3}\cdot\left(27{,}3-|Q_i|^2\right)\right]}{1+10^{0{,}1|Q_i|}}, & \text{если } Q_i\le 0,\\ 1-\dfrac{0{,}78+5{,}46\cdot\exp\left[-4{,}3\cdot10^{-3}\cdot\left(27{,}3-|Q_i|^2\right)\right]}{1+10^{0{,}1|Q_i|}}, & \text{если } Q_i>0,\end{cases}$$

$$Q_i=q_i-\Delta A_i,$$

где q_i – отношение «уровень речевого сигнала/уровень шума» в месте измерения в i-й октавной полосе, дБ, и рассчитывается по формуле

$$q_i=L_{\text{сi}}-L_{\text{ш}i},$$

где $L_{\text{сi}}$ – средний спектральный уровень речевого сигнала в месте измерения в i-й октавной полосе, дБ; $L_{\text{ш}i}$ – уровень шума (помехи) в месте измерения в i-й октавной полосе, дБ; ΔA_i – значение формантного параметра спектра речевого сигнала в i-й октавной полосе, дБ; N – количество октавных полос, в которых проводится измерение.

Восприятия речи в шуме сопровождается потерями составных элементов речевого сообщения. Понятность речевого сообщения характеризуется количеством правильно принятых слов, отражающих качественную область понятности, которая выражена в категориях подробности справки о перехваченном разговоре, составляемой «агентом».

Можно выделить шкалу оценок качества перехваченного речевого сообщения:

1. Перехваченное речевое сообщение содержит количество правильно понятых слов, достаточное для составления подробной справки о содержании перехваченного разговора.

2. Перехваченное речевое сообщение содержит количество правильно понятых слов, достаточное только для составления краткой справки-аннотации, отражающей предмет, проблему, цель и общий смысл перехваченного разговора.

3. Перехваченное речевое сообщение содержит отдельные правильно понятые слова, позволяющие установить предмет разговора.

4. При прослушивании фонограммы перехваченного речевого сообщения возможно установить факт наличия речи, но нельзя установить предмет разговора

Из формулы расчета словесной разборчивости следует, что для снижения разборчивости речи необходимо стремиться уменьшить отношение сигнал/шум в местах возможного размещения датчиков аппаратуры акустической разведки. Уменьшение отношения сигнал/шум возможно путем или уменьшения уровня речевого сигнала, или увеличения уровня шума, т.е. создания акустических и вибрационных помех.

ЛИТЕРАТУРА

1. Железняк В.К., Макаров Ю.К., Хореев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. 2000. № 4.

2. Тяпкин В.Н., Золотарев В.В. Технические средства и методы защиты информации: учеб.-метод. Издание / Сиб. гос. аэрокосмич. ун-т. Красноярск, 2007.

3. Хореев А.А. Защита информации от утечки по техническим каналам. Ч. 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998. 320 с.

ЭЛЕКТРОННЫЕ КЛЮЧИ eToken и ruToken

Е.А. Смаль, А.В. Лысова, студенты 5-го курса, каф. КИБЭВС,
Ю.М. Филимонов, науч. рук,. доцент каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-409-06-63, lysovaa@sibmail.com

Назначение электронного ключа состоит в аутентификации пользователя при доступе к защищенным ресурсам и безопасном хранении паролей для входа в систему, ключей шифрования, цифровых сертификатов, а также любой другой секретной информации.

Электронные ключи безопасности предоставляют высокую степень надежности вследствие используемого двухфакторного механизма аутентификации: пользователь знает персональный идентификационный номер (PIN), с помощью которого система опознает определенного владельца ключа; в свою очередь электронный ключ, получая сигнал от системы, высвечивает на своем дисплее число, ввод которого и позволяет провести авторизацию.

Использование электронного ключа при входе в сеть позволяет существенно повысить уровень защищенности и удобства работы с системой. Пользователям не нужно запоминать сложные пароли, достаточно подключить электронный ключ к USB порту и ввести PIN-код.

Интеллектуальные USB-ключи или токены предназначены для работы в составе программных приложений, где требуется сохранить конфиденциальные или персональные данные в отдельном устройстве. Токен подключается к USB-порту компьютера непосредственно или

с помощью соединительного кабеля. Токены, используемые в качестве средства доступа, являются небольшим физическим средством, при помощи которого человек, обладающий токеном, осуществляет доступ к определенным сетевым ресурсам [1].

Некоторые возможности и свойства eToken*:*

1) надежность и безопасность;

2) закрытые ключи, сгенерированные eToken или импортированные в него, хранятся в закрытой памяти микросхемы смарт-карты и не могут быть из нее извлечены;

3) в eToken PRO и NG-OTP предусмотрена возможность шифрования трафика, передаваемого по шине USB, с использованием механизма Secure Messaging по алгоритму 3DES (CBC);

4) в eToken RTE реализован контроль длины и качества задаваемого пользователем PIN-кода и запрет использования «слабых» комбинаций;

5) при форматировании eToken имеется возможность задания максимально допустимого количества введенных подряд неправильных значений PIN-кодов пользователя и/или паролей администратора, при достижении которого блокируется доступ к eToken на уровне пользователя / администратора (защита от атаки методом перебора). eToken может быть разблокирован с использованием пароля администратора: без потери пользовательских данных (смена PIN-кода); с потерей пользовательских данных (форматирование);

6) с помощью системы централизованного управления eToken TMS операция смены PIN-кода может быть произведена удаленно;

7) eToken корректно работает и обеспечивает возможность выписки и хранения нескольких сертификатов в свою защищенную память для Microsoft CA (Windows 2000, 2003 Server), КриптоПро УЦ, RSA Keon, VeriSign, Thawte, Entrust, Globalsing, GTE CyberTrust и имеет соответствующие сертификаты совместимости от производителей;

8) скорость генерации ключевой пары RSA 1024 бит < 10 с;

9) формирование ЭЦП с использованием RSA 1024 бит < 1 с [2].

Свойства ruToken:

1) в зависимости от версии накопитель содержит от 8 до 128 Кбайт энергонезависимой памяти и поддерживает до 1 млн. циклов записи. Память организована в виде файловой системы, которая позволяет создавать объекты нескольких типов и присваивать им права доступа, при этом прямой доступ к блокам памяти полностью запрещен;

2) для разграничения прав доступа используются PIN-коды. Всего возможны три уровня доступа: гостя, пользователя и администратора;

3) также поддерживается алгоритм шифрования по ГОСТ 28147–89 в режимах простой замены, гаммирования и гаммирования с обратной

связью; ключи для шифрования могут создаваться и храниться без возможности экспорта из токена;

4) реализована поддержка следующих интерфейсов взаимодействия: PC/SC, PKSC #11, Microsoft Cripto API, а также собственная библиотека функций, облегчающая интеграцию решений на основе ruToken в имеющиеся программы;

5) скорость шифрования симметричным ГОСТом составляет 1 кБ ~ 1,4 с;

6) ruToken служит для строгой двухфакторной аутентификации, защиты электронной переписки, установления защищенных соединений (VPN, SSL), проведения финансовых транзакций и криптографической защиты информации [3, 4].

В первую очередь проверили работоспособность основных функций, таких как создание/удаление файлов и каталогов и запись/считывание данных. Все операции проходят успешно, причем скорость создания и удаления файлов напрямую зависит от их объема. При непрерывном повторе попытки чтения из защищенного файла и внесении небольших помех проверялось, чтобы при передаче данных из памяти один или несколько битов в пакете менялись. В процессе чтения запрещающие атрибуты удается подменить разрешающими и получить доступ к содержимому защищенного файла. Если при инициализации ruToken происходит остановка или сбой в системе, то ruToken блокируется, после чего восстановить его работоспособность может только производитель. Реализованное в токене аппаратное шифрование позволяет минимизировать вероятность несанкционированного доступа к данным. Собственная библиотека функций и поддержка API заметно облегчают использование токена с различными приложениями. В общем, итоговая оценка ruToken довольно высока, хотя есть и небольшие недостатки [4].

Целью нашей работы является анализ продуктов rutoken и etoken, разработка консольных приложений, для использования в качестве учебной программы для студентов, которая полностью заменяет программное обеспечение, поставляемое с данными продуктами.

ЛИТЕРАТУРА

1. http://www.nihol.com/ru//index.php?option=com_content&task=view&id=140&Itemid=154

2. http://www.aladdin.ru/

3. http://www.ancud.ru/catalog/rutoken.html

4. http://www.rutoken.ru/news/publications/10082004.html

ТЕСТОВЫЙ СЕРВЕР ДЛЯ ВЗЛОМА

П.П. Свешников, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-411-15-80, writeme@sibmail.com

В последние несколько лет растет интерес к технологии изучения поведения хакеров. В представленном тестовом сервере для взлома подход к изучению поведения и мотивации взломщиков основан на игровом подходе. «Игрой называют такой вид человеческой деятельности, который отражает (воссоздает) другие ее виды» [1].

Тестовый сервер для взлома – это средство безопасности, значение которого состоит в подверженности его сканированиям, атакам и взломам. Ключевым моментом является то, что сервер не ограничивается решением только одной проблемы, а имеет несколько различных областей применения. Чтобы лучше понять ценность серверов, можно подразделить их на две различные категории: производственные и исследовательские. Производственные серверы используются для защиты сети, они напрямую помогают обеспечить безопасность организации. Исследовательский «сервер» используется для сбора информации. Эта информация затем может быть использована для различных целей, таких как: раннее предупреждение и предсказание, накопление информации и обеспечение правопорядка.

Назначение и область применения. Ни одно из решений не превосходит другое, все зависит от того, что необходимо достичь. В данной работе сконцентрируем внимание на исследовательских методах.

Тестовый сервер для взлома (далее – система) предназначен для постановки экспериментов по взлому автоматизированной системы. Для этого были созданы блог и новостная страница (находятся по адресу: http://ctf.keva.tusur.ru/).

Для информационного обеспечения, размещения статей, «системы», для обсуждения текущей ситуации использовалась кафедральная конференция (http://keva.tusur.ru/forum/).

Отметим, что система использовалась в учебных целях.

Рассмотрим подробнее работу и функции системы.

Функции:

– предоставление стандартных служб обслуживания в сети (хостинг, почта, фтп и т.д.);

– анализ защищенности системы, используя специальное программное обеспечение, анализ атак доступа и др., делаются выводы о защищенности системы;

– обработка найденных уязвимостей, в случае если в системе найдена уязвимость, даются рекомендации по ее устранению.

Постановка и проведение эксперимента

Так как основной упор делается на исследовательском использовании системы, рассмотрим, как проводятся эксперименты. Физически

на системе расположены как основная ОС (FreBSD 7.1) с информационной страничкой и сервисами, предоставляемыми для участников (тестеров), так и виртуальная машина, которая и выступает в качестве сервера для взлома, каждый раз администратор планирует, какая система будет использоваться на виртуальной машине, будь то FreeBSD, Linux, Windows или другая система. На ней размещаются уязвимые сервисы, также допускаются ошибки в администрировании (нестойкие пароли и т.п.).

В роли атакующих выступают тестеры, которые выполняют взлом «системы».

Хочется отметить, что окончательной целью проведения эксперимента является обоснованная на результатах эксперимента защита от той или иной атаки. В то же время необходимо понимать, что дать рецепт окончательной информационной безопасности невозможно, так как «информационная безопасность – это процесс».

Статистические данные. Представим проанализированные результаты эксперимента в виде списка кратких тезисов:

– хост обнаруживается злоумышленниками в течение 5–6 мин после включения;

– в течение трех часов все хосты и все сетевые сервисы были атакованы;

– средняя длительность атаки – несколько секунд;

– плотность атак не зависела от времени суток;

– иногда перед нападением проводилось сканирование всех сервисов хоста, а иногда атака была направлена только на какой-то один произвольный сервис;

– между сканированием и атакой могло пройти несколько дней, но обычно атака следовала сразу же;

– большинство взломщиков интересовал только определенный тип сетевого сервиса;

– самыми привлекательными для взломщиков оказались сетевые ресурсы Windows-систем (DCOM RPC, netbios-ssn и т.п.) – 64% атак; следующие по значимости цели – почтовые и веб-серверы – 23 и 9% соответственно;

– значительная часть атак была проведена с Windows-хостов – 57%. Следующие по распространенности среди атакующих операционные системы FreeBSD – 26% и Linux – 12%.

ЛИТЕРАТУРА

1. Комаров В.Ф. Управленческие имитационные игры. Новосибирск: Наука, Сибирское отделение, 1989. 256 с.

2. Мейволд Э. Безопасность сетей. М.: ЭКОМ, 2006. 528 с.

3. Фленов М.Е. Linux глазами хакера. СПб.: БХВ-Петербург, 2008. 543 с.

БЕЗОПАСНЫЕ USB FLASH DRIVE

С.Д. Тиунов, студент 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, t5d@ms.tusur.ru

С недавнего времени на рынке появились USB Flash-память с некоторыми функциями безопасности. Эти функции могут быть направлены на решение как задачи конфиденциальности (монолитный корпус, прозрачное шифрование, аутентификация), так и задачи целостности (ударопрочный или водонепроницаемый корпус).

В данной статье рассмотрены одна модель USB Flash-памяти (Transcend JetFlash 220) и ее система безопасности.

Носитель оснащен двумя устройствами: собственно Flash-память и swipe-type сканер отпечатка пальца для аутентификации.

Память устройства разделена (логически) на 3 части: открытый раздел, закрытый раздел и раздел виртуального CD. Открытый раздел доступен всем пользователям, имеющим логический доступ к памяти (устройство, определенное как flash-память), а закрытый раздел доступен только после аутентификации. На разделе виртуального CD размещено ПО, поставляемое вместе с устройством, которое позволяет пользователю провести регистрацию отпечатков, аутентификацию и некоторые другие функции. При аутентификации логический раздел, соответствующий открытому разделу, заменяется на закрытый, таким образом, пользователь получает к нему доступ.

Сканер предназначен для регистрации отпечатков (при первом запуске) и дальнейшей аутентификации пользователя. Для сканирования отпечатка необходимо провести палец по сканирующей полоске. Эта конструкционная особенность обеспечивает некоторый уровень защиты от использования побочных отпечатков, оставленных законным пользователем на других вещах.

По общему описанию устройства, приведенному выше, сложно судить о безопасности. В рамках данной работы было проведено исследование защитных свойств устройства.

Было исследовано штатное ПО устройства, прежде всего модуль аутентификации. При прослушивании USB-порта во время аутентификаци было обнаружено, что программа периодически запрашивает большие порции данных у устройства (600h байт). Эти порции данных, очевидно, содержат текущее состояние сканирующего слоя. Следовательно, решение о соответствии принятого отпечатка эталонному принимается программой.

В Интернете была найдена статья [1], которая сообщает о небезопасности подобных устройств и предлагает способ переключения на закрытый раздел без аутентификации. Для этого достаточно послать

устройству единственную команду, например, с помощью программы plscsi. Приведенный в статье [1] способ взлома действительно сработал для данного устройства. Поэтому использовать данное устройство в серьезных целях невозможно.

Известно, что сканер отпечатка пальца можно использовать в системах аутентификации, однако, как правило, эти сканеры являются встроенными в систему. В рамках данной работы штатное ПО устройства было исследовано на предмет использования библиотек работы со сканером, найдены точки входа для работы с устройством, получения отпечатка, точки входа для работы с отпечатками, выделения особенностей (minutaes), сравнения отпечатков.

На основе полученных данных была реализована альтернативная система аутентификации в Windows NT. Реализованная система использует устройство как сканер и поэтому не обладает недостатками безопасности самого устройства. Важная информация эталонных отпечатков хранится в защищенных ключах реестра Windows, поэтому для взлома такой системы аутентификации теоретически следует предпринять настолько же сложные действия, как и для взлома стандартной парольной системы защиты Windows: как минимум получить эталонные отпечатки.

Вообще эталонные отпечатки не являются отпечатками в прямом смысле, они являются аналогом хеш-функции для отпечатков пальца. Поэтому считается, что по эталонным отпечаткам нельзя получить рисунок отпечатка, который пройдет проверку. Это должно затруднить взлом системы уже после получения эталонного отпечатка.

ЛИТЕРАТУРА

1. http://www.heise-online.co.uk/security/features/110280

РАСПОЗНАВАНИЕ СМЫЧНЫХ СОГЛАСНЫХ

С.Д. Тиунов, студент 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, t5d@ms.tusur.ru

Смычные (взрывные) согласные – это класс согласных, выделенных по способу образования: при произнесении смычных согласных возникает т.н. смычка, полное смыкание активного и пассивного органов, прерывающее ход воздушной струи [1]. Смычные согласные произносятся в две фазы: собственно смычка и размыкание. На спектрограмме такая структура представлена как область низкой энергии длительностью около 30 мс и область высокой энергии длительностью около 5 мс (рис. 1).

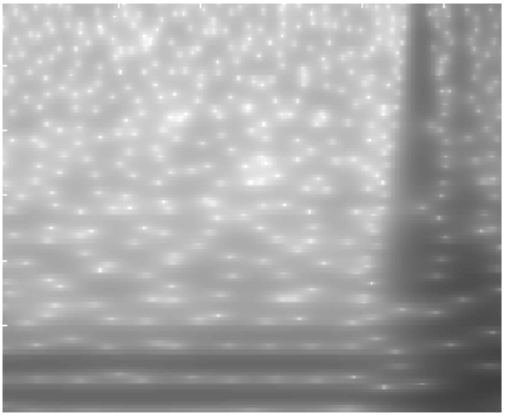


Рис. 1. Типичная спектрограмма смычного звука (звук Т)

Исследовательская работа по автоматическому распознаванию смычек была проведена в рамках проекта ГПО. Для автоматического распознавания в проекте используются нейронные сети прямого распространения, а для подготовки сигнала к обработке нейронными сетями из окна спектра выделяются некоторые параметры.

Исследовательская работа состояла из следующих этапов:

– выделение (создание) эффективных параметров (для выделения смычек);

– подборка обучающей и тестовой выборки;

– обучение и проверка нейронных сетей.

В ходе работы было выделено пять параметров – кандидатов для использования в нейронной сети распознавания смычек. Два параметра из них оказались наиболее эффективными:

– conc128 – концентрация спектра (128 каналов) в окне 30 мс – доля окна, содержащая 90% энергии;

– rel128 – отношение энергии последних 3 мс окна к энергии 30 мс окна.

Реакция этих параметров на смычку состоит в том, что первый параметр принимает низкие значения (близкие к 0), а второй – высокие, близкие к 1. В остальных звуках, как правило, значения параметров противоположные.

Обучающая выборка представляет собой отрезки сигналов для обучения нейронной сети. Изначально в обучающей выборке было несколько экземпляров смычек и несколько несмычных звуков. Причем сегментация проводилась «под параметр» с помощью реализованного в рамках проекта исследовательского комплекса, и для обучаю-

щей выборки брались только наиболее ярко выраженные отрезки (где лучше всего проявляются указанные выше свойства параметров по определению смычек).

Однако процесс обучения проводился итерационно, и обучающая выборка редактировалась с каждой новой нейронной сетью с целью улучшить характеристики (уменьшить количество ошибок).

Тестовая выборка представляет собой набор сигналов, на которых проверяется обученная нейронная сеть с целью определить процент ошибок. Подсчет ошибок в данной работе проводился вручную. В данной работе использовались две тестовых выборки.

Первая тестовая выборка состояла из 6 групп по 7 сигналов четырех дикторов – всего 42 сигнала. Благодаря этой выборке была выяснена потенциальная возможность использования данных параметров для реализации дикторонезависимых нейронных сетей, так как для обучения использовались сигналы только одного диктора, при этом ошибки составили в среднем для смычных звуков:

– 16% ошибок I рода (смычка не проставлена);

– 165 ошибок II рода (смычка проставлена там, где ее нет), при количестве смычек – 210.

Уже при тестировании на первой выборке были выделены следующие проблемы:

– проблема классификации звуков «Ч’», «Ц»;

– проблема классификации звуков «Р», «Р’».

Первая группа звуков в фонетике называется аффрикатами и, как показала практика, выделенные параметры плохо реагируют на них, хотя аффрикаты содержат смычку.

Звуки «Р», «Р’» с точки зрения фонетики относятся к классу дрожащих. При этом дрожащие звуки могут быть одноударными, двухударными и т.д.

Для чистоты эксперимента проблемные звуки намеренно не добавлялись в обучающую выборку, а использовалось свойство нейронных сетей к обобщению. В результате эксперимента оказалось целесообразным не включать эти звуки в класс смычек, так как нейронные сети реагировали на них меньше, чем в половине случаев. Таким образом, в классе остались лишь т.н. взрывные согласные.

Вторая тестовая выборка составлялась с тем расчетом, чтобы она содержала достаточное количество каждого из смычных звуков. Количество вхождений смычных звуков колебалось от 6 (у звука «Г’») до 28 (у звука «Т»). При этом выборка содержала по 34 сигнала от двух дикторов.

Результаты проверки лучшей нейронной сети из построенных следующие:

– 17,5% ошибок I рода у обоих дикторов;

– 150 ошибок II рода у первого диктора, 160 – у второго, при количестве смычек – 160.

При этом распределение ошибок между звуками у разных дикторов разное, так, для первого диктора можно подобрать такую классификацию звуков, что ошибка I рода для первого диктора составляла 8,6%.

Ошибки II рода в основном имеют место на проблемных звуках, упомянутых выше, а также в абсолютном начале, в местах перехода звука со слабой энергией в звук с сильной энергией (например, ударную гласную).

ЛИТЕРАТУРА

1. Буланин Л.Л. Фонетика современного русского языка. М.: Высшая школа, 1970. 206 с.

ОБМЕН СООБЩЕНИЯМИ В ДЕЦЕНТРАЛИЗОВАННОЙ ЗАЩИЩАЕМОЙ СИСТЕМЕ

В.А. Цевменков, студент 4-го курса, каф. КИБЭВС

г. Томск, ТУСУР, т. 8-923-409-76-65, klonts@sibmail.com

Целью работы проектной группы КИБЭВС-0733 является создание бессерверной системы передачи сообщений в сети Интернет. В рамках темы освещена проблема передачи сообщений в разработанной системе. Сложность решения поставленной задачи заключается в особенности построения связей между пользователями. В ходе реализации системы было принято решение о разделении всех пользователей на два вида: «активных» и «пассивных». «Активные» могут принимать входящие подключения, тем самым они напрямую связаны с каждым участником общения. «Пассивные» не обладают возможностью приема входящих подключений, но могут подключиться ко всем «активным» пользователям. В итоге получается неполносвязная система, в которой отсутствуют связи между «пассивными» участниками общения. После разработки архитектуры связей, представленной на рис. 1, перед группой встал вопрос о надежной доставке сообщений в режиме «чата» и «приватного» общения.

Обмен данными, ориентированный на соединения, может использовать надежную связь, для обеспечения которой протокол транспортного уровня посылает подтверждения о получении данных и запрашивает повторную передачу, если данные не получены или искажены. Протокол TCP использует именно такую надежную связь. Протокол

TCP требует, чтобы перед отправкой сообщения было открыто соединение [1]. Передачу сообщениями было решено строить, опираясь на высоконадежный протокол TCP. В рабочем порядке группой рассматривалось несколько вариантов организации протокола передачи сообщений.

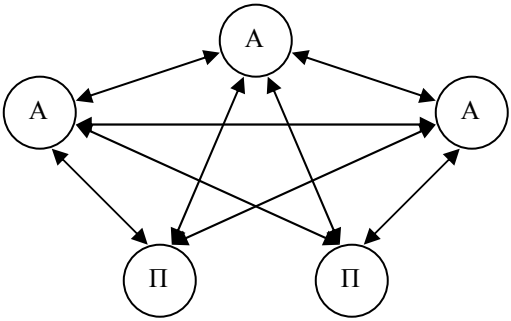


Рис. 1. Архитектура связей децентрализованной системы
(А – «активный» пользователь; П – «пассивный» пользователь)

Самым очевидный и надежный способ доставить данные – это передать их напрямую от одного пользователя другому. Такой способ не подходит для децентрализованной системы, так как в режиме типа «чат» вся нагрузка придется на терминал пользователя. Сообщения придется передавать каждому участнику общения в порядке очереди, что вызовет накапливаемую задержку и высокие затраты на исходящий трафик. Кроме того, в разработанной системе отсутствуют связи между «пассивными» пользователями, а это означает невозможность непосредственного обмена между ними.

Следующим рассмотренным вариантом передачи информации стала пересылка сообщений от одного пользователя нескольким. Такой подход позволяет значительно снизить затраты отправителя, несколько снижает время задержки, но возникает ряд серьезных проблем. При такой рассылке сообщений возникает необходимость в маршрутных картах для сообщений, чтобы одна и та же информация не приходила к пользователю несколько раз. В этом случае возрастает объем служебной информации для каждого сообщения и время ее обработки на каждом терминале.

Окончательным решением поставленной задачи стал алгоритм передачи сообщений типа «цепь». Отправитель выбирает случайно из множества подключенных к нему пользователей следующее звено цепочки. К сообщению добавляется информация об отправители, чтобы он не получил это сообщение вторично, и пакет отправляется дальше.

Сложность возникает, когда все «активные» пользователи уже получили сообщение, а «пассивные» еще нет. Тогда «активным» пользователям приходится играть роль транзитных инстанций между «пассивными», чтобы обеспечить целостность системы.

Результатом проделанной работы в рамках данной темы явилось создание алгоритмов передачи сообщения, которые нашли отражение в программе, написанной в среде Visual Studio. Эта среда объединяет средства.Net разработки в интегрированную среду [2].

ЛИТЕРАТУРА

1. Кровчик Э., Кумар В., Лагари Н. Net.Сетевое программирование для профессионалов. М.: Лори, 2005. 400 с.

2. Торстейнсон П., Оберг Р. Архитектура.Net и программирование на Visual C++. СПб.: Вильямс, 2002. 642 с.

ОБЗОР СПОСОБОВ ЗАЩИТЫ БАЗ ДАННЫХ АРХИТЕКТУРЫ КЛИЕНТ–СЕРВЕР

А.Н. Уразаева, студентка 4-го курса, каф. КИБЭВС

г. Томск, ТУСУР, u.alina88@mail.ru

Защита баз данных (БД) является одной из самых сложных задач, стоящих перед подразделениями, отвечающими за обеспечение информационной безопасности. Определение уровня безопасности зависит от важности информации, хранящейся в БД.

Классический взгляд на решение данной задачи включает обследование предприятия с целью выявления таких угроз, как хищения, утрата, уничтожение, модификация, отказ от подлинности. На втором этапе следует составление математических моделей основных информационных потоков и возможных нарушений, моделирование типовых действий злоумышленников; на третьем – выработка комплексных мер по пресечению и предупреждению возможных угроз с помощью правовых, организационно-административных и технических мер защиты.

Сети клиент/сервер обеспечивают более высокий уровень производительности и безопасности. Система клиент/сервер – локальная сеть, состоящая из клиентских компьютеров, которые обслуживает компьютер-сервер.

Первым делом для защиты СУБД необходимо защитить подключение к серверу. Если СУБД и Web-сервер, обрабатывающий сценарий, расположены на одном физическом компьютере или сервере, то необходимо запретить любые подключения к СУБД извне. Должны быть разрешены только локальные подключения. Если СУБД и Web-сервер физически разделены, то необходимо разрешить подключения

только с определенных IP-адресов: самого Web-сервера и компьютеров, на которых работают администраторы. Это можно сделать с помощью межсетевого экрана (файрвола). Файрвол – программа, представляющая собой защитный барьер между компьютером и внешним миром. Файрвол блокирует внешние атаки, утечку информации, действия злоумышленников в локальной сети, предоставляет полный контроль над всей сетевой активностью.

Чтобы сценарий Web-сервера смог получить данные, он подключается к определенной БД и в зависимости от прав доступа выполняет какие-либо действия. Большинство сценариев просто выбирает данные из таблиц и отображает их пользователю. Для этого достаточно иметь права только на выборку данных (оператор SELECT). Вполне логично будет запретить учетную запись, через которую сценарий подключается к СУБД, изменять структуру БД, т.е. добавлять и удалять такие объекты, как базы данных, таблицы и т.д. То есть нужно запретить выполнение команд CREATE TABLE, ALTER TABLE, DROP TABLE. Для внесения таких изменений необходимо иметь отдельную учетную запись или запись администратора и вмешиваться в структуру БД напрямую (с помощью утилит администрирования), а не через сценарий.

Администратор Web-сервера должен иметь больше прав, поэтому в сценарии администрирования можно для подключения использовать другие права, например те, которые вводит пользователь при входе в закрытую часть Web-сервера. Это удобно, когда несколько администраторов с разными правами. В этом случае правильный доступ гарантируется не только проверками в сценарии, но и самой СУБД.

Практически все СУБД устанавливаются с настройками по умолчанию, при которых учетная запись администратора установлена по умолчанию. Необходимо как минимум установить сложный пароль, а лучше переименовать учетную запись. Необходимо заблокировать анонимный доступ к СУБД. Подключения должны осуществляться только авторизованными пользователями. Лучше всего запретить удаленное подключение к СУБД и удалить все БД, созданные для тестирования и отладки.

В СУБД существует два механизма: назначение полномочий (называемых также привилегиями) с помощью команд SQL GRANT и REVOKE и создания курсоров. Использование курсоров в сочетании с командами GRANT и REVOKE предоставляет избирательный доступ к различным подмножествам данных.

Команды GRANT и REVOKE указывают, каким пользователям можно выполнять определенные операции в отношении определенных таблиц, курсоров и столбцов. С помощью курсора пользователи могут запрашивать и модифицировать только те данные, которые они могут

видеть. Остальная часть базы данных является для них и невидимой, и недоступной.

Решить проблему устранения коллизий при одновременном поступлении нескольких запросов от разных пользователей на получение одних и тех же данных позволяет управление транзакциями. Транзакции необходимы для контроля совпадений (устранения конфликтов пользователей, пытающихся одновременно обратиться к базе данных) и восстановления (предоставления возможности системе базы данных вернуть эту базу данных в нормальное состояние после сбоя программного или аппаратного обеспечения).

Физический ущерб базе данных может быть нанесен сбоем носителя информации. Защитой от этого вида сбоя является регулярное получение резервных копий базы данных и ведение системного журнала транзакций.

Все современные СУБД умеют работать с триггерами. Триггер в Transact-SQL представляет собой именованную совокупность операторов SQL, описывающую действие, которое необходимо выполнить при попытке выполнения указанной операции модификации данных в отношении определенного столбца или таблицы. Триггерные условия могут указывать дополнительные критерии, которые определяют, приведут ли к выполнению триггерного действия попытки выполнения команд INSERT, DELETE или UPDATE.

Администраторы очень часто должны иметь доступ к БД удаленно. В этом случае можно выбрать один из следующих шагов:

1. Разрешить удаленное подключение, но при этом защитить его с помощью межсетевого экрана. Необходимо запретить для всех доступ к порту и разрешить доступ только с определенных IP-адресов, где работают администраторы.

2. Использовать шифрование данных. В этом случае данные между сервером и клиентом будут передаваться в зашифрованном виде.

Обеспечение информационной безопасности современных информационных систем требует комплексного подхода. Оно невозможно без применения широкого спектра защитных средств, объединенных в продуманную архитектуру. Для полного решения проблемы защиты данных администратор безопасности должен иметь возможность проводить мониторинг действий пользователей, в том числе с правами администратора.

ЛИТЕРАТУРА

1. Фленов М. Web-сервер глазами хакера. СПб.: БХВ-Петербург, 2007. 271 с.

2. Давыдова Е.М., Новгородова Н.А. Базы данных: метод. пособие. Томск, 2005. 115 с.

3. http://www.aladdin.ru/presscenter/publications/publication5219.php

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ ОБМЕНА СООБЩЕНИЯМИ

Д.Н. Вечерина, студентка 4-го курса, каф. КИБЭВС
г. Томск, ТУСУР, vedahsa@sibmail.com.

В данной статье рассмотрены перспективы применения спроектированной в рамках группового проектного обучения децентрализованной системы обмена сообщениями в сети Интернет.

При передаче информации любого содержания по локальной сети или сети Интернет одной из главных проблем является ограниченная скорость передачи данных. Наиболее распространенная в настоящее время архитектура сетевых приложения «клиент–сервер» очень уязвима к влиянию данного фактора. В клиент-серверной архитектуре вся информации передается через центральное звено – сервер. При увеличении числа клиентских приложений, подключенных к данному серверу, возрастает количество информации, передаваемой через сервер, что приводит к снижению скорости передачи.

Спроектированная система является децентрализованной, т.е. в ней нет центрального звена – сервера. Это позволяет производить передачу информации непосредственно от пользователя к пользователю. Такой вид передачи существенно сокращает ограничение по максимальной скорости передачи каждого отдельно взятого пользователя. Отсутствие сервера делает данную систему удобной для передачи различных типов информации. К моменту написания статьи система успешно справлялась с задачей передачи текстовых сообщений. Но каковы же ее возможности?

Одним из приоритетных направлений развития системы является передача звуковой и видеоинформации. При передаче этих типов информации основным требованием является пропускная способность канала передачи. При использовании сервера на него ложится очень большая нагрузка, так как объемы передаваемой информации велики. Также стоит отметить, что при наличии сервера пользователи, имеющие по каким-либо причинам, малую скорость обмена информации с сервером, оказываются не способными для обмена аудио и видеоинформацией. В случае децентрализованной системы информация передается от пользователя пользователю, что позволяет обойтись без дорогостоящего сервера. При передаче информации в децентрализованной системе появляется возможность выбора оптимального с точки зрения скорости маршрута передачи информации. Это позволяет расширить круг пользователей данной системы, избегая невозможность обмена информацией между пользователями, имеющими низкую скорость передачи друг с другом, но не другими пользователями. Также

стоит отметить, что отсутствие сервера делает систему довольно гибкой – созданная сеть работоспособна, пока хотя бы один пользователь ее использует. Еще одним плюсом отсутствия сервера является высокая степень защищенности. Как было сказано выше, информация передается от пользователю к пользователю, причем не всегда напрямую, что снижает вероятность ее перехвата. А если учесть, что созданная система поддерживает аутентификацию и шифрование передаваемой информации, то она становится практически идеальным инструментом для создания «приватных» сетей. Это очень удобно, если нужно ограничить круг общения (передачи информации). Таким образом, систему можно использовать в качестве голосового или видеочата, аудио-, видеоконференции, с ограниченным доступом и конфиденциальностью передаваемой информации.

Еще одним важным направлением развития системы является создание среды обмена файлами. Сейчас существует большое количество пиринговых сетей. Однако большинство из них так или иначе требуют наличие сервера, который, как правило, отличается от клиентских приложений. В случае использования децентрализованной системы все приложения равнозначны. Это открывает широкие возможности для построения пиринговых сетей. Так как все приложения равнозначны, можно использовать один или несколько компьютеров в качестве псевдосерверов. Псевдосервер представляет собой компьютер с запущенным приложением созданной системы. Адрес этого компьютера будет использоваться как опорный для создания сети. При выходе всех пользователей из сети всегда можно построить новую сеть, подключившись к компьютеру, адрес которого всем известен. Это позволит увеличить количество пользователей, обменивающихся информацией в пределах одной сети. Однако это не означает, что система превращается в клиент-серверную. Во-первых, псевдосервер – это такое же приложение, как и все другие, образующие сеть. Во-вторых, наличие псевдосервера вовсе не обязательно – это сделано лишь для увеличения «размеров сети», ведь при увеличении количества пользователей в сети увеличивается количество доступной для обмена информации. При выходе псевдосервера из сети сеть останется работоспособной, так как все приложения равнозначны, а значит, каждое в момент нахождения в сети исполняет роль псевдосервера. Очевидно, что для ограничения доступа к информации можно либо построить «приватную» сеть, как в случае с закрытой конференцией, либо при использовании аутентификации создать списки групп пользователей, имеющих право доступа к той или иной информации.

Подводя итог, можно сказать, что созданная децентрализованная система обмена сообщениями является гибкой, надежной системой для построения сетей различного назначения.

МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Е.С. Волокитина, аспирантка каф. КЗИС
Курский государственный технический университет,
т. (4712)554-538, eva_kursk@mail.ru

Анализ состояния дел в сфере информатизации показывает, что в настоящее время сформировалась концепция и структура защиты информации, основу которой составляют:

1. Развитый арсенал технических средств защиты информации, производимых на промышленной основе.
2. Значительное число организаций, специализирующихся на решении вопросов защиты информации.
3. Четко очерченная система взглядов на проблему обеспечения безопасности информации.
4. Наличие практического опыта обеспечения защиты информации.

Тем не менее, как свидетельствует отечественная и зарубежная печать [1–3], число злоумышленных действий по несанкционированному доступу к информации не только не уменьшается, но и имеет достаточно устойчивую тенденцию к росту. Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов.

Именно это обуславливает необходимость глубокого изучения и анализа существующей обстановки и особенно выявления актуальных угроз информационной безопасности. При этом должны быть оценены все угрозы, с которыми можно столкнуться, и выбраны только те, которые могут повлиять на безопасность информации. Стандарт ИСО/МЭК 15408 предполагает, что при описании угроз должны быть идентифицированы источники этих угроз, методы воздействия, уязвимости, присущие объекту, и многое другое.

Целесообразно создать методологический инструмент формирования поля возможных проявлений угроз, основанный на изучении всех влияющих факторов и позволяющий рассмотреть все возможные, даже самые маловероятные варианты.

Такая методология анализа и оценки возможностей реализации угроз информационной безопасности должна быть основана на построении модели угроз, классификации, анализе и оценке источников угроз, уязвимостей (факторов) и методов реализации.

Моделирование процессов нарушения информационной безопасности (ИБ) целесообразно осуществлять на основе рассмотрения логической цепочки: «угроза – источник угрозы – метод реализации – уязвимость – последствия» (рис. 1).

Под угрозой понимается потенциально существующая возможность случайного или преднамеренного действия (бездействия), в результате которого могут быть нарушены основные свойства информации и систем ее обработки: доступность, целостность и конфиденциальность. Знание спектра потенциальных угроз защищаемой информации, умение квалифицированно и объективно оценить возможность их реализации и степень опасности каждой из них являются важным этапом сложного процесса организации и обеспечения защиты. Определение полного множества угроз информационной безопасности практически невозможно, но относительно полное описание их, применительно к рассматриваемому объекту, может быть достигнуто при детальном составлении модели угроз.

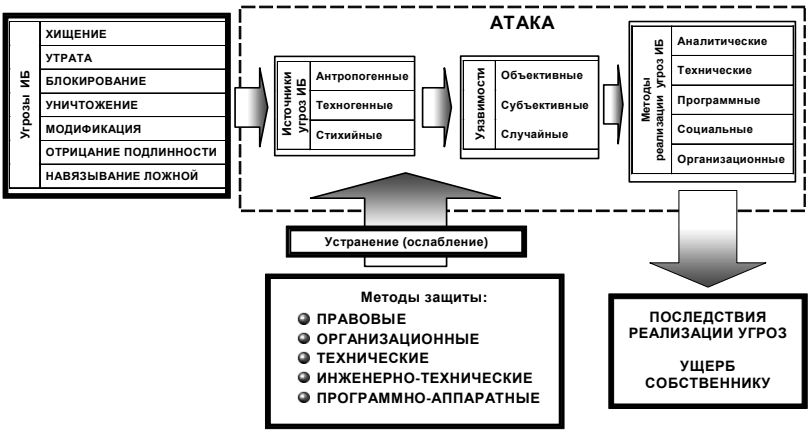


Рис. 1. Модель реализации угроз ИБ

Наложение угроз безопасности информации на модель сети позволяет в первом приближении оценить их опасность и методом исключения определить наиболее актуальные для конкретного объекта защиты. Кроме того, можно в первом приближении оценить объемы необходимых работ и выбрать магистральное направление по обеспечению защиты информации.

Анализ уязвимости – необходимый этап в создании эффективной системы информационной безопасности. По его результатам разрабатываются проектные варианты технических комплексов безопасности.

Для оценки показателей уязвимости (устойчивости) используются методы математического моделирования, для чего разрабатываются

специальные модели и методики. Модель оценки представляет собой формализованный алгоритм расчета указанных показателей.

На сегодня известны модели и методики оценки показателей уязвимости (устойчивости), разработанные в США, других странах [4, 5]. Существуют такие модели и в ряде ведомств России, но последние носят внутриведомственный характер и не нашли еще широкого применения и признания.

Практика применения подобных моделей показала, что они весьма удобны и полезны при обосновании проектных решений. Сам процесс создания и применения моделей оценки, анализа получаемых результатов дает исключительно богатую информацию для специалистов. Главное в использовании моделей – формализация процедур оценок и анализа, снижения субъективности в оценках, ясное представление эффекта реализации конкретной системы информационной безопасности. Лучше всего иметь набор моделей оценки, использующих различные методы расчета и моделирования, уровни детализации и представления структуры объекта и исходных данных.

ЛИТЕРАТУРА:

1. Кораблев С. О статистике, статистах и утечках персональных данных // Information Security. 2008. № 5. Сентябрь. С. 21.

2. Ульянов В. Персональные данные в России 2008 // Information Security. 2008. № 5. Сентябрь. С. 22–25.

3. Баева Т. Персональная защита банковской информации // Information Security. 2008. № 3. Апрель–май. С. 24–25

4. Городецкий В.И., Котенко И.В., Юсупов Р.М. Защита компьютерных сетей // Вестник российской академии наук. 2006. Т. 76. № 7. С. 668–670.

5. Garcia Mary Lynn. Design and evaluation of physical protection systems. 2007. 370 с.

РЕГИСТРАЦИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ СЕТИ

А.С. Яценко, студент 3-го курса, каф. КИБЭВС

г. Томск, ТУСУР, y_a_s@sibmail.com

В современном мире, мире новых информационных и сетевых технологий нельзя представить деятельность фирмы или корпорации без средств вычислительной техники, так как объемы обрабатываемой и хранимой информации очень велики. Если раньше в основном были одиночно стоящие компьютеры, то сейчас, как правило, это сети различных размеров. Хотя сетевые технологии значительно расширили возможности бизнеса, новые возможности всегда сопряжены с новыми

рисками. Чем сложнее сеть, тем выше риск осуществления по отношению к ней различных угроз.

Для построения системы защиты информации необходимо использовать одну из моделей оценки уязвимости и защиты информации. Но используемые модели не всегда дают желаемый результат, поскольку подразумевают большое количество допущений, а также для обеспечения работы моделей необходимы большие объемы таких исходных данных, подавляющее большинство которых в настоящее время отсутствует. Следовательно, данные модели требуют доработки. Но для доработки требуется большое количество статистической информации, которую необходимо накапливать.

Для решения проблемы накопления статистической информации о нарушениях информационной безопасности в корпоративной сети была реализована автоматизированная система (АС). АС состоит из базы данных под управлением СУБД InterBase и программной части разработанной в системе визуального программирования Borland Delphi 7. Программная часть обладает удобным пользовательским интерфейсом. В программе реализованы механизмы идентификации и аутентификация, проходящие на уровне СУБД. Пользователи системы разделены на три группы с различными правами доступа к базе данных. Программная часть позволяет регистрировать, обрабатывать и хранить информацию о пользователях, отделах, компьютерах корпоративной сети и нарушениях информационной безопасности выявленных в сети. Над собранной статистической информацией можно проводить различные выборки, с помощью запросов с параметрами реализованных в программной части АС, посредством которых можно выявлять слабые места в защите корпоративной сети.

Сбор статистической информации достаточно трудоемкий, но если люди, отвечающие за безопасность сетей, будут использовать данную автоматизированную систему или подобные ей, то можно будет создать новые или значительно улучшить уже существующие модели оценки уязвимости и защиты информации.

ЛИТЕРАТУРА

1. Мещеряков Р.В. Основы информационной безопасности: метод. указания. Томск: ТУСУР, 2001. 75 с.

2. Бобровский С. Delphi7: учеб. курс. М., 2002. 640 с.

3. Давыдова Е.М., Новгородова Н.А. Базы данных: учеб. пособие. Томск: ТУСУР, 2007. 127 с.

4. Конноли Т., Бегг К. Базы Данных. Проектирование, реализация и сопровождение. Теория и практика. 3-е изд. М.: Изд. дом «Вильямс», 2003. 1440 с.

ПОРТАТИВНЫЙ КОМПЛЕКТ ДЛЯ ОБНАРУЖЕНИЯ СРЕДСТВ СЪЕМА ИНФОРМАЦИИ И ВЫЯВЛЕНИЯ КАНАЛОВ ЕЕ УТЕЧКИ «ПКУ-6М»

Д.А. Зайцев, В.А. Нопин, студенты 4-го курса, каф. КИБЭВС,
А.П. Зайцев, науч. рук., к.т.н., проф. каф. КИБЭВС
г. Томск, ТУСУР, т. 413-426, zap@keva.tusur.ru

Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М» представляет собой удобную в работе многофункциональную поисковую систему. Рассмотрим особенности выявления каналов утечки информации на примерах виброакустического канала и обнаружения микрофонов.

Виброакустический канал. При визуальном обследовании помещения отмечаются все жесткие конструкции (балки, колонны, бетонные стены, трубы и т.п.), выходящие за пределы контролируемой зоны. Исследование предполагаемого виброакустического канала утечки информации проводится по схеме рис. 1.

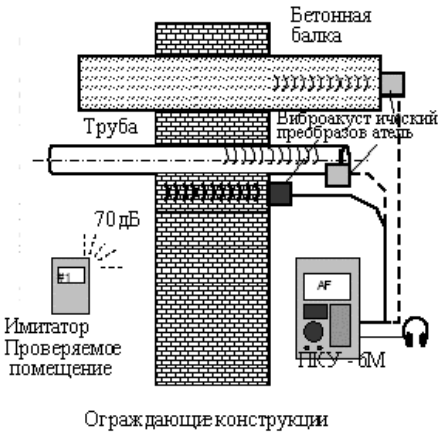


Рис. 1. Схема исследования виброакустических каналов

Схема исследования виброакустических каналов такая же, как и схема исследования акустических каналов, только микрофон заменяется виброакустическим датчиком, который должен иметь плотный контакт с жесткой конструкцией с усилием порядка 5 кг.

Имитатор в режиме «AUDIO» создает со стороны проверяемого помещения тестовый акустический сигнал с уровнем 70 дБ. Уровень прошедшего через ограждение сигнала измеряется виброакустическим датчиком и основным блоком, работающим в режиме AF.

Выявление микрофонного эффекта и обнаружение скрытых микрофонов. Перед началом поисковых работ необходимо изучить все проводные коммуникации, выходящие за пределы контролируемой зоны, и провести исследования по схеме рис. 2.

Наличие микрофонного эффекта осуществляется следующим образом. Имитатор переводится в режим работы «AUDIO» и последовательно устанавливается на расстоянии 1 м от офисного оборудования. Основной блок подключается через входной комплектный низковольтный кабель к проверяемой проводной линии. Наличие микрофонного эффекта оценивается по появлению сигналов в головных телефонах. Офисное оборудование исследуется при всех режимах его работы.

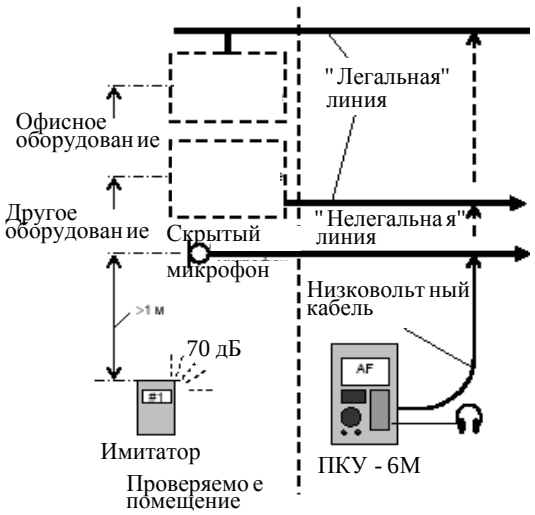


Рис. 2. Выявление микрофонного эффекта и обнаружение скрытых микрофонов

Для выявления скрытно установленных микрофонов в ограждающих конструкциях основной блок подключается к проводной линии неизвестного назначения. В линию от основного блока подается постоянное напряжение 15 В с поочередной сменой полярности и включается имитатор. Наличие микрофона оценивается по характерному сигналу в головных телефонах.

На базе комплекта разработано две лабораторные работы по выявлению каналов утечки информации.

МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЛЕЧЕБНО-ПРОФИЛАКТИЧЕСКИХ УЧРЕЖДЕНИЙ ТОМСКОЙ ОБЛАСТИ

В.Д. Зыков, аспирант каф. КИБЭВС
г. Томск, ТУСУР, т. 412-500, zvd@udcs.ru

В соответствии с Федеральным законом «О персональных данных» [1] операторы (к которым относятся все медицинские учреждения) при обработке персональных данных обязаны «принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним».

В соответствии с Законом «О персональных данных» 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.

Методы и способы защиты информации в информационных системах в зависимости от класса ИСПД также изложены в нормативно-методических документах ФСБ и ФСТЭК.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям ФЗ «О персональных данных», в Томской области является Управление Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Россвязьохранкультура) по Томской области.

В соответствии с вышеизложенным предлагаются следующие этапы для осуществления мер по обеспечению безопасности персо-

нальных данных при их обработке в информационных системах лечебно-профилактических учреждений Томской области:

1. Определение перечня, структуры и связей информационных систем, обрабатывающих персональные медицинские данные.

2. Определение типов и содержания обрабатываемых персональных медицинских данных.

3. Определение списка сотрудников, имеющих доступ к персональным данным, обрабатываемым в информационных системах.

4. Документальное регламентирование работы с персональными данными.

5. Формирование модели угроз персональным данным.

6. Уведомление Управления Россвязьохранкультуры по Томской области об обработке персональных данных.

7. Проектирование и внедрение системы защиты персональных данных на основании модели угроз.

8. Заключение договора с лицензиатом по технической защите конфиденциальной информации об аутсорсинге.

9. Аттестация (сертификация) ИСПД.

10. Эксплуатация и сопровождение ИСПД.

Ранее созданные информационные системы персональных данных должны быть приведены в соответствие с [1] не позднее 1 января 2010 г. Неисполнение требований Федерального закона может привести к следующим рискам для медицинских учреждений:

1. Неправомерный случайный или предумышленный доступ к персональным данным третьих лиц.

2. Гражданско-правовые иски со стороны пациентов.

3. Административные санкции со стороны регуляторов: ФСТЭК России, ФСБ России, Россвязьохранкультуры.

ЛИТЕРАТУРА

1. Федеральный закон № 152-ФЗ от 27.07.06 «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».

КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ СЕРВИСОВ ДОВЕРЕННОЙ ТРЕТЬЕЙ СТОРОНЫ

В.Д. Зыков, аспирант каф. КИБЭВС
г. Томск, ТУСУР, т. 412-500, zvd@udcs.ru

В лечебно-профилактических учреждениях Томской области обрабатывается информация о состоянии здоровья граждан, которая относится к персональным данным и сведениям, составляющим врачебную тайну. Обработка данной информации производится как в информационных системах персональных данных (ИСПД), так и традиционными методами.

В соответствии с Федеральным законом «О персональных данных» [1] были утверждены «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 ИСПД, и «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [3], которое устанавливает требования к обеспечению безопасности персональных данных при их обработке традиционными методами. Согласно [2] безопасность персональных данных при их обработке в ИСПД обеспечивается с помощью системы защиты персональных данных, которая включает в себя:

1. Организационные меры.
2. Средства защиты информации:
2.1. Шифровальные (криптографические) средства.
2.2. Средства предотвращения несанкционированного доступа.
2.3. Средства предотвращения утечки информации по техническим каналам.
2.4. Средства предотвращения программно-технических воздействий на технические средства обработки персональных данных.
3. Информационные технологии.

Защите подлежат:

1. Речевая информация.
2. Информация, обрабатываемая техническими средствами.
3. Носители информации.
4. Каналы связи (организационными мерами и/или техническими средствами).
5. Помещения, оборудование системы защиты информации.

При обработке персональных данных в ИСПД должно быть обеспечено:

1. Предотвращение несанкционированного доступа к персональным данным.

2. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

3. Недопущение нежелательного воздействия на технические средства.

4. Возможность незамедлительного восстановления персональных данных.

5. Постоянный контроль за обеспечением уровня защищенности персональных данных.

6. Регистрация запросов пользователей ИСПД и фактов предоставления ПД по этим запросам в электронном журнале.

В качестве базовой технологической составляющей для защиты персональных данных, обрабатываемых в ИСПД, предлагается использование технологии инфраструктуры открытых ключей с использованием служб «Доверенной третьей стороны».

«Доверенная третья сторона (ДТС)» – технология оказания доверенных электронных услуг различного назначения.

Указания по применению и управлению службами ДТС включены в рекомендации Международного союза телекоммуникаций (ITU) серии X.842 [4].

Роль доверенной третьей стороны предполагает гарантию того, что сообщения и транзакции своевременно и точно передаются требуемому получателю и что в случае возникновения любых разногласий существуют соответствующие методы подготовки и доставки требуемых свидетельств, позволяющих восстановить ход событий. Сервисы доверенной третьей стороны могут включать управление ключами и сертификатами, поддержку идентификации и аутентификации, службу привилегий, поддержку неотвергаемости, фиксацию времени (time stamping), электронные нотариальные службы и службы каталогов. ДТС может предоставлять все перечисленные службы либо их часть.

Для защиты персональных данных, обрабатываемых в ИСПД лечебно-профилактических учреждений Томской области, предлагается, в качестве основных, использование следующих служб ДТС:

1. Службы управления ключами и сертификатами.

2. Служба фиксации времени.

3. Службы электронного нотариата.

ЛИТЕРАТУРА

1. Федеральный закон № 152-ФЗ от 27.07.06 «О персональных данных».

2. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности пер-

сональных данных при их обработке в информационных системах персональных данных».

3. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4. Рекомендации Комитета по стандартизации электросвязи МСЭ Х.842 «Информационные технологии – Методы защиты – Руководящие указания по применению и управлению сервисами доверенной третьей стороны».

ТЕХНОЛОГИЯ ОТБОРА ПРЕТЕНДЕНТОВ ДЛЯ РАБОТЫ И УЧЕБЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.В. Дереглазова, студентка 4-го курса, каф. ИСУ

г. Омск, СибАДИ, т. 8-908-111-86-53, dereglazova.svet@mail.ru

В течение многих лет основное направление защиты информационных ресурсов от несанкционированного доступа строились на нейтрализации внешних угроз. В последние годы было осознано, что наиболее опасной угрозой являются внутренние нарушители – инсайдеры. Более 60% всех инцидентов нарушений безопасности связаны с нынешними, бывшими и временными сотрудниками компаний. В 2006 г. за счет внутренних инцидентов потери мировой экономики составили 700 млрд долл., средний ущерб в год от инсайдерской атаки составляет 355 тыс. долл. Приведенные цифры дают основания считать, что нейтрализация внутренних угроз становится определяющим фактором в стратегии борьбы за безопасность информационных ресурсов. В то же время они иллюстрируют непреложный факт: существующие технологии противодействия внутренним угрозам требуют усовершенствования, особенно когда речь идет о защите государственной тайны.

Анализ обозначенной проблемы на системном уровне показал, что из 9 факторов, порождающих внутренние угрозы, ключевыми являются уровень профессионализма сотрудников служб безопасности и морально-психологический портрет лиц, допущенных к работе с информационными ресурсами. По существующим оценкам уровень профессионализма работников в информационной сфере колеблется от 0,3 до 0,8 (максимум 1), а нравственный облик работников России, начиная с начала перестройки, падает. Снизить остроту проблемы позволит отбор кадров по соответствующим методикам, выявляющим неспособных к работе в сфере информационной безопасности (ИБ).

Признанная в мире технология отбора кадров по способностям Дж. Баррета [1, 2] требует доработки: в ней отсутствуют профили при-

годности к работе в области ИБ. В рамках проведенной работы удалось решить эту проблему и разработать программный комплекс для одновременного тестирования нескольких человек.

В основу разработанной методики оценки способностей испытуемого и определения его пригодности к специальности в сфере ИБ положен принцип многофакторного тестирования личности. По результатам анкетирования узконаправленных специалистов ИБ выявлены способности, необходимые для работы и учебы в сфере ИБ. В качестве оцениваемых способностей, дающих достаточно полное представление о потенциале тестируемого, отобраны такие показатели, как абстрактное мышление, пространственная ориентация, системность (организованность), вычислительные способности, трехмерная визуализация, логический анализ, память, сообразительность, внимание. Для каждой из способностей подобран соответствующий тест, большинство тестов осуществлены по методике британского ученого Дж. Баретта. Для определения пригодности тестируемого к определенной профессии необходимо учитывать результаты всех тестов и проводить сравнение результатов испытуемого с эталоном для данной специальности. Сравнение производится на основе корреляции показателей, а эталон составляется из усредненных результатов группы людей соответствующей специальности.

Для автоматизации процесса тестирования и обработки полученных результатов создано клиент-серверное программное приложение, с помощью которого по представленной методике оценки способностей было проведено тестирование успешных студентов третьего курса специальности ИБ. После статистической обработки полученных результатов было выявлено, что показатели по всем рассматриваемым способностям высокие, а дисперсия в испытуемой группе для каждого показателя небольшая, что подтверждает правильность выбора тестируемых способностей. По обработанным результатам создан эталон (таблица), который можно применять для определения профпригодности претендентов на учебу по специальности ИБ. Для создания эталона на другие специальности и социальные статусы (кандидат-соискатель на должность) необходимо

Эталон претендентов на учебу по специальности ИБ

Способность	Правильные ответы, %
Абстрактное мышление	73
Пространственная ориентация	65
Системность (организованность)	93
Вычислительные способности	79
Трехмерная визуализация	85
Логический анализ	90
Память	75
Сообразительность	89
Внимание	100

провести тестирования соответствующих групп, а затем обработать статистику и получить необходимые эталоны.

Предложенная методика проведения оценки профессиональной пригодности претендентов для работы и учебы в сфере информационной безопасности может помочь отобрать кандидатов, способных к успешному освоению профессии в сфере ИБ.

ЛИТЕРАТУРА

1. Баррет Дж. Карьера: способности и выбор. М.: АСТ, 2003. 204 с.
2. Баррет Дж. Протестируй себя. СПб.: Питер, 2003. 254 с.

ИДЕНТИФИКАЦИЯ ЯЗЫКА ЗАШУМЛЕННОГО ТЕКСТА

О.С. Дулькейт, аспирантка
каф. комплексных систем защиты информации
г. Омск, ОмГУ им. Ф.М. Достоевского, т. 8-960-981-94-05,
osdulkeyt@inbox.ru

В настоящее время множество различных приложений занимается распознаванием текстов, переводом с одного языка на другой, выбором нужной кодировки и т.п. (программы распознавания отсканированных текстов, программы категоризации данных, почтовые программы, браузеры, переводчики) [1, 2]. В этих приложениях предполагается указание языка или кодировки для отображения текстов. Выбор языка выполняется либо пользователем, либо самим приложением. Идентификация языка также является первым шагом в работе спам-фильтров, а также программ поиска запрещенных веб-страниц и сайтов. Кроме того, для обеспечения доступности важной информации необходимо иметь способ ее восстановления (например, автоматический выбор кодировки для корректного отображения).

Если слова текста состоят из разноязычных символов либо содержат много ошибок (например, после неудачного сканирования текста, после передачи по зашумленным каналам связи или преднамеренного искажения злоумышленником), то определение принадлежности данного текста к какому-либо языку оказывается затруднительным.

Анализ существующих методов. Существующие методы распознавания языка позволяют достичь точности до 99% [3], однако область их применения является ограниченной.

В работе [4] упоминается метод распознавания языков по акцентированным символам. Этот метод привязан к конкретной кодировке и не может применяться при работе с зашумленными текстами. В [5] предлагается использовать словарь коротких слов и уникальных сочетаний символов (метод обладает тем же ограничением, что и преды-

дущий). В [6] предлагается использовать статистические данные (Марковская модель). Эта модель рассчитывает вероятность встретить данную строку в языке. Для сравнения используются данные, полученные в ходе обучения системы на тренировочных текстах. Метод не требует лингвистических знаний для определения языка и может быть основан только на символах, однако также привязан к кодировке. В работе [7] описывается метод распознавания на основе наиболее часто встречающихся *N*-грамм – один из наиболее успешных методов согласно [3]. Такой метод удобно применять для языков со схожим алфавитом, например для европейских языков. Этот метод не требует знания лингвистики. Кроме того, мелкие опечатки мало влияют на общую статистику и не мешают определить язык. В книге предлагается использовать только 300 наиболее часто встречаемых *n*-грамм для каждого языка. Этот метод также хорошо работает для очень коротких текстов, например из 1–2 слов. Достигает высоких результатов, если текст содержит более 20 символов. Однако данный метод не работает для азиатских языков. Для решения проблемы с азиатскими языками в [8] вводится расширение статистического метода, работающее с байтами. Однако оба метода также привязаны к кодировкам.

Среди известных методов не зависящим от кодировки является метод PPM (prediction by partial matching) [9]. Шаблонные тексты сжимаются специальным алгоритмом. Тексты для распознавания тоже сжимаются и затем вычисляется число бит, необходимых для кодирования полученного документа. Оптимальное число бит для кодирования дает результат, совпадающий с шаблоном для языка.

Так как этот метод не имеет таких ограничений, как привязанность к кодировке и большой объем словаря, то рассмотрим его подробнее и проведем оценку его трудоемкости.

Для поиска оптимального метода кодирования автор предлагает использовать так называемые смешанные контекстные модели [10].

Контекстной модели с абсолютными вероятностями символов присваивается порядок 0, модели с условными вероятностями текущего символа в зависимости от одного предыдущего символа – порядок 1, от цепочки двух символов – порядок 2 и так далее. Каждой модели присваиваются веса и вычисляется взвешенная сумма вероятностей: если $p_o(\varphi)$ – вероятность символа φ из алфавита A для модели порядка 0, ω_o – вес модели, m – максимальный порядок используемых моделей, то комбинированные вероятности могут быть вычислены как

$$p(\phi) = \sum_{o=-1}^{m} \omega_o \cdot p_o(\phi) .$$

Пусть $c_o(\varphi)$ – количество раз использования символа φ в текущем контексте; C_o – количество раз появления контекста.

$$C_o = \sum_{\phi \in A} c_o(\phi).$$

Тогда вероятности можно вычислить как $p_o(\phi) = \frac{c_o(\phi)}{C_o}$.

Пусть e_0 – вероятность встретить не встречавшийся ранее символ в модели 0. Тогда веса можно выразить как

$$\omega_o = (1 - e_o) \times \prod_{i=o+1}^{l} e_i, \quad -1 \le o \le l, \quad \omega_l = (1 - e_l),$$

где l – максимальный порядок для ненулевых условий.

Простейший способ расчета e_o: $e_o = \frac{1}{C_o + 1}$.

Тогда количество операций расчета вероятности одного символа при известных вероятностях для всех моделей: m операций умножения вероятности на вес, для расчета каждого из m весов требуется l умножений e_i и одно деление для расчета каждого e_i. Таким образом, общее число операций для расчета вероятностей: $n*m*(l + 1)$. А общее число операций для расчета энтропии $2n^2*m*(l + 1)$. В лучшем случае при $m = 1$ и $l = 0$, число операций $2n^2$ (если уже рассчитаны все условные вероятности символов). То есть алгоритм требует дополнительных расчетов условных вероятностей и $2n^2$ – наилучшая оценка.

Новый метод идентификации языка

Покажем, что можно предложить другой метод, также не зависящий от кодировки и не требующий большого словаря, но при этом меньшей трудоемкости.

Возьмем за основу метода аналогию для передачи информации по каналам связи, однако будем опираться не на кодирование информации, а на шифрование. Наименее трудоемким при передаче данных по каналам связи является метод поточного шифрования.

В качестве характеристики преобразования информации будем использовать не количество бит для кодирования, как в предыдущем методе, а матричный оператор, соответствующий преобразованию.

Как известно из [11], шифру гаммирования соответствует циркулянт (квадратная матрица, полученная циклическим сдвигом первой строки), построенный на основе вероятностей символов алфавита текста. Характеристикой преобразования, задаваемого матрицей, независимо от базиса являются собственные числа [12]. Они и будут рассмотрены в работе.

Существуют различные алгоритмы нахождения собственных чисел матриц, например – обобщенный метод Якоби [13], степенной метод, различные QR-алгоритмы, основанные на приведении матриц к подобным, имеющим треугольный или квазитреугольный вид. Однако для циркулянтов собственные числа можно находить проще. Для этого в настоящей работе предлагается конкретная формула для каждого собственного числа.

Рассмотрим циркулянт, полученный циклическим сдвигом первой строки вправо

$$P=\begin{pmatrix} p_0 & p_{n-1} & \cdots & p_1 \\ p_1 & p_0 & \cdots & p_2 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ p_{n-1} & p_{n-2} & \cdots & p_0 \end{pmatrix}, \qquad (1)$$

где p_j – частота встречаемости j-го символа в тексте, $j = 0, 1, \ldots, n-1$.

Найдем собственные числа матрицы (1). Как известно, они находятся из нелинейного уравнения

$$|P - E\lambda| = 0. \qquad (2)$$

Преобразуем это выражение, учитывая, что P – циркулянт. Перепишем (2) в виде $|P'| = 0$, где P' получается из P заменой p_0 на $(p_0 - \lambda)$. Далее воспользуемся формулой вычисления определителя циркулянтов. Определитель циркулянта вычисляется [11] по формуле

$$|P| = f(\varepsilon_0) \cdot f(\varepsilon_1) \cdot \ldots f(\varepsilon_{n-1}), \qquad (3)$$

$\{\varepsilon_0,\ldots,\varepsilon_{n-1}\}$ – множество всех корней степени n из 1, а $f(x) = p_0 + p_{n-1} \cdot x + \ldots + p_1 \cdot x^{n-1}$.

Учитывая, что мы заменили p_0 на $(p_0 - \lambda)$, выделим λ из каждой скобки правой части равенства $|P'| = 0$ и получим n собственных чисел. Выражение для j-го собственного числа выглядит следующим образом:

$$\lambda_j = \sum_{k=0}^{n-1} p_{n-k} \cdot \varepsilon_j^k, \text{ где } j = 0, 1, \ldots, n-1. \qquad (4)$$

В ходе исследования естественных языков были рассчитаны частотные характеристики польского, чешского, литовского, норвежского, венгерского, эстонского, финского и арабского языков, эсперанто, латыни и иврита [14]. Исследования проводились по материалам [15]. Для остальных языков были взяты известные частоты встречаемости символов [11].

Для языков 8 языковых групп на основе формулы (4) были вычислены модули всех собственных чисел циркулянтов, построенных на основе частот, упорядоченных по возрастанию (таблица). Количество собственных чисел составляло от 21 до 44 в зависимости от языка. По-

лученные значения были отсортированы в порядке невозрастания. Максимальные значения собственных чисел (не считая единицу) оказались близкими внутри языковых групп. Следующие за ними собственные числа оказались также близкими внутри языковых групп, однако позволяют различить языки между собой.

Был проведен расчет устойчивости собственных чисел к колебаниям значений частоты символов текста. Оказалось, что собственные числа являются более устойчивой характеристикой, чем частоты использования символов алфавита.

Модули собственных чисел естественных языков

Языковая группа	Язык	Макс. значения модулей собств. чисел	
		1	2
Славянские языки	Польский	0,3175	0,6093
	Чешский	0,3097	0,6315
	Русский	0,3765	0,6090
	Украинский	0,2532	0,5895
Балтийские языки	Латышский	0,3223	0,6332
	Литовский	0,3665	0,6310
Германские языки	Норвежский	0,3585	0,7148
	Английский	0,3822	0,7373
	Немецкий	0,3922	0,7470
Романские языки	Французский	0,4215	0,7858
	Испанский	0,4253	0,7805
	Итальянский	0,4471	0,7917
Уральские языки: Финно-угорские языки	Венгерский	0,3150	0,5350
	Эстонский	0,4103	0,7537
	Финский	0,4411	0,7954
Искусственные языки	Эсперанто	0,4306	0,7727
Италийские языки	Латынь	0,4345	0,7931
Афразийские яз.: Семитские яз.	Иврит	0,3585	0,7399

Учитывая, что максимальными собственными числами являются всегда числа с известными заранее номерами, то для каждого конкретного текста достаточно вычислить только пару характеристических значений. Таким образом, словарь для идентификации языков будет содержать два значения для каждого языка. А трудоемкость вычисления для конкретного текста составляет $8n + 4$ квадратичных операций, где n – объем алфавита текста, что меньше трудоемкости приведенного ранее алгоритма ($2n^2$), основанного на кодировании текста.

В качестве практического подтверждения приведенных выше теоретических результатов для циркулянтов была разработана программа RestorerNoiseFile [16]. Программа предназначена для распознавания языка зашумленных тестов и их дальнейшего восстановления. Выполняет вычисление собственных чисел текстов и определяет на их основе язык исследуемого документа. Восстанавливает текст в соответствии с определенным языком.

С помощью данной программы были проведены эксперименты по выявлению области применения полученной характеристики. Процент ошибок при выборе языка как литературных, так и естественно-научных текстов составил 0,03 при эксперименте для 100 текстов размером от 1 до 200 Кбайт юникода. При этом неверно определялся язык для текстов маленького объема (1–2 Кбайта) с нехарактерными частотами использования символов. Невозможным определить язык оказалось для текстов, содержащих большое количество аббревиатур (например, различные пользовательские документации к приложениям) и иноязычных названий или имен собственных. Процент неверного определения языка внутри группы составляет около 30%, что подтверждает результат о близости значений собственных чисел циркулянтов для языков одной языковой группы.

Полученные результаты говорят о том, что собственные числа циркулянтов более успешно могут применяться в задаче распознавания языковой группы, что позволит значительно сократить количество предполагаемых языков.

Выводы

1. Собственные числа циркулянтов, соответствующих текстам, можно использовать в качестве характеристики языка, что предоставит еще один метод идентификации языков зашумленных текстов.
2. Предложенный метод не зависит от кодировки исследуемого текста.
3. Идентификация языка на основе собственных чисел требует хранения только двух шаблонных значений для каждого языка.
4. Трудоемкость предложенного метода меньше трудоемкости известного метода на основе количества бит для кодирования.
5. Предложенный метод позволяет идентифицировать языковую группу исследуемого текста с точностью 97%, а также сам язык (вероятность ошибки внутри группы 30%).
6. Предложенный метод является более эффективным для текстов объемом от 1000 символов, не содержащих значительного количества аббревиатур и иноязычных названий/имен.

ЛИТЕРАТУРА

1. Soumen Chakrabarti. Mining the WEB. Discovering knowledge from hypertext data / S. Chakrabarti. Bombay: Indian Institute of Technology, 2003. 345 p.

2. Martin, Melanie Jeanne. Reliability and verification of natural language text on the World Wide Web. New Mexico State University, 2005. 144 p.

3. Simon Kranig Bogentorstr. Evolution of language identification methods. University of Tubingen International Studies in Computational Linguistics, 2006. 24 p.

4. Kenneth R. Language Identifier: A Computer Program for Automatic Natural-Language Identification of on-line text. // 29th Annual Conference of the American Translators Association, 12–16 October, 1988. P. 47–54.

5. Grefenstette G. Comparing two language identification schemes. // 3rd International Conference on Statistical Analysis of Textual Data, Rome, 11–13 December, 1995. 6 p.

6. Dunning T. Statistical Identification of language. New Mexico State University, 1994. P. 94–273.

7. Cavnar W.B., Trenkle J. M. N-gram-based text categorization.// Symposium on Document Analysis and Information Retri-eval in Las Vegas, 1994. P. 161–175.

8. Kikui G. Identifying, the coding system and language, of on-line documents on the Internet. // 16th conference on Computational Linguistics, 1996. P. 652–657.

9. Teahan, W. and Harper D. Using Compression-Based Language Models for Text Categorization. Workshop on Language Modeling and Information Retrieval, 2001. 10 p.

10. Witten I.H., Bell T.C., Moffat A. et al. Semantic and Generative Models for Lossy Text Compression // The Computer Journal. 1994. Vol. 37. P. 83–87.

11. Алферов А.П. Основы криптографии. М.: Гелиос, 2002. 480 с.

12. Курош А.Г. Курс высшей алгебры. М.: Наука, 1975. 432 с.

13. Уилкинсон Дж.Х. Справочник алгоритмов на языке Алгол. Линейная алгебра. М.: Машиностроение, 1976. 390 с.

14. Ефимова О.С., Файзуллин Р.Т. Применение собственных чисел при гаммировании текстов и идентификации языков // Омский научный вестник. Информационные технологии. 2006. № 9 (46). Декабрь. С. 146–152.

15. Язык как инструмент познания мира – www.multikulti.ru

16. Ефимова О.С. Программа восстановления зашумленных текстов // ОФАП Федерального агентства по образованию РФ. 2007 (Рег. № 7633). 7 с.

МЕХАНИЗМ СОБЫТИЙНО-ОБУСЛОВЛЕННОГО ДЕЛЕГИРОВАНИЯ И ОТЗЫВА ПОЛНОМОЧИЙ

Д.В. Кириллов, соискатель каф. БИС

г. Самара, САМГУ, т. 8-927-294-31-81, kirillov@ssu.samara.ru

Сущностью механизма делегирования полномочий является предоставление пользователям АС (автоматизированной системы) права передавать (временно или постоянно) часть или все полномочия из множества назначенных им полномочий другим пользователем.

Особенно широко данный принцип применяется в контроле доступа на основе ролей (КДОР), где, в соответствии с принципами данного механизма разграничения полномочий, традиционно все операции по назначению прав доступа выполняет администратор (офицер безопасности системы).

Использование делегирования полномочий делает систему КДОР более гибкой и простой с точки зрения администрирования системы, однако порождает следующие проблемы:

1) высокую вероятность ошибки пользователя, в связи с его низкой квалификацией или недостаточным вниманием при выполнении операций;

2) снижение общего уровня управляемости системы безопасности, и, как следствие этого, снижение общего уровня безопасности.

Автором предлагается альтернативный подход к управлению политикой безопасности на основе КДОР – событийно-обусловленное делегирование и отзыв полномочий, далее СОДОП, который, с одной стороны, позволяет использовать преимущества механизма делегирования полномочий, а с другой – делает процесс распространения прав доступа более управляемым.

Сущностью подхода является то, что процедура делегирования или отзыва полномочий производится в результате некоторого события или последовательности событий и решение о выполнении процедуры делегирования или отзыва полномочий принимается на основе условий, описывающих некоторое состояние системы, причем в качестве элементов условия могут использоваться как компоненты КДОР и отношения между ними, так и атрибуты объектов, определяемые на уровне бизнес-логики автоматизированной системы (АС).

Понятие делегирования полномочий как процесса передачи прав на выполнение некоторого множества операций от одного пользователя другому или от пользователя к некоторой роли неассоциированной с пользователем, делегирующим полномочия, в контексте КДОР, впервые было рассмотрено в работе Барка, Сандху и др. [1].

Дальнейшие исследования в этом направлении касались либо расширения исходной схемы делегирования полномочий на множество инвариантов модели КДОР [2], либо на реализации ограничений делегирования, позволяющих разрабатывать более гибкие в управлении и безопасные с точки зрения предотвращения эскалации прав схемы делегирования полномочий [3].

Предлагаемая модель делегирования полномочий (СОДОП) расширяет существующие модели путем внесения понятия события и связанного с ним автоматическим принятием системы решения о делегировании полномочий.

Событийно-обусловленное делегирование и отзыв полномочий (*СОДОП*) – это процесс передачи или отзыва ранее делегированных полномочий от одного пользователя к другому пользователю или роли, не ассоциированной с пользователем, делегирующим полномочия, в результате возникновения некоторого события или последовательности событий в автоматизированной системе, и в соответствии с формально описанными условиями делегирования и отзыва полномочий, хранимых в некотором виде в АС.

СОДОП имеет следующие отличия от традиционных моделей делегирования полномочий:

1) в СОДОП принятие решение о делегировании (отзыве) полномочий и процедура делегирования (отзыва) полномочий могут быть значительно разнесены во времени;

2) инициатор делегирования полномочий и субъект, чьи полномочия делегируются, в общем случае не являются одним и тем же субъектом.

СОДОП применяется в контексте той или иной инвариантной модели КДОР и одной (или более) их базовых моделей делегирования полномочий. Рассмотрим компоненты, формирующие базовую модель СОДОП, реализуемую на основе «плоского» КДОР и базовой модели делегирования полномочий [2].

К базовым компонентам КДОР, формирующий модель «плоского» КДОР, относятся множества пользователей (*USERS*), ролей (*ROLES*), объектов (*OBS*), операций (*OPS*), полномочий (*PRMS*) и сеансов пользователей (*SESSIONS*).

Взаимосвязь компонентов «плоского» КДОР ($RBAC_0$) представлена на рис. 1.

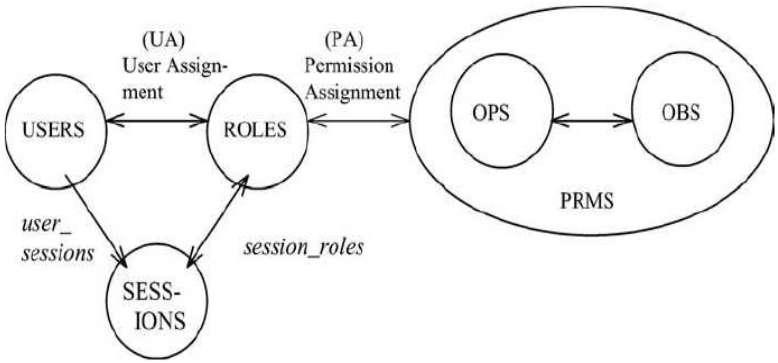


Рис. 1. Компоненты «плоского» КДОР и связи между ними

Рассмотрим основные отношения между компонентами системы.

Отношение назначения пользователям ролей (*UA*) – это отношение вида «многие-ко-многим», формально описываемое как

$$UA \subseteq USERS \times ROLES . \quad (1)$$

Множество полномочий *PRMS* представляет собой отношение вида «многие-ко-многим» между элементами множества операций и объектов системы и формально описывается как

$$PRMS = 2^{OPS \times OBS} . \quad (2)$$

Отношение назначения ролям полномочий (*PA*), представляет собой отношение вида «многие-ко-многим» между элементами множеств полномочий и ролей и формально описывается как

$$PA \subseteq PRMS \times ROLES . \quad (3)$$

В базовой модели делегирования полномочий в контексте КДОР ($RBDM_0$), расширяющей модель «плоского» КДОР, путем внесения понятия делегирования пользовательских полномочий определяются дополнительные компоненты и отношения. В контексте $RBDM_0$ для каждой роли, принадлежащей множеству $ROLES$, определяется два подмножества назначенных на эту роль пользователей:

1) оригинальные пользователи, ассоциированные с ролью $Users_O(r)$;

2) пользователи, ассоциированные с ролью в результате делегирования полномочий $Users_D(r)$.

В дополнение к модели $RBAC_0$ вводятся следующие отношения:

1) отношение *UAO* вида «многие-ко-многим», связывающее элементы множества ролей и назначенных на эти роли оригинальных пользователей, формально определяемое как

$$UAO \subseteq USERS \times ROLES ; \quad (4)$$

2) отношение *UAD* вида «многие-ко-многим», связывающее элементы множества ролей и назначенных в результате делегирования на эти роли пользователей, формально определяемое как

$$UAD \subseteq USERS \times ROLES . \quad (5)$$

Кроме того, в связи с внесением нового типа отношений назначения пользователя на роль переопределяется отношение назначения пользователей на роль следующим образом:

$$UA = UAO \cup UAD;$$

$$UAO \cap UAD = \varnothing.$$

Функции принадлежности оригинальных пользователей к некоторой роли *r* и пользователей, назначенных на роль, в результате делегирования полномочий формально описываются соответственно:

$$USERS_O(r)=\{U\,|\,(U,r)\in UAO\};\quad (7)$$

$$USERS_D(r)=\{U\,|\,(U,r)\in UAD\}.\quad (8)$$

Одним из центральных понятий в контексте $RBDM_0$ является понятие длительности делегирования полномочий, определяющего для каждой операции делегирования время, в течение которого делегированные полномочия действительны. Элементы множества длительностей делегирования и элементы множества отношения *UAD* связываются функцией отображения:

$$delegate_roles: UAD \to T\,.\quad (9)$$

В качестве ограничения на выполнение операции делегирования полномочий выступает отношение *can_delegate*, определяемое как

$$can_delegate \subseteq ROLES \times ROLES\,.\quad (10)$$

Например, $(a\in ROLES, b\in ROLES)\in can_delegate$ означает что пользователь, назначенный на некоторую роль *a*, может делегировать роль *a* некоторому пользователю, назначенному на роль *b*.

Отношение *can_delegate* не рефлексивно, что означает недопустимость операции делегирования пользователю, назначенному на ту же роль, на которую назначен делегирующий пользователь и которую этот пользователь делегирует.

Рассмотрим компоненты и отношения, реализующие на базе моделей $RBAC_0$ и $RDBM_0$ базовую схему СОДОП.

Как было отмечено выше, в отличие от традиционной схемы делегирования решение о выполнении процедуры делегирования полномочий может принимать субъект, отличный от того, чьи полномочия делегируются. Определим субъекта, принимающего решение о выполнении процедуры делегирования или отзыва полномочий, как *инициатора делегирования*.

Инициатор делегирования – субъект, принимающий решение о делегировании полномочий путем описания условий делегирования.

При этом субъекта (пользователя), чьи полномочия делегируются, будут делегированы, назовем *делегатором*, а субъекта (пользователя или роль), которому делегируются полномочия, назовем *делегатом*.

В качестве делегата полномочий может выступать любой субъект системы, если выполняются следующие условия:

1) не нарушаются системные ограничения используемого инварианта КДОР [1];

2) не нарушаются базовые принципы делегирования полномочий [2];

3) не нарушаются ограничения делегирования (если их присутствие допустимо в контексте выбранной базовой схемы делегирования

полномочий), такие как ограничения на переделегирование полномочий [4].

В общем виде процесс выполнения операций делегирования полномочий в контексте СОДОП представляет собой описание условий делегирования полномочий инициатором делегирования, уполномоченным на это действие, от делегатора полномочий делегату, причем полномочия передаются либо путем ассоциирования с ролью, одновременно назначенной и делегатору полномочий, и инициатору делегирования, либо путем создания так называемой временной роли, наделенной множеством делегируемых полномочий (причем данное множество полномочий также должно быть одновременно назначено инициатору делегирования и делегатору).

Дополнительно к отношениям *UAO* (4) и *UAD* (5) определим отношение *UAC*, связывающее множество инициаторов делегирования, делегаторов и делегатов полномочий, следующим образом:

$$UAC \subseteq USERS \times USERS \times ROLES \ . \qquad (11)$$

Либо в соответствии с ранее данными определениями:

$$UAC \subseteq USERS \times UAD \ . \qquad (12)$$

Таким образом, отношение (7) остается без изменений.

В качестве ограничения на отношение делегирования полномочий введем отношение *can_init_del*, формально описываемое следующим образом:

$$can_init_del \subseteq (USERS \cup ROLES) \times ROLES \times ROLES \ . \qquad (13)$$

Отношение *can_init_delegation* означает, что некоторый пользователь или пользователь некоторой роли, являющийся инициатором делегирования, может инициировать делегирование членства в некоторой роли от пользователя, также являющегося членом этой роли, пользователю, являющимуся членом другой роли, отличной от делегируемой. Очевидно, что данное отношение можно записать в виде

$$can_init_del \subseteq (USERS \cup ROLES) \times can_delegate \ . \qquad (14)$$

Чтобы обеспечить взаимосвязь между компонентами КДОР и компонентами бизнес-логики системы, необходимо иметь некоторые характеристики этих объектов. Для этого введем понятие с*войств или атрибутов объектов*.

Свойства (*атрибуты*) *объектов* – некоторые отличительные характеристики объектов, присущие тому или иному объекту в контексте системы, в котором данный объект присутствует.

Условия делегирования и отзыва полномочий (УДОП) являются фундаментальной основой СОДОП и используются для задания точки принятия решения о начале процедуры делегирования полномочий или отзыва полномочий. УДОП задаются с использованием специального

языка и правил формальной логики. Фактически УДОП составляются путем объединения событий и свойств некоторых объектов. В случае если условие истинно, выполняется операция делегирования или отзыва полномочий, если условие ложно, никаких действий не предпринимается.

Решение о выполнении операции делегирования или отзыва полномочий принимается в том случае, если условие имеет значение логической истины. В противном случае условие игнорируется до следующего изменения состояния системы.

Событие – изменение состояния системы, результатом которого стало изменение некоторых свойств компонентов автоматизированной системы, отношений между компонентами системы, а также свойств самой системы. Фактически любое событие в системе связано с выполнением той или иной операции, причем как в контексте системы разграничения полномочий, так и в рамках АС в целом.

Правила делегирования полномочий регламентируют порядок выполнения процедур делегирования полномочий с точки зрения их корректности и безопасности.

Правила делегирования и отзыва полномочий – базовые принципы СОДОП, гарантирующие корректность и безопасность выполнения процедур делегирования и отзыва полномочий в соответствии с заданными алгоритмами.

Для того чтобы непосредственно осуществлять выполнение операций делегирования и отзыва полномочий, в системе должен существовать субъект, наделенный правами выступать делегатором полномочий для любого пользователя или роли. В СОДОП таким субъектом является *монитор СОДОП*.

Монитор СОДОП – специальный субъект системы, отслеживающий события, возникающие в системе, сопоставляющий события в системе с описанными условиями делегирования и отзыва полномочий и выполняющий процедуры делегирования и отзыва полномочий на основе этих условий и в соответствии с правилами *СОДОП*.

Очевидно, что для внесения монитора СОДОП в модель КДОР, необходимо переопределить множество субъектов КДОР следующим образом:

$$S_{СОДОП} = S \cup \{d_monitor\}. \quad (14)$$

В качестве остальных компонентов модели СОДОП и ее инвариантов выступают компоненты тех инвариантов моделей КДОР и базовых схем делегирования полномочий, в контексте которых применяется модель СОДОП.

К базовым алгоритмам модели СОДОП относятся внесение условий делегирования и отзыва полномочий и выполнение операций по делегированию и отзыву ранее делегированных полномочий. Рассмотрим алгоритмы выполнения этих операций.

Внесение условия делегирования или отзыва полномочий. При внесении нового условия делегирования или отзыва полномочий выполняется следующая последовательность действий:

1) проверка корректности и непротиворечивости условия;

2) проверка достижимости состояния системы, в результате возникновения цепочки событий, описанной в условии;

3) проверка непротиворечивости вновь вносимого условия ранее описанным условиям;

4) проверка соответствия условия системным ограничениям, ограничениям используемого инварианта КДОР, ограничениям схемы делегирования, ограничениям СОДОП.

Выполнение операции делегирования полномочий. В каждый момент времени τ_i монитор СОДОП находится в ожидании возникновения некоторого события. Пусть произошло некоторое событие $event_1$, в этом случае монитор СОДОП выполняет следующие действия (блок-схема алгоритма приведена на рис. 2):

1) проход по множеству всех зарегистрированных в системе условий СОДОП и выбор из них тех, для которых событие $event_1$ является ожидаемым для делегирования полномочий;

2) для каждого найденного условия событие $event_1$ выталкивается из цепочки ожидаемых событий;

3) после того как событие вытолкнуто, определяется длина цепочки ожидаемых событий;

4) если длина цепочка событий не равна нулю, происходит переход к следующему условию;

5) если длина цепочки равна 0, то происходит вычисление выражения условия делегирования;

6) если вычисленное значение равно «ЛОЖЬ», происходит переход к следующему условию;

7) если вычисленное значение равно «ИСТИНА», производится переход к блоку проверки ограничений;

8) последовательно выполняется проверка системных ограничений, ограничений инварианта КДОР, ограничений схемы делегирования, ограничений СОДОП;

9) если хотя бы один из видов ограничений нарушен, происходит переход к следующему условию СОДОП;

10) если ни одно из ограничений не нарушено, выполняется операция делегирования полномочий в соответствии с определенными правилами делегирования полномочий.

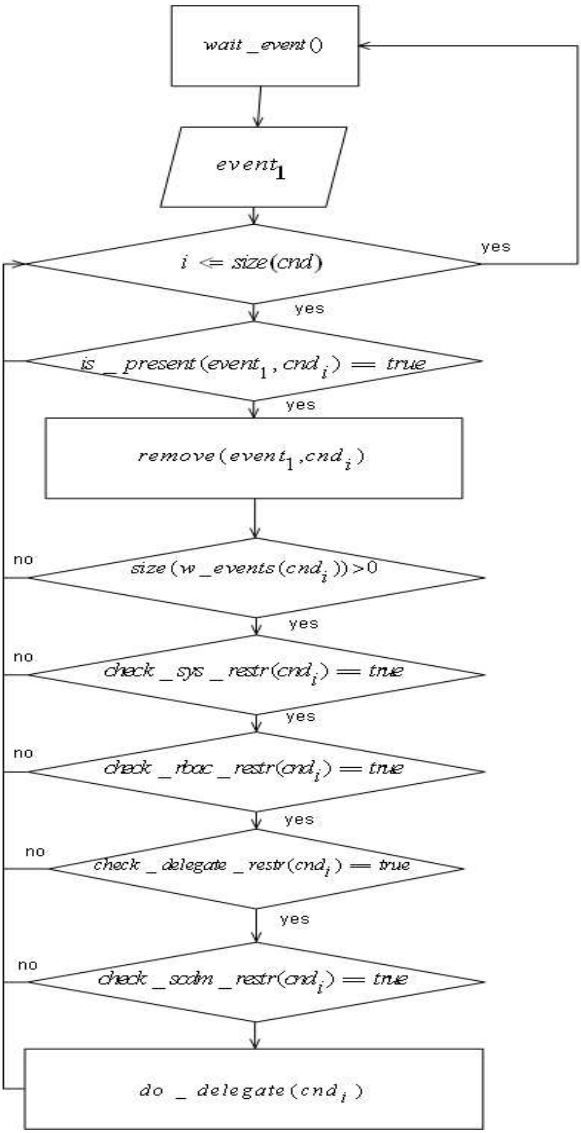


Рис. 2. Блок-схема алгоритма выполнения операции делегирования в СОДОП

Выполнение операции отзыва полномочий. При выполнении операции отзыва делегированных полномочий последовательность шагов аналогична последовательности шагов при выполнении операции делегирования полномочий, с той разницей, что при проходе по списку условий среди них отбираются те, в которых в качестве выполняемой операции указан отзыв полномочий. Кроме того, после завершения операции отзыва полномочий условие отзыва уничтожается.

Очевидно, что описанные алгоритмы являются весьма обобщенными, так как в них не учитываются особенности реальных систем, в которых они применяются.

Необходимо отметить, что в реальных условиях, алгоритм выполнения операции отзыва полномочий принимает значительно более сложный вид, так как в приведенном алгоритме не учитываются случаи циклически выполняемых условий, а также особенности, связанные с реализацией отзыва переделегированных полномочий.

Представленная в работе модель СОДОП позволит решить ряд задач, среди которых:

1) сокращение нагрузки на администратора безопасности;

2) появление возможности отложить решение о делегировании полномочий до возникновения определенного события, описанного в условии делегирования или отзыва полномочий (реализация принципа исполнения обязанностей);

3) увеличение общей гибкости системы за счет большей степени связанности уровней безопасности и бизнес-логики;

4) ошибки в назначении привилегий вероятны только в случае неправильности принципов управления и разделения обязанностей в системе.

Указанные преимущества модели СОДОП перед традиционными схемами делегирования полномочий говорят о широких перспективах использования ее в практических целях.

ЛИТЕРАТУРА

1. Sandhu R., Coyne E., Feinstein H., Youman C. Role-based access control models // IEEE Computer. 1996. № 29(2). P. 38–47.

2. Barka E., Sandhu R. A role-based delegation model and some extensions // Proceedings of Sixteenth Annual Computer Security Applications Conference (ACSAC’ 00). 2000. P. 168–177.

3. Jong Soon Park, Young Lok Lee, Hyung Hyo Lee, Bong Nam Noh. A role-based delegation model using role hierarchy supporting restricted permission inheritance // Proceedings of the International Conference on Security and Management. SAM '03, CSREA Press, 2003. P. 294–302.

4. Tamassia R., Yao D., William H. Winsborough. Role-based cascaded delegation // Proceedings of the 9th ACM Symposium on Access Control Models and Technologies. ACM, 2004. P. 146–155.

ПРОТОКОЛ КЛЮЧЕВОГО СОГЛАШЕНИЯ НА ОСНОВЕ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ С ВОЗМОЖНОСТЬЮ ВЫЯВЛЕНИЯ ЗЛОУМЫШЛЕННИКА

Д.О. Косолапов,
аспирант каф. информационной безопасности ДВГУ
г. Владивосток, ДВГУ, т. 8-914-652-22-38, dk@vl.ru

После появления в 1976 г. протокола ключевого соглашения Диффи и Хеллмана было разработано большое количество подобных протоколов [1, 2]. В связи с развитием групповых криптосистем в настоящее время актуальной является разработка протоколов ключевого соглашения для криптоконференции, т.е. протоколов, вырабатывающих ключ для 3 или большего количества абонентов [3]. В 2000 г. Антуаном Жу [4] был предложен однораундовый протокол трехстороннего ключевого соглашения. Однако протокол Жу не является аутентифицированным и подвержен атаке «человек в середине». Позже Боне и Сильверберг [5] предложили однораундовый протокол ключевого соглашения, являющийся обобщением протокола Жу и основанный на мультилинейных отображениях. Отметим, что мультилинейные отображения пока имеют только теоретическое значение, так как в настоящее время не построены какие-либо n-мультилинейные отображения со степенью мультилинейности $n \geq 3$. Кроме того, данный протокол не является аутентифицированным и поэтому, как и протокол Жу, подвержен атаке «человек в середине». Хо-Кю Ли, Хуанг-Сук Ли и Ян-Рэн Ли [6] предложили однораундовые протоколы ключевого соглашения MAK-A, MAK B-j и MAK-C на основе мультилинейных отображений и протоколов MTI и MQV. Среди протоколов Ли наиболее безопасным является MAK-C. Данный протокол был взят за основу для построения нового протокола ключевого соглашения на основе идентификационных данных с возможностью выявления злоумышленника.

Рассмотрим модель безопасности нового протокола и назовем ее расширенной моделью безопасности ключевого соглашения (FullSec). Модель безопасности представлена списком фундаментальных и дополнительных требований безопасности.

Рассмотрим фундаментальные требования безопасности.

1. Ключевая аутентификация. Ключевая аутентификация включает неявную и явную ключевую аутентификацию. При неявной ключевой аутентификации абонент A полагает, что только B может вычислить ключ, в то время как при явной ключевой аутентификации A полагает, что только B может вычислить ключ и что абонент B действительно его вычислил.

2. Ключевое подтверждение. Ключевое подтверждение заключается в проверке абонентом A того, что абонент B действительно вычислил секретный ключ K.

Рассмотрим дополнительные требования безопасности:

1. Безопасность при известном ключе сессии. Протокол является безопасным при известном ключе сессии, если он безопасно вырабатывает ключ сессии, когда злоумышленнику известны ключи предыдущих сессий.

2. Совершенная секретность в будущем. Протокол является совершенно секретным в будущем, если при компрометации долгосрочных закрытых ключей всех абонентов не нарушается секретность ключей предыдущих сессий.

3. Отсутствие подмены при ключевой компрометации. Пусть долгосрочный закрытый ключ абонента скомпрометирован. Протокол является стойким к подмене при ключевой компрометации, если компрометация одного из абонентов не позволяет злоумышленнику подменить остальных абонентов.

4. Отсутствие неизвестного разделения ключа. В данном случае злоумышленник убеждает группу абонентов в том, что она вырабатывает ключ со злоумышленником, в то время как в действительности ключ вырабатывается между группой и другим абонентом.

5. Отсутствие ключевого контроля. Отсутствие ключевого контроля означает, что любой абонент (или злоумышленник) не может контролировать (или предугадать) значение ключа сессии.

6. Выявление злоумышленника во время выполнения алгоритма. Во время проведения протокола должна существовать возможность выявления злоумышленника.

Как и для всех протоколов на основе идентификационных данных, в новом протоколе устраняется необходимость в поддержке инфраструктуры открытых ключей (PKI). Вместо PKI используется единственный центр генерации закрытых ключей PKG, что значительно проще.

Новый протокол представлен следующими процедурами.

Инициализация. Пусть G_1 и G_2 – конечные циклические группы одинакового простого порядка p, а g – генератор G_1. Пусть заданы 2 хеш-функции $H_1:\{0,1\}^* \to G_1^*$ и $H_2:G_1^* \to Z_p^*$. Пусть $A_1,...,A_n$ – n абонентов, вырабатывающих общий секретный ключ. Пусть $e_{n-1}:G_1^{n-1} \to G_2$ – $(n-1)$-мультилинейное отображение.

Генерация и рассылка закрытых ключей. Для каждого абонента с идентификатором ID_i $(1 \le i \le n)$ PKG вычисляет открытый ключ

абонента $Q_{ID_i} = H_1(ID_i) \in G_1$. Далее PKG генерирует набор случайных целых чисел $s_1,...,s_n \in [1, p-1]$, являющихся мастер-ключами абонентов. По данным мастер-ключам PKG генерирует набор открытых ключей $P_{pub_1} = g^{H_2(H_1(ID_1)^{s_1})},...,P_{pub_n} = g^{H_2(H_1(ID_n)^{s_n})} \in G_1$, предоставляет их в открытый доступ, генерирует набор долгосрочных закрытых ключей $d_{ID_1} = H_1(ID_1)^{s_1},...,d_{ID_n} = H_1(ID_n)^{s_n} \in G_1$ и каждому абоненту передает его закрытый ключ по защищенному каналу.

Публикация. Каждый абонент A_i выбирает случайное целое число $a_i \in [1, p-1]$ и вычисляет $g^{a_i} \in G_1$. Каждый абонент A_i рассылает всем остальным абонентам краткосрочный открытый ключ g^{a_i}, а a_i сохраняет в секрете.

Выработка ключа. По полученным значениям и идентификаторам i-й абонент вычисляет набор открытых ключей $Q_{ID_i} = H_1(ID_i) \in G_1$ $(1 \le i \le n)$. Далее вычисляет ключ:

$$K_{A_i} = e_{n-1}(g^{a_1 + H_2(g^{a_1} \| Q_{ID_1})} P_{pub_1},...,g^{a_{i-1} + H_2(g^{a_{i-1}} \| Q_{ID_{i-1}})} P_{pub_{i-1}},$$

$$g^{a_{i+1} + H_2(g^{a_{i+1}} \| Q_{ID_{i+1}})} P_{pub_{i+1}},...,g^{a_n + H_2(g^{a_n} \| Q_{ID_n})} P_{pub_n})^{a_i + H_2(g^{a_i} \| Q_{ID_i}) H_2(d_{ID_i})}$$

$$= e_{n-1}(g,...,g)^{a_1 + H_2(g^{a_1} \| H_1(ID_1)) H_2(H_1(ID_1)^{s_1}) ... a_n + H_2(g^{a_n} \| H_1(ID_n)) H_2(H_1(ID_n)^{s_n})}.$$

Верификация. Выработанный ключ каждый абонент зашифровывает с помощью своего идентификатора (например, алгоритмом шифрования Боне и Франклина) и отправляет полученное значение центру генерации закрытых ключей PKG. PKG расшифровывает полученные значения и проверяет равенство всех выработанных ключей. В случае равенства PKG отправляет всем абонентам сигнальное сообщение одобрения начала передачи. В случае обнаружения одного или более ключей, не совпадающих с другими ключами, PKG отправляет сообщение отказа передачи и идентификаторы абонентов, являющихся злоумышленниками.

Заметим, что абонент может и не зашифровывать выработанный ключ для передачи центру PKG при наличии защищенного канала обмена информацией с PKG (таковой должен существовать в качестве условия реализации любых алгоритмов на основе идентификационных данных). Также абонент может передавать не сам зашифрованный ключ, а зашифрованную хеш-функцию от ключа. В качестве хеш-функции могут быть использованы SHA-1 или MD5.

Докажем безопасность предложенного протокола.

Теорема. Предложенный протокол является стойким к атакам активного злоумышленника в модели безопасности FullSec при предположении сложности MDH и доверия к PKG.

Доказательство.

Напомним, что модель безопасности FullSec представлена следующими требованиями безопасности:

1. Ключевая аутентификация.
2. Ключевое подтверждение.
3. Безопасность при известном ключе сессии.
4. Совершенная секретность в будущем.
5. Отсутствие подмены при ключевой компрометации.
6. Отсутствие неизвестного разделения ключа.
7. Отсутствие ключевого контроля.
8. Выявление злоумышленника во время выполнения протокола.

1. Протокол обладает свойством неявной ключевой аутентификации, т.к. при предположении сложности MDH и доверия к PKG только абонент, у которого есть закрытый ключ, может вычислить общий секретный ключ.

2. Требование ключевого подтверждения выполняется, т.к. каждый абонент, получая от PKG сообщение корректности выработки ключа, убеждается в том, что все остальные абоненты выработали одинаковый ключ.

3. Протокол является безопасным при известном ключе сессии, т.к. все атаки данного типа нейтрализуются по причине связи краткосрочного и долгосрочного ключей абонента хеш-функцией.

4. Протокол является совершенно безопасным в будущем, т.к. ключ $K_{A_1 \ldots A_n}$ включает компоненту, объединяющую краткосрочные ключи сессии, $e_{n-1}(g,\ldots,g)^{a_1 a_2 \ldots a_n}$.

5. Протокол является стойким к подмене при ключевой компрометации, т.к. в процессе вычисления $K_{A_1 \ldots A_n}$ долгосрочные ключи комбинированы с краткосрочными ключами.

6. Протокол является стойким к неизвестному разделению ключа за счет использования хеш-функции.

7. Ни один из абонентов в протоколе не может предсказать или контролировать значение ключа сессии за счет использования краткосрочных закрытых ключей и сложности MDH.

8. Требование выявления злоумышленника выполняется в связи с тем, что протокол основан на идентификационных данных, а PKG хранит идентификационные данные абонентов и осуществляет проверку легитимности выработанного ключа. Теорема доказана.

Недостатками данного протокола являются необходимость наличия третьей доверенной стороны (в данном случае PKG), необходимость наличия защищенного канала для передачи закрытых ключей абонентам, возможность депонирования ключей, а также дополнительная вычислительная и связная нагрузка на абонентов и PKG.

Эффективность реализации протокола определяется оценкой его вычислительной и связной сложности.

Рассмотрим вычислительную сложность протокола.

На этапе инициализации и генерации закрытых ключей требуется вычисление центром PKG n функций H_1 и H_2 и $2n$ возведений в степень в G_1.

На этапе публикации каждому абоненту требуется провести 1 возведение в степень в G_1.

На этапе выработки ключа каждому абоненту требуется вычислить n функций H_1 и $n+1$ функций H_2, n возведений в степень в G_1, $3n-3$ произведений в G_1, 1 произведение и сумму в G_2 и применение n-мультилинейного отображения.

На этапе верификации каждому абоненту требуется применить алгоритм шифрования Боне и Франклина, а PKG требуется провести n расшифрований алгоритмом Боне и Франклина.

Рассмотрим связную сложность протокола.

На этапах инициализации и генерации закрытых ключей требуется проведение широковещательной рассылки n абонентам элементов группы G_1.

На этапе публикации каждому абоненту необходимо провести рассылку $n-1$ абоненту элемента G_1.

На этапе верификации каждому абоненту необходимо отправить PKG 3 элемента G_1 (напомним, что шифротекст в алгоритме Боне и Франклина представлен тремя элементами G_1), а также провести широковещательную рассылку центром PKG n абонентам сигнального сообщения.

Так как в настоящее время не построено эффективно вычислимых мультилинейных отображений со степенью мультилинейности $n \geq 3$, то полученные выше результаты пока имеют только теоретическое значение. Однако данный протокол может быть использован в частном случае при количестве абонентов $n = 3$. В качестве мультилинейного отображения выступает билинейное спаривание в группе точек эллиптической кривой. Рассмотрим протокол для $n = 3$.

Инициализация. Пусть G_1 и G_2 – конечные циклические группы одинакового простого порядка p, а g – генератор G_1. Пусть заданы 2 хеш-функции $H_1:\{0,1\}^* \to G_1^*$ и $H_2:G_1^* \to Z_p^*$. Пусть A_1, A_2, A_3 – абоненты, вырабатывающие общий секретный ключ. Пусть $e:G_1 \times G_1 \to G_2$ – билинейное спаривание (например, модифицированное спаривание Вейля).

Генерация и рассылка закрытых ключей. Для абонентов с идентификаторами ID_1, ID_2, ID_3 PKG вычисляет соответствующий открытый ключ

$$Q_{ID_1} = H_1(ID_1), Q_{ID_2} = H_1(ID_2), Q_{ID_3} = H_1(ID_3) \in G_1.$$

Далее PKG генерирует набор случайных целых чисел $s_1, s_2, s_3 \in [1, p-1]$, являющихся мастер-ключами абонентов. По данным мастер-ключам PKG генерирует набор открытых ключей $P_{pub_1} = g^{H_2(H_1(ID_1)^{s_1})}, P_{pub_2} = g^{H_2(H_1(ID_2)^{s_2})}, P_{pub_3} = g^{H_2(H_1(ID_3)^{s_3})} \in G_1$, публикует их, генерирует набор долгосрочных закрытых ключей $d_{ID_1} = H_1(ID_1)^{s_1}, d_{ID_2} = H_1(ID_2)^{s_2}, d_{ID_3} = H_1(ID_3)^{s_3} \in G_1$ и каждому абоненту передает его закрытый ключ по защищенному каналу.

Публикация. Каждый абонент A_i $(1 \le i \le 3)$ выбирает случайное целое число $a_i \in [1, p-1]$ и вычисляет $g^{a_i} \in G_1$. Каждый абонент A_i рассылает остальным абонентам краткосрочный открытый ключ g^{a_i}, а a_i сохраняет в секрете.

Выработка ключа. По полученным значениям и идентификаторам абонент A_1 вычисляет ключ

$$K_{A_1} = e(g^{a_2 + H_2(g^{a_2} \| H_1(ID_2)) H_2(H_1(ID_2)^{s_2})},$$
$$g^{a_3 + H_2(g^{a_3} \| H_1(ID_3)) H_2(H_1(ID_3)^{s_3})})^{a_1 + H_2(g^{a_1} \| H_1(ID_1)) H_2(H_1(ID_1)^{s_1})}.$$

Абонент A_2 вычисляет ключ

$$K_{A_1} = e(g^{a_1 + H_2(g^{a_1} \| H_1(ID_1)) H_2(H_1(ID_1)^{s_1})},$$
$$g^{a_3 + H_2(g^{a_3} \| H_1(ID_3)) H_2(H_1(ID_3)^{s_3})})^{a_2 + H_2(g^{a_2} \| H_1(ID_2)) H_2(H_1(ID_2)^{s_2})}.$$

Абонент A_3 вычисляет ключ

$$K_{A_1} = e(g^{a_1 + H_2(g^{a_1} \| H_1(ID_1)) H_2(H_1(ID_1)^{s_1})},$$
$$g^{a_2 + H_2(g^{a_2} \| H_1(ID_2)) H_2(H_1(ID_2)^{s_2})})^{a_3 + H_2(g^{a_3} \| H_1(ID_3)) H_2(H_1(ID_3)^{s_3})}.$$

Несложно заметить, что $A_1 = A_2 = A_3$.

Верификация. Аналогично описанному выше для 3 абонентов.

Данный протокол является стойким к атакам активного злоумышленника в расширенной модели безопасности ключевого соглашения при предположении сложности билинейной проблемы Диффи–Хеллмана. Билинейная версия предложенного протокола может быть использована в модели k-ичного дерева для выработки общего ключа n абонентами.

Итак, в рамках данной работы был разработан протокол ключевого соглашения на основе идентификационных данных с возможностью выявления злоумышленника, сформулирована расширенная модель безопасности ключевого соглашения, доказана безопасность протокола в рамках предложенной модели, проведена оценка эффективности реализации протокола. Также был рассмотрен частный случай выработки ключа тремя абонентами, который может быть использован в модели k-ичного дерева для выработки ключа n абонентами ($n \geq 3$). Данная работа является дополнением и продолжением всех работ по протоколам ключевого соглашения начиная с 1976 г. Предложенный протокол удовлетворяет требованиям безопасности, предъявляемым к информационным коммуникациям в настоящее время.

ЛИТЕРАТУРА

1. Menezes A., van Oorschot P.C., Vanstone S. Handbook of Applied Cryptography. CRC Press, Boca Raton, 1997.

2. Blake-Wilson S., Menezes A. Security profs for entity authentication and authenticated key transport protocols employing asymmetric techniques / B. Christinason, B. Crispo, T. Lomas, and M. Roe, eds. // Proceedings of the 5th International Workshop on Security Protocols, volume 1361 of Lecture Notes in Computer Science. Springer Verlag, 1997. P. 137–158.

3. Burmester M., Desmedt Y. A Secure and Efficient Conference key Distribution System // Advances in Cryptology-Eurocrypto'94. LNCS. Springer Verlag, 1995. P. 275–286.

4. Joux A. A one round protocol for tripartite Diffie-Hellman // Proc. ANTS IV, Lecture Notes in Computer Science 1838. 2000. P. 385–394.

5. Boneh D., Silverberg A. Applications of Multilinear Forms to Cryptography, 2002.

6. Ho-Kyu Lee, Hyang-Sook Lee, Young-Ran Lee. Multi-party authenticated key agreement protocols from multilinear forms. Department of Mathematics, Ewha Womans University, Seoul, Korea. 2002.

КОНТРОЛЬ НЕ ПОКРЫТЫХ ВИДЕОНАБЛЮДЕНИЕМ УЧАСТКОВ С ПОМОЩЬЮ ДОПОЛНИТЕЛЬНЫХ ИСТОЧНИКОВ ОСВЕЩЕНИЯ

А.В. Лисин, студент 5-го курса,
каф. «Средства связи и информационная безопасность»
г. Омск, ОмГТУ, т. 8-913-616-78-26, andrey.lisin@gmail.com

Видеонаблюдение – один из методов обеспечения безопасности. Он предоставляет возможности круглосуточного контроля за охраняемой территорией и при необходимости детального восстановления событий. Системы видеонаблюдения представляют собой комплекс технических средств, состоящий, как правило, из видеокамер, мониторов и устройств обработки изображений (последовательный видеокоммутатор, мультиплексор и т.д.). Системы видеонаблюдения также позволяют распознавать движения, собирать информацию по событиям, а в случае наличия встроенных систем анализа изображений распознавать лица, номера машин и другие элементы изображений [1].

Однако, несмотря на большое количество достоинств, системы видеонаблюдения обладают также рядом серьезных недостатков. Одним из самых существенных недостатков является высокая стоимость подобных комплексов. Второй недостаток в определенной степени вытекает из первого. Во всем комплексе технических средств систем видеонаблюдения число видеокамер, необходимых для контроля охраняемой территории, является наиболее варьирующимся параметром, а чем больше видеокамер необходимо установить, тем, соответственно, выше цена комплекса в целом. Еще одной проблемой является высокая стоимость качественного расчета мест установки видеокамер. Все это приводит к появлению непокрытых видеонаблюдением участков, а также «мертвых зон» под видеокамерами.

Однако даже при очень качественном решении задачи оптимизации расстановки камер наблюдения не удается достичь стопроцентного покрытия охраняемой территории. Это обусловливается тем же экономическим фактором и положением о том, что стоимость охраняемой информации должна быть меньше стоимости системы защиты. В реальных условиях наилучшим вариантом является покрытие видеонаблюдением наиболее ответственных участков: контрольно-пропускных пунктов, пространства около дверей особо важных помещений и т.д. Таким образом, видеонаблюдение как один из самых эффективных методов безопасности применяется для предотвращения наибольших возможных потерь.

Из всего вышесказанного становится очевидно, что полное покрытие видеонаблюдением охраняемой территории практически не-

осуществимо, но появилась возможность использования оптических эффектов (например, тени), которые проявляются на изображениях, полученных с помощью камер наблюдения, при отсутствии в кадре объекта, их создающего.

В данной работе описан способ обнаружения объекта, находящегося вне зоны видимости, но отбрасывающего тени, попадающие в кадры двух расположенных рядом видеокамер.

В рассматриваемом в работе случае объект наблюдения находится в зоне между двумя расположенными рядом видеокамерами и при этом не попадает в кадр ни одной из них. Также под каждой видеокамерой расположен источник света (в дальнейшем будет показано, что такое расположение является наиболее выгодным). Тени объекта падают на плоскость наблюдения (в данном случае на противоположную стену) и регистрируются видеокамерами. Описанное взаимное положение объекта и видеокамер показано на рис. 1.

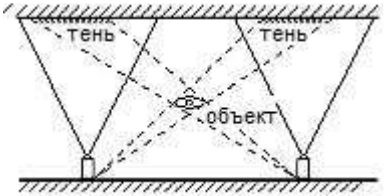


Рис. 1. Взаимное расположение видеокамер, объекта и теней

Необходимость как минимум двух источников света объясняется неоднозначностью определения размеров и положения объекта по одной его тени, т. к. объекты одной формы, но разных размеров могут отбрасывать одинаковую тень в случае, если более мелкий объект находится близко к источнику света, а большой – далеко.

Задача состоит в нахождении местоположения объекта, отбросившего тени, попавшие в кадр. Задачу можно разбить на 3 этапа:

1) поиск тени на изображении;

2) определение ее реальных линейных размеров;

3) вычисление положения объекта в пространстве, исходя из размеров его теней [2].

Определение положения объекта осуществляется однозначным образом, так что два дополнительных, правильно расположенных осветительных прибора заменяют лишнюю видеокамеру. Единственное ограничение предлагаемого метода заключается в том, что для успешного его применения в объективы видеокамер должны попасть обе тени, а для этого объект должен находиться в некоторой ограниченной

области. Учитывая прямолинейный характер распространения света, можно показать эту область графически: она представляет собой «пересечение» треугольников с вершинами в точках, где находятся источники света, и граничных точках видимости видеокамер (рис. 2).

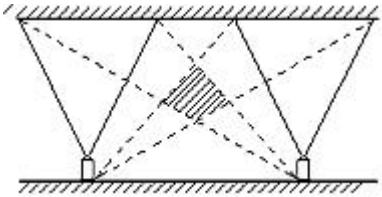


Рис. 2. Область видимости теней объекта

Несмотря на то, что область видимости теней объекта не охватывает всю непокрытую видеонаблюдением площадь, возможность ее контроля представляет множество преимуществ. Например, с помощью видеокамер, следящих за территорией напротив главного входя в здание, но не следящих непосредственно за входной дверью, можно находить объекты, стоящие напротив двери, установив два дополнительных осветительных прибора. Таким образом, при продуманной расстановке видеокамер и осветительных приборов можно добиться значительного улучшения покрытия территории видеонаблюдением, особенно учитывая низкую стоимость подобного комплекса (которая фактически складывается из стоимости осветительных приборов).

Из рис. 2 также видно, что расположение осветительных приборов непосредственно под видеокамерами дает наилучший эффект, поскольку в случае сближения или удаления друг от друга источников света область видимости теней уменьшается.

Далее будут подробно рассмотрены три этапа решения задачи о поиске положения объекта.

Фактически задача поиска тени на изображении тождественна задаче распознавания образов. В зависимости от условий варианты поиска могут различаться.

Самым простым, но далеко не самым редким случаем является случай с однородным фоном контролируемой территории. Однородным фоном может являться, например, стена в помещении или асфальт на улице. При этом тень на снимках просматривается достаточно ясно, и ее выявление может быть осуществлено с помощью пороговой фильтрации: зная цвет фона, можно выделить отличные от него объекты, просто определяя цвет каждого пикселя изображения. Если значение цвета для него меньше некоторого порогового, то пиксель помеча-

ется как содержащий тень, иначе – определяется как фон. Таким образом, процедуру поиска можно описать следующим образом:

$$\begin{cases} x<T, f(x)=1, \\ x>T, f(x)=0, \end{cases}$$

где x – яркость пикселя; T – пороговое значение [3]. В случае неоднородности фона существует два варианта решения проблемы. Первый – создание базы эталонных изображений, отснятых в «нормальных» условиях, т.е. при отсутствии посторонних объектов и их теней в кадре; второй – использование пороговой фильтрации с адаптивным определением порога либо поиск объекта методом *k*-средних.

Вариант с использованием эталонных изображений представляется простым и эффективным даже при неоднородном фоне, однако в случае изменяющейся освещенности (как, например, при уличном видеонаблюдении) приходится хранить достаточно объемную базу эталонов, соответствующих различным освещенностям. В остальных же случаях метод представляет собой не что иное, как попиксельное сравнение полученных изображений с эталоном.

Метод поиска теней с использованием адаптивной пороговой фильтрации полезен при однородном фоне, но неоднородной освещенности, т. к. позволяет вычислять порог автоматически для отдельных областей. Для автоматического определения порога необходимо построить гистограмму распределения яркостей пикселей. Пример такой гистограммы приведен на рис. 3.

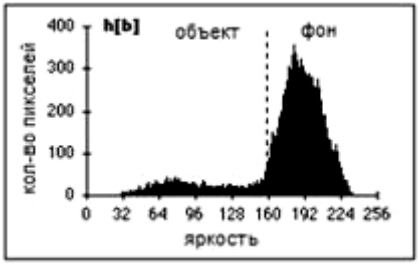


Рис. 3. Распределение яркостей объекта и фона на изображении

После построения гистограммы необходимо найти максимальную яркость $h_{\max}$. Далее на стороне диаграммы, не относящейся к объекту (в приведенном на рисунке случае – справа), найти яркость h_p, количество пикселей с яркостью $h>h_p$ равняется p (например 5%) от пикселей, яркости которых $h>h_{\max}$. После этого новое значение порога пересчитывается по формуле $T=h_{\max}-(h_p-h_{\max})$ [3].

Наиболее универсальным (однако не самым быстрым) способом обнаружения теней является метод *k*-средних. Алгоритм бинаризации изображения методом *k*-средних выглядит следующим образом:

1) выбирается порог T, равный середине диапазона яркостей;

2) вычисляется средняя яркость всех пикселей с яркостью меньшей чем T m_1 и m_2 для пикселей с яркостью большей чем T;

3) новый порог высчитывается по формуле $T_1 = (m_1 + m_2)/2$;

4) шаги 2 и 3 повторяются до тех пор, пока T не перестанет изменяться [3].

Вычисление реальных линейных размеров тени определяется исходя из размеров изображения и угла обзора видеокамеры. На рис. 4 показан примерный вид зоны видимости видеокамеры.

Очевидно, что расстояние a равно $a = 2L \cdot tg\left(\frac{\alpha}{2}\right)$. Таким образом, для определения реальных линейных размеров тени можно вычислить коэффициент пересчета, равный ширине изображения в пикселях, разделенной на реальную ширину наблюдаемой области:

$$k = \frac{width}{a} = \frac{width}{2L} \cdot tg\left(\frac{\alpha}{2}\right).$$

Зная реальные размеры теней объекта и расстояние от видеокамер до плоскости наблюдения, определение положения объекта в пространстве сводится к решению геометрической задачи [2].

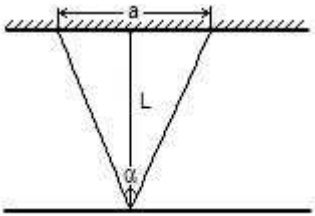


Рис. 4. Зона видимости видеокамеры

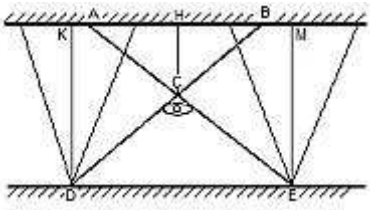


Рис. 5. Геометрическая интерпретация поиска объекта

На рис. 5 точки A и B соответствуют границам тени на изображениях. Из рисунка видно, что поиск расстояния от объекта до наблюдаемой плоскости сводится к поиску высоты CH треугольника ΔABC. DK и EM – перпендикуляры, опущенные из точек, где располагаются видеокамеры и источники света. Длина этих перпендикуляров известна из условия задачи. Также известны расстояния DE и AB, так как линейные размеры тени определены. Очевидно, что KB равно сумме половины ширины зоны видимости ($a/2$), расстояния между зонами видимости и расстоянию от края зоны видимости до

тени. Все эти величины являются либо известными, либо вычисленными. Тогда $BD=\sqrt{DK^2+KB^2}$. Аналогично находится AE. Исходя из подобия треугольников ΔABC и ΔCDE, можно записать $\frac{BC}{CD}=\frac{AB}{DE}$ или, обозначив BC за x, $\frac{x}{BD-x}=\frac{AB}{DE}\Rightarrow x=\frac{AB\cdot BD}{DE+AB}$. AC находится аналогично. Значение CH находится из системы уравнений:

$$\begin{cases} CH^2=AC^2-AH^2, \\ CH^2=BC^2-(AB-AH)^2. \end{cases}$$

Стоит заметить, что полученное в ходе решения системы расстояние AH позволяет найти расстояние от видеокамеры до объекта: $KH = KA + KH$. Повторив эту процедуру для случая, когда точки A и B являются противоположными границами тени, найдем расстояние от объекта до прямой DE. Таким образом, местоположение объекта будет определено.

В работе описан метод нахождения объекта по двум его теням. С его помощью можно добиться значительного увеличения контролируемой с помощью видеонаблюдения территории.

ЛИТЕРАТУРА

1. Лаврус В.С. Охранные системы. М.: Наука и техника, 1998.
2. Меженин А.В., Тозик В.Т. Реконструкция трехмерных моделей по растровым изображениям. СПб.: Научно-технический вестник СПБГУ ИТМО. № 45. С. 203–207.
3. Гонсалес Р., Вудс Р., Эддинс С. Цифровая обработка изображений в среде MathLab. М.: Техносфера, 2006. 616 с.

МЕТОД ОЦЕНКИ СХОДСТВА ЛИЦ НА ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ

А.В. Черепанов, курсант 5-го курса факультета информационной безопасности

г. Орел, Академия ФСО, т. 8-910-200-43-73, cherep_lion@mail.ru

В условиях повышения уровня угроз террористической активности, угроз безопасности личности криминогенного характера особую актуальность приобретает задача оценки сходства лиц на цифровых изображениях. При задании порога подобного сходства данная задача вырождается в задачу идентификации личности на основе фотоизо-

бражений, а при отсутствии порога – в задачу отбора и ранжирования фотоизображений по степени их сходства.

В большинстве случаев под идентификацией личности понимается процесс определения основных персональных данных применительно к неизвестному человеку. Классическое понимание термина «идентификация личности» в криминалистике связано с установлением соответствия между двумя объектами – трупом и прижизненной фотографией человека, фотографией разыскиваемого преступника и подозреваемым и т.д. [1]. Однако при решении широкого класса прикладных задач обеспечения безопасности и оперативно-следственной деятельности (обеспечение пропускного режима, установления личности на основе фото или видеоизображения и др.) понятие идентификации приобретает смысл установления соответствия между объектом-оригиналом и неизвестным объектом, зафиксированным посредством фото- или видеосъемки.

Формально прикладная задача оценки сходства лиц на цифровых изображениях требует математического решения задачи распознавания образа, в качестве которого выступает изображение лица человека.

В условиях, когда местоположение и ракурс лица на фото- или видеоизображении, характеристики яркости и контрастности элементов изображения могут изменяться в достаточно широком диапазоне, эффективность распознавания в значительной мере будет определяться вектором признаков объекта распознавания и процедурой их выделения. Это определяет актуальность задачи параметризации изображения лица, сущность которой состоит в выделении на произвольном фотоизображении такового вектора признаков, который позволяет установить соответствие объект–оригинал, представленного непосредственно или на другом фотоизображении лица.

Для решения данной задачи разработаны методы распознавания, основанные на теории нейронных сетей, корреляционно-экстремальные алгоритмы, методы вычислений статических и алгебраических моментов, контурный анализ, 3D-моделирование и др. [2]. Значительные практические результаты разработки систем идентификации личности по фотоизображениям появились в 90-х гг. и сразу начали вызывать интерес у армии и спецслужб. В результате полученные результаты не находят широкого освещения в доступных источниках, а сведения об эффективности разработанных алгоритмов не приводятся.

В этой связи появление эффективных систем идентификации личности на основе методов оценки сходства лиц на цифровых фото- и видеоизображениях для широкого круга прикладных задач во многом сдерживается отсутствием открытых алгоритмов данного класса.

В работе на основе анализа существующих подходов к решению задачи параметризации лица на фото- или видеоизображении предложен метод, позволяющий выделить информативный набор признаков, отражающих геометрию лица человека, предложен метод оценки сходства лиц на цифровых изображениях, проведена предварительная оценка его эффективности, а также показаны прикладные области его применения.

1. Описание существующих методов

В 1993 г. агентство DARPA и Исследовательская лаборатория армии США разработали программу Feret (face recognition technology). Цель программы – оценить эффективность алгоритмов распознавания лиц и стимулировать развитие лучших из них. В ходе реализации программы Feret три алгоритма продемонстрировали самый высокий уровень точности распознавания для больших баз данных (1200 человек) в наиболее сложных для распознавания условиях тестирования. Это алгоритм, разработанный в Университете Южной Калифорнии, алгоритм, созданный в Media Laboratory Массачусетского технологического института (МТИ), и алгоритм Университета штата Мэриленд. Первые два алгоритма накладывают минимальные ограничения на процедуры обнаружения и распознавания лиц, а последний предполагает обязательное приближение глаз.

Проведенный анализ публикаций в области распознавания изображений лиц позволил выделить следующие процедуры, основанные на соответствующих математических методах (рис. 1):

− преобразования исходного изображения в начальное представление (может включать в себя как предобработку, так и математические преобразования, например вычисление главных компонент);

− выделения ключевых характеристик (например, главные компоненты или коэффициенты дискретного косинусного преобразования);

− классификации (кластерная модель, метрика, нейронная сеть и др.).

Реализация перечисленных процедур опирается на априорную информацию о характеристиках лица человека и корректируется экспериментальной информацией, появляющейся по ходу реализации [3].

Первым этапом процесса распознавания является начальное представление изображения, включающее предобработку (нормализацию) и преобразование.

Наибольшее распространение в современных алгоритмах распознавания получил **метод главных компонент** (Principal Component Analysis, PCA), применяемый для сжатия информации без существенных потерь информативности. Он состоит в преобразовании входного вектора **X** размерности N в выходной вектор **Y** размерности M, где

$M < N$. При этом компоненты вектора **Y** являются некоррелированными, и общая дисперсия после преобразования остаётся неизменной.

Рис. 1. Классификация методов распознавания изображений

Применение метода главных компонент для задачи распознавания человека по изображению лица состоит в следующем. Входные вектору представляют собой отцентрированные и приведённые к единому масштабу изображения лиц. Собственные векторы, вычисленные для всего набора изображений лиц, называются собственными лицами (eigenfaces). Собственные лица имеют полезное свойство, заключающееся в том, что изображение, соответствующее каждому такому вектору, имеет лицеподобную форму (рис. 2). С помощью вычисленных ранее матриц входное изображение разлагается на набор линейных коэффициентов, называемых главными компонентами. Сумма главных компонент, умноженных на соответствующие собственные векторы, является реконструкцией изображения.

Рис. 2. Пример изображений собственных векторов (собственные лица)

Для каждого изображения лица вычисляются его главные компоненты. Обычно берётся от 5 до 200 главных компонент. Остальные компоненты кодируют мелкие различия между лицами и шум. Процесс распознавания заключается в сравнении главных компонент неизвестного изображения с компонентами всех остальных изображений. Для этого обычно применяют какую-либо метрику (простейший случай – Евклидово расстояние).

Линейный дискриминантный анализ (линейный дискриминант Фишера [4, 5], Linear Discriminant Analysis, LDA). Выбирают проекцию пространства изображений на пространство признаков таким образом, чтобы минимизировать внутриклассовое и максимизировать межклассовое расстояние в пространстве признаков. Так же, как и собственные векторы, изображения базисных дискриминантных векторов имеют лицеподобную форму.

Гибкие контурные модели лица. В данных методах распознавание производится на основе сравнения контуров лица. Контуры обычно извлекаются для линий головы, ушей, губ, носа, бровей и глаз. Контуры представлены ключевыми позициями, между которыми положения точек, принадлежащих контуру, вычисляются интерполированием. Для локализации контуров в различных методах используется как априорная информация, так и информация, полученная в результате анализа тренировочного набора.

Главной задачей при распознавании по контурам является правильное выделение этих контуров. В общем виде эта задача по сложности сравнима непосредственно с распознаванием изображений. Кроме того, использование этого метода самого по себе для задачи распознавания недостаточно.

На этапе выделения ключевых признаков следует выделить методы:

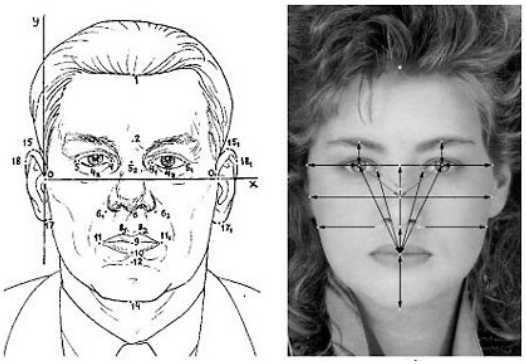
Метод первых главных компонент – является методом, рассмотренным ранее, где априорно задается количество главных компонент, извлекаемых из изображений.

Первые коэффициенты частотного преобразования. После проведения определенного преобразования (Фурье, косинусного, вейвлет) производится переход от картинки к спектральной интерпретации пространственных волн картинки. Затем из полученной матрицы коэффициентов выбираются первые коэффициенты.

Джеты – характеризуют локальные области изображений и служат для двух целей: во-первых, для нахождения точек соответствия в заданной области на двух различных изображениях; во-вторых, для сравнения двух соответствующих областей различных изображений.

Ключевые точки. Изначально применялся в криминалистике и был там детально разработан. Суть его заключается в выделении набо-

ра ключевых точек (или областей) лица и последующем выделении набора признаков. Каждый признак является либо расстоянием между ключевыми точками, либо отношением таких расстояний. Наборы наиболее информативных признаков выделяются экспериментально. Ключевыми точками могут быть уголки глаз, губ, кончик носа, центр глаза и т.п. (рис. 3). В качестве ключевых областей могут быть прямоугольные области, включающие глаза, нос, рот.



а *б*

Рис. 3. Идентификационные точки и расстояния: *а* – используемые при криминалистической фотоэкспертизе; *б* – наиболее часто применяемые при построении автоматизированных систем идентификации

В процессе распознавания сравниваются признаки неизвестного лица с признаками, хранящимися в базе.

Завершающим этапом является механизм классификации. В каждом конкретном случае он выбирается исходя из поставленных задач. Чаще всего применяется метрика (Евклидова) или Нейронная сеть.

Все представленные выше методы обладают определенными недостатками. Наиболее эффективные методы, такие как метод главных компонент, ключевые точки, можно применять в качестве базовых для комплексного подхода, что показано ниже.

2. Анализ функциональных возможностей существующих систем идентификации

Системы распознавания по лицу, присутствующие на рынке. Лидерами в настоящий момент являются следующие системы:

– коммерческая система (Viisage «FaceFinder»), созданная на базе алгоритма, разработанного в Университете Рокфеллера, – применяется в АНБ, Министерстве обороны США;

– система, созданная на базе МТИ (Visionic «FaceIt»), – применяется в Министерстве обороны США, Министерстве юстиции США, Министерстве обороны Израиля;

– ZN Vision Technologies AG (Германия) предлагает на рынке ряд продуктов, в которых применяется технология распознавания лиц. Эти системы представляются на российском рынке компанией «Солинг»;

– в системе распознавания лиц «TrueFace» компании Miros используется технология нейронных сетей, а сама система применяется в комплексе выдачи наличных денег корпорации Mr. Payroll и установлена в казино и других увеселительных заведениях многих штатов США.

В США независимыми экспертами было проведено сравнительное тестирование различных технологий распознавания лиц. Результаты тестирования представлены на рис. 4 [6].

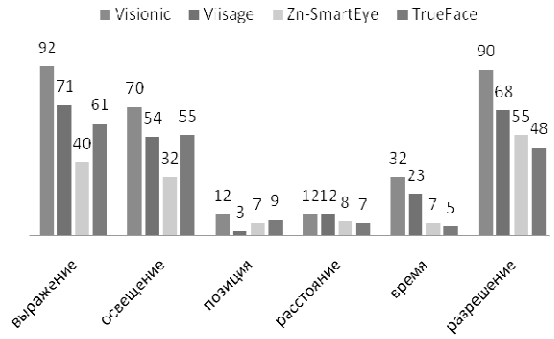


Рис. 4. Сравнительный анализ эффективности распознавания лиц в различных системах

Частная компания Yano Research Institute обнародовала информацию о том, что объем национального рынка биометрических систем контроля достиг по итогам 2004 г. 79,5 млн долл. США, что на 39% больше, чем два года назад. По прогнозам аналитиков, к 2010 г. отрасль разрастется до 245 млн долл. США, что связывается с адаптацией биометрических систем идентификации под мобильные телефоны и портативные компьютеры [7]. Представленная информация позволяет сделать вывод об экономической эффективности вложения денег в научные разработки биометрических систем.

3. Метод оценки сходства лиц на цифровых изображениях

Каждый из существующих методов, реализованных в системах распознавания по лицу, присутствующих на рынке, обладает опреде-

ленными недостатками: не позволяет автоматически распознавать (гибкие контурные модели лица); вычислительная сложность (Марковские модели) и так далее. Для устранения выявленных недостатков необходимо применять комплексный подход [8], на основании которого разработан метод оценки сходства лиц, представленный на рис. 5.

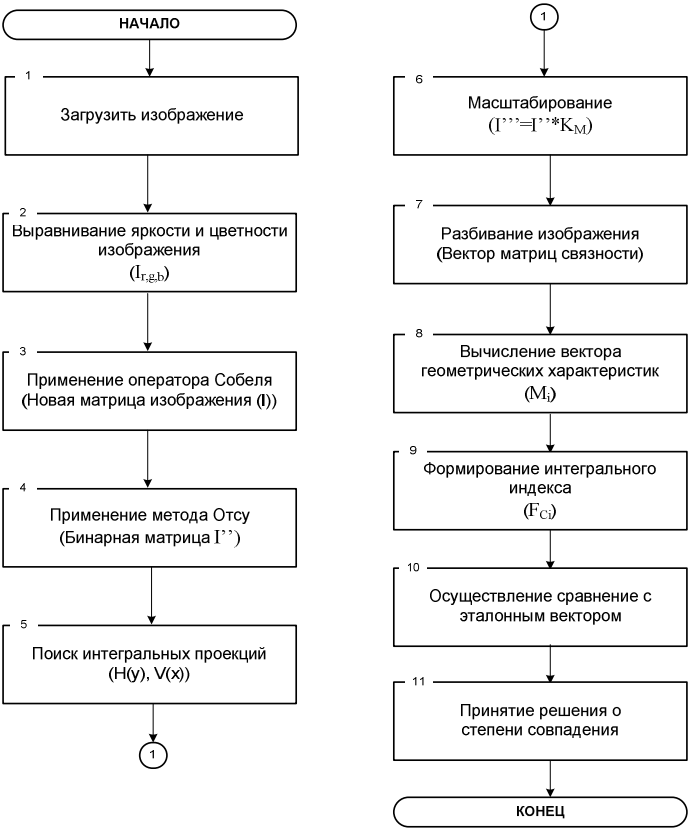


Рис. 5. Метод оценки сходства лиц на цифровых изображениях

Алгоритм метода идентификации личности человека по цифровому изображению лица:

Блок № 1 – загрузка изображения. Производится посредством устройства считывания цифровой информации (фотоаппарат, сканер, видеокамера (считывание происходит покадрово) с объекта.

Блок № 2 – ищутся минимальная и максимальная яркость, на их основании выравнивается яркость по всему спектру. Аналогично выравнивается по каждому цвету.

Блок № 3 – применяется оператор Собеля. Создается тоновая (255 цветов) матрица (1)

$$E_{i,j} = \lfloor ((I_R)_{i,j} + (I_G)_{i,j} + (I_B)_{i,j})/3 \rfloor, \quad (1)$$

где $(I_R)_{i,j}$, $(I_G)_{i,j}$, $(I_B)_{i,j}$ – значение интенсивности цвета (соответственно, красный, зеленый, голубой) в точке с координатами $x = i, y = j$ $i = 1..H, y = 1..W$.

Применяются два фильтра (S_v, S_h) (2,3), которые позволяют очистить изображение от шумов:

$$\begin{aligned}(S_v)_{i,j} = {} & (-1)\cdot E_{i-1,j-1} + (-2)\cdot E_{i,j-1} + \\ & + (-1)\cdot E_{i+1,j-1} + (1)\cdot E_{i-1,j+1} + \\ & + (2)\cdot E_{i,j+1} + (1)\cdot E_{i+1,j+1}; \end{aligned} \quad (2)$$

$$\begin{aligned}(S_h)_{i,j} = {} & (-1)\cdot E_{i-1,j-1} + (-2)\cdot E_{i-1,j} + \\ & + (-1)\cdot E_{i-1,j+1} + (1)\cdot E_{i+1,j-1} + \\ & + (2)\cdot E_{i+1,j} + (1)\cdot E_{i+1,j+1}, \end{aligned} \quad (3)$$

где $E_{i,j}$ – значение интенсивности в точке с координатами $x = i, y = j$ $i = 1..H, y = 1..W$; H, W – значение ширины и высоты изображения соответственно; $(S_v)_{i,j}$ – значение применения фильтра устранения вертикальных шумов; $(S_h)_{i,j}$ – значение применения фильтра устранения горизонтальных шумов.

Затем вычисляется свертка применения данных фильтров (4)

$$I_{i,j} = \sqrt{((S_h)_{i,j} \otimes E_{i,j})^2 + ((S_v)_{i,j} \otimes E_{i,j})^2}. \quad (4)$$

На выходе получаем новую матрицу изображения (I).

Блок № 4 – Применяется метод Отсу [9] (5). Метод заключается в бинаризации изображения по заданному граничному параметру T^{opt}:

$$I''_{i,j} = \begin{cases} 0, I_{i,j}' \le T^{opt}, \\ 1, I_{i,j}' > T^{opt}. \end{cases} \quad (5)$$

Граница бинаризации T^{opt} (6) вычисляется на основании интегральной освещенности изображения (7)

$$T^{opt} = 0{,}5 \cdot IO, \quad (6)$$

$$IO = \frac{\sum_i \sum_j I_{i,j}}{i * j}, \quad (7)$$

интегральная освещенность вычисляется как сумма интенсивностей всех пикселей изображения, нормированная на их количество.

Блок № 5 – поиск интегральных проекций. Нахождение интегральных проекций по каждой из осей производится по выражениям (8), (9):

$$H(y) = \sum_{x=x_1}^{x_2} I(x,y), \quad (8)$$

$$V(x) = \sum_{y=y_1}^{y_2} I(x,y), \quad (9)$$

где $I(x,y)$ – значение интенсивности изображения в точке с координатами *x, y*; x_1, x_2 – крайние значения координат изображения по ширине; y_1, y_2 – крайние значения координат изображения по высоте; $H(y)$ – массив значений горизонтальных проекций по высоте; $V(x)$ – массив значений вертикальной проекции по ширине.

Блок № 6 – масштабирование по всплескам интегральных проекций на ось OX и априорной информации о средней ширине лица. Значение пропорционального коэффициента масштабирования (K_M) изображения масштаба вычисляется как (10)

$$K_M = \frac{\left|\arg(\max_1(V(x)) - \arg(\max_2(V(x))\right|}{H_a}, \quad (10)$$

где H_a – значение априорного значения ширины лица, должно применяться одинаковое значение для всех изображений; $\max_1(V(x))$, $\max_2(V(x))$ – первые два максимума в $V(x)$, и по ним определяется пропорциональный показатель масштабирования изображения.

Блок № 7 – разбивают изображение. Сегментация изображения является алгоритмически сложной процедурой. Применяется подход к сегментации по связности элементов, согласно которому единичные значения бинарной матрицы изображения объединяются в один класс, если они связаны между собой (рассматриваются по квадрату, с шириной 3). На выходе данной процедуры имеется кортеж объектов, т.е. полученный массив матриц связности, которые фактически являются элементами лица. Данная процедура разбиения является новой, основывается на теории кластерного анализа при отсутствии априорно заданного количества кластеров.

Блок № 8 – вычисляется вектор геометрических характеристик. Из полученных матриц связности извлекаются значения координат крайних точек и рассчитываются геометрические расстояния между ними, площади. На основании координат крайних точек объектов получаются геометрические характеристики лица. Выходной вектор параметров (M_i) является итогом извлечения.

Блок № 9 – формируется интегральный индекс. Данный индекс формируется на основании вектора значений, в зависимости от выбранной метрики (Евклидова, Городская и др.). Используя Евклидову метрику, интегральный индекс (Fc_i) вычисляется по выражению (11). Данный индекс применяется для повышения оперативности сравнения при наличии нескольких объектов сравнения:

$$Fc_i = \sqrt{\sum_j (M_{i,j})^2} \ , \qquad (11)$$

где $M_{i,j}$ – значение *j* геометрической характеристики *i* объекта.

Блок № 10 – осуществление сравнения с эталонным вектором. Загружается вектор эталонного изображения (полученный ранее таким же методом) и производится последовательное покомпонентное сравнение (12):

$$\mathbf{T}_j = \left| M_{\text{эталонное } j} - M_{\text{искомое } j} \right| , \qquad (12)$$

где **T** – вектор различий компонент.

Блок № 11 – принятие решений о степени совпадения. Путем аддитивной свертки вектора **T** вычисляется SX – обобщенный индекс сходства (13):

$$\text{SX} = \sum \mathbf{T}_i \, . \qquad (13)$$

Задав априорный порог совпадения, принимается решение о соответствии, и метод оценки сходства вырождается в метод идентификации лиц на основании цифрового изображения лица.

Таким образом, предложенный метод оценки сходства лиц на цифровых изображениях обеспечивает устойчивое формирование вектора признаков цифрового изображения лица в условиях естественной зашумленности изображения и разных ракурсов, что позволяет оценить сходство лиц с требуемым уровнем точности и оперативности.

4. Оценка эффективности метода оценки сходства лиц на цифровых изображениях и его практические приложения

Для оценки эффективности метода была взята ORL-база, специально созданная для тестирования программ распознавания лиц. База ORL содержит 400 изображений 40 человек – по 10 изображений каждого. Для каждого эксперимента база делилась на две части – обучаю-

щую и тестовую, по пять изображений одного человека в каждой части. Исследовались возможности распознавания на основе метода оценки сходства лиц на цифровых изображениях на базе алгоритма параметризации фотоизображения лица для идентификации личности [8].

Реализация и экспериментальная оценка алгоритма, основанного на предлагаемом методе оценки сходства изображений лиц, показывают возможность повышения точности соответствующих процедур распознавания до 92%. Точность распознавания зависит от того, какие изображения попадут в обучающую выборку при очередном разделении. Если в обучающей выборке нет изображения лица при аналогичных условиях (ракурса, например), то система имеет тенденцию ошибаться.

При проведении другого эксперимента база разбивалась на три набора, причём из третьего набора классов примеров в обучающей выборке не было. Метод параметризации фотоизображения лица для идентификации личности показал достаточно хорошие результаты, хотя потребовал подстройки порога свой–чужой для сравнения векторов. В итоге в зависимости от разбиения базы точность отнесения к классам менялась с 90 до 92%.

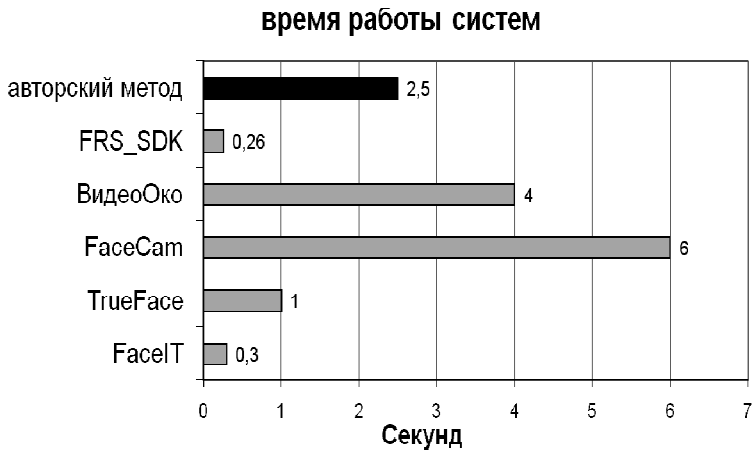


Рис. 6. Сравнительный анализ времени работы процедуры оценки схожести лиц в различных системах

Сравнительный анализ времени работы процедуры оценки схожести лиц в различных системах, при размере изображения 314×225, по-

казывает, что авторский метод по скорости работы превосходит коммерческие системы ВидеоОко, FaceCam, но уступает системам FaceIT, TrueFac (рис. 6) [9]. Это связано с различием в использовании методов параметризации лиц, что также влияет на точность распознавания.

По результатам тестирования авторского метода оценки сходства лиц по цифровым изображениям видно, что он обладает высокой скоростью работы, точностью распознавания, превышающей многие коммерческие системы, а также может быть использован для решения широкого класса задач, за счет извлечения контента (геометрических характеристик лица).

Выводы. В работе рассмотрены существующие методы идентификации изображения, их характеристики и проведен анализ существующих систем идентификации личности. Предложен комплексный подход для решения задачи оценки сходства лиц на цифровых изображениях, который позволил разработать метод параметризации на фото- или видеоизображении в задачах оценки сходства лиц, имеющий характеристики, сопоставимые с современным уровнем систем, существующих на рынке. Разработан метод оценки сходства лиц на цифровых изображениях. Проведено тестирование метода на базе созданного прототипа.

Достоверность полученных результатов подтверждается применением формальных математических методов решения, экспериментальной оценкой эффективности применения разработанного метода, апробацией на научных конференциях.

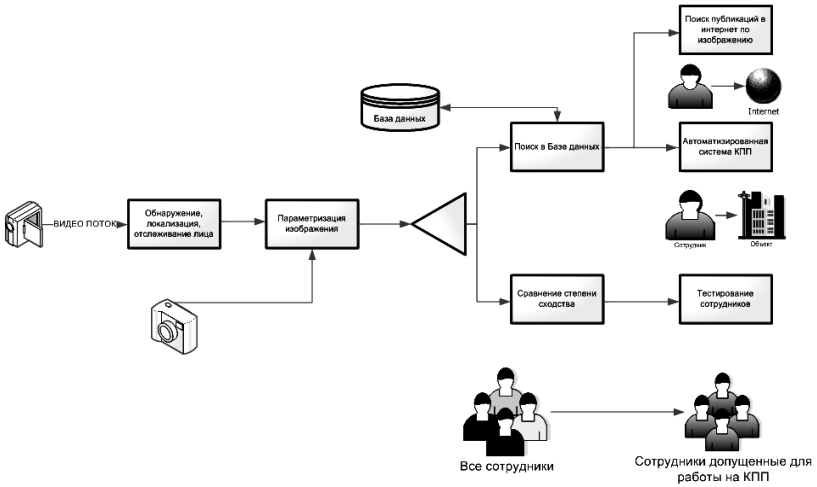


Рис. 7. Варианты использования системы

Научная новизна представляемой работы, определяется разработкой прикладного решения на основе комплексного использования наиболее результативных в области обработки цифровых изображений математических методов и процедур. Разработана авторская процедура разбиения изображения. Полученный в результате метод оценки сходства лица обеспечивает устойчивое распознавание лица человека в условиях естественной зашумленности изображения и различных ракурсов съемки и оценку сходства.

Практической ценностью работы является возможность применять метод для широкого класса прикладных задач (установление идентичности личности на разных цифровых изображениях, поиск публикаций в Интернете по фотоизображению, подбор персонала для работы на контрольно-пропускных пунктах и др.) (рис. 7).

ЛИТЕРАТУРА

1. Самищенко С.С. Судебная медицина: Учебник для юридических вузов. М., 2006.

2. Глазунов А.С. и др. Компьютерное распознавание человеческих лиц // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. 1997. № 8. С. 3–14.

3. Брилюк Д., Старовойтов В. Распознавание человека по изображению лица и нейросетевые методы. Минск: ИТК НАНБ, 2001. 54 с.

4. Belhumeur P.N., Hespanha J.P., Kriegman D.J. Eigenfaces vs Fisherfaces: Recognition Using Class Specific Linear Projection. // IEEE Transactions on Pattern Analysis and Machine Intelligence. 1997. Vol. 19. P. 711–720.

5. Lanitis A., Taylor C.J., Cootes T.F. Automatic Interpretation and Coding of Face Images Using Flexible Models // IEEE Transactions on Pattern Analysis and Machine Intelligence. 1997. Vol. 19. P. 743–756.

6. Татарченко Н.В., Тимошенко С.В. Биометрическая идентификация в интегрированных системах безопасности // Специальная техника. 2002. № 2.

7. Заславская В. Мировой рынок биометрических систем к 2008 году достигнет 4,6 млрд. долларов США – http://security.compulenta.ru/222414 – Доступно на сервере журнала «Компьютерра»: http://compulenta.ru [14.05.2008].

8. Бочков М.В., Черепанов А.В. Алгоритм параметризации цифрового изображения лица // Труды «I Всероссийской научно-технической конференции «Современные информационные технологии в деятельности органов государственной власти». Курск, КГТУ, 2008.

9. Самаль Д.И. Алгоритмы идентификации человека по фотопортрету на основе геометрических преобразований: дисс. … канд. техн. наук. Минск, 2002. 167 с.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ АНАЛИЗА ПРОЦЕССОВ

М.Ю. Дьяконов, аспирант каф. ВТиЗИ

г. Уфа, УГАТУ, т. 8-927-237-77-60, dyakonov_maksim@mail.ru

Множество современных средств защиты (антивирусы, фаерволы, системы обнаружения/предотвращения вторжений) используют сигнатурные методы обнаружения вредоносного кода и/или различные эвристики. Несмотря на их огромную значимость для задачи эффективной защиты информации, рассмотрим другую технологию, основанную не на сигнатурных методах обнаружения, а на поведенческом анализе ПО.

На рис. 1 приведена классификация методов обнаружения аномалий, рассматриваемых в работах [1–10]. Элементы классификации приведены в следующем порядке:

– информация, используемая для построения модели представления;

– модель представления (математическая модель);

– способ мониторинга.

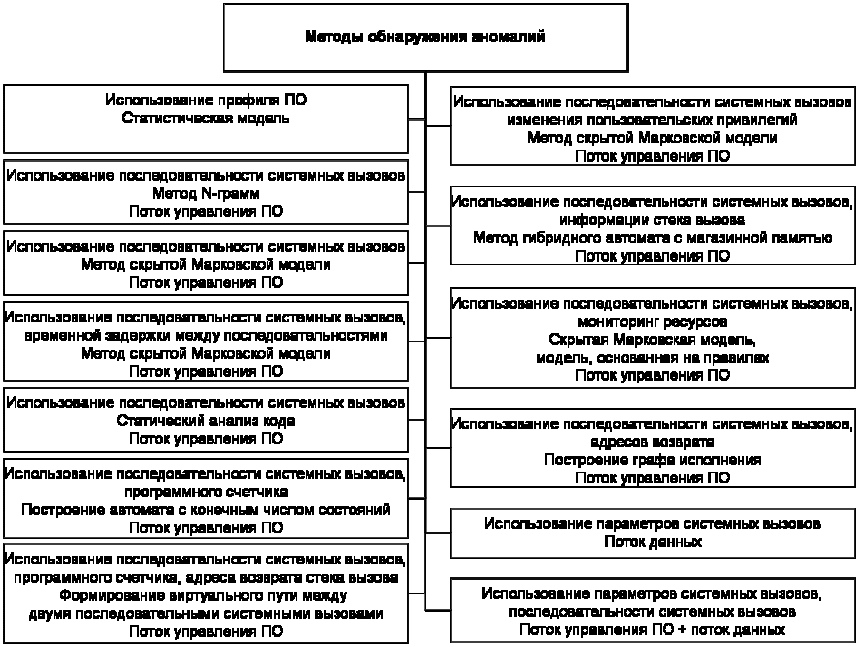


Рис. 1. Методы обнаружения аномалий

Мониторинг поведения процессов. При использовании динамического или статического анализа программного кода возникают два случая, приводящие к затруднениям при мониторинге ПО во время исполнения, а также приводящие к ошибкам классификации.

1) При использовании динамического анализа в режиме обучения возникает сложность построения всех возможных путей исполнения кода ПО. В связи с этим полученное множество является неполным и в режиме мониторинга приводит к значительным ошибкам первого и второго рода.

2) При использовании статического анализа возникают две основные проблемы: недоступность исходного кода ПО, а также обфускационные методы, используемые разработчиками ПО для сокрытия алгоритмов работы.

Первую проблему обычно решают с использованием дизассемблирования кода. Вторая проблема несколько сложнее и решается с использованием интерактивных средств отладки. В этих двух случаях задействован человек-эксперт, причем достаточно высокой квалификации. При этом часть анализа производится вручную даже для сравнительно небольшого объема кода.

Как известно из [11], основной единицей в операционной системе (ОС) является процесс. Процесс для ОС представляется в общем случае как совокупность нескольких составляющих:

1) Логическое представление процесса в ОС в виде структур данных, содержащих необходимую информацию для управления потоком исполнения, областями адресного пространства, обеспечения планирования, сохранения контекста исполнения и т.д.

2) Физически процесс представлен как бинарный образ программы, располагающийся в оперативной памяти компьютера.

При этом представляется возможным построение некоторой спецификации ПО, которая будет содержать информацию о возможных разрешенных потоках кода ПО, возникающих во время исполнения. Наибольший интерес представляют функции кода, в которых происходит вызов системных служб.

При совершении системного вызова формируется контекст вызова C_{ij}, который представляет собой адреса возврата в вызывающие функции [4]. С точки зрения поведения программы интерес представляют переходы, совершаемые при вызове служб ядра ОС: два последовательно совершаемых системных вызовов. Так как только ядро способно управлять системными вызовами и через них предоставлять доступ к различным ресурсам [11], то через него возможно осуществлять контроль за поведением программы.

В качестве примера можно привести цепочку системных вызовов (рис. 2).

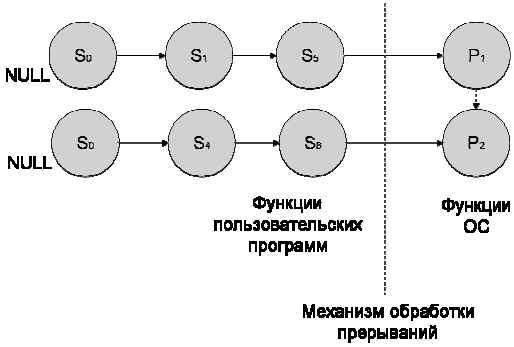


Рис. 2. Цепочка вызовов

Таким образом, при последовательном совершении системных вызовов P_1 и P_2, они будут характеризоваться совокупностью контекстов: P_1C_5, C_{51}, C_{10}, C_{04}, C_{46}, C_6P_2.

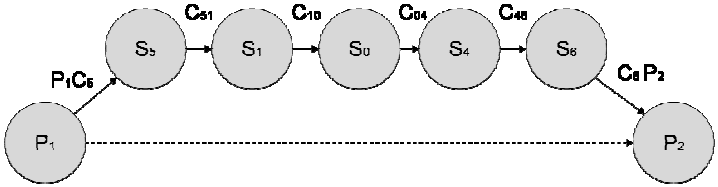
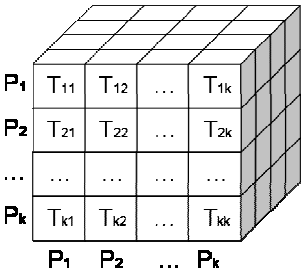


Рис. 3. Совокупность контекстов

В итоге для двух данных системных вызовов можно получить характерные паттерны поведения. Для примера: на рис. 3 паттерном будет являться следующее упорядоченное множество:

$$T^{i}_{p1p2} = \langle P_1C_5, C_{51}, C_{10}, C_{04}, C_{46}, C_6P_2 \rangle,$$



где $i = 1 \div n$, n – число паттернов при последовательном совершении системных вызовов P_1, а затем P_2.

Полное множество паттернов исполнения программного кода представлено на рис. 4.

Рис. 4. Полное множество паттернов системных вызовов

Совокупность всех возможных паттернов позволяет классифицировать поведение программы на нормальное (обычное) и аномальное – в случае воздействия вредоносного кода на ОС. В качестве классификатора можно использовать самоорганизующиеся карты Кохонена.

Сбор статистики поведения процессов и классификация состояний на основе самоорганизующихся карт Кохонена. Система сбора статистики и классификации состояний представляет собой специально разработанный модуль, встраиваемый в микроядро ОС (прототип модуля встраивается в ОС Minix3). Структура модуля представлена на рис. 5.

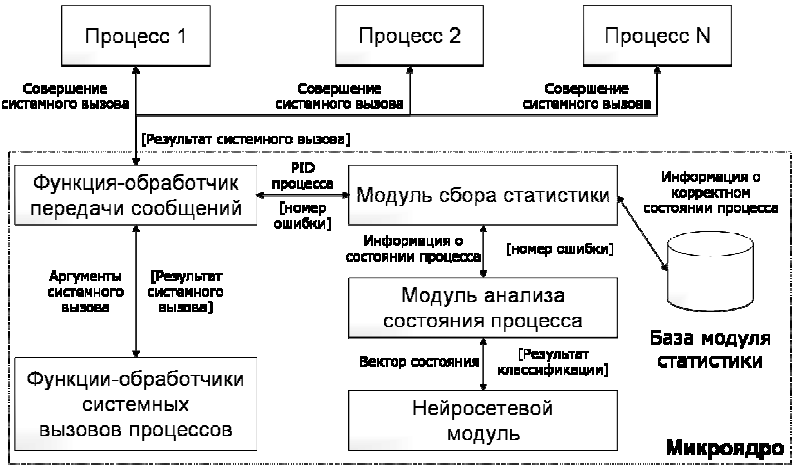


Рис. 5. Структура модуля сбора статистики и классификации

Модуль осуществляет сбор статистики совершения системных вызовов процессами с соответствующими им контекстами. Далее в режиме off-line проводится обучение сети.

Моделирование самоорганизующихся карт проводилось в пакете Matlab с использованием модуля расширения somtoolbox [12]. Исходные данные для обучения самоорганизующейся сети Кохонена представлены в табл. 1

Таблица 1

Исходные данные для обучения сети

Количество кластеров	Количество входных векторов	Размерность вектора	Функция окрестности	Алгоритм обучения
4	211	14	Гауссова	Пакетный с указанием меток

Результаты моделирования приведены на рис. 6–8.

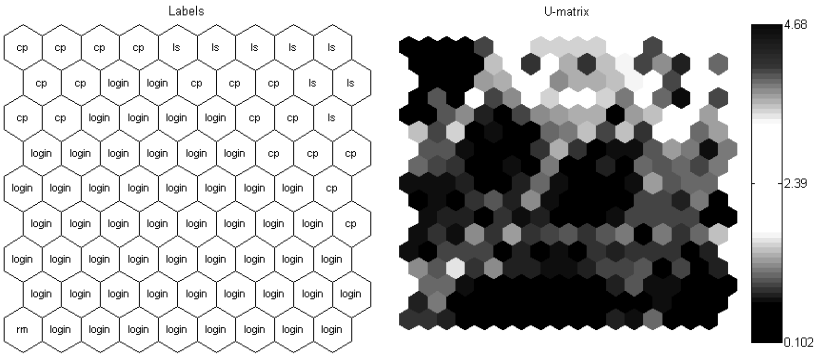


Рис. 6. Результаты обучения сети 9x9

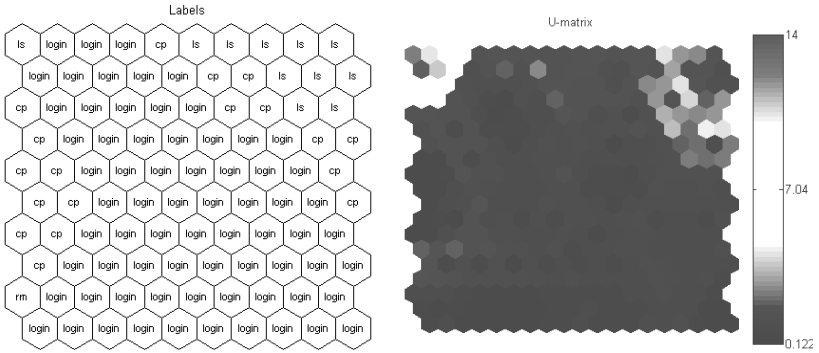


Рис. 7. Результаты обучения сети 10x10

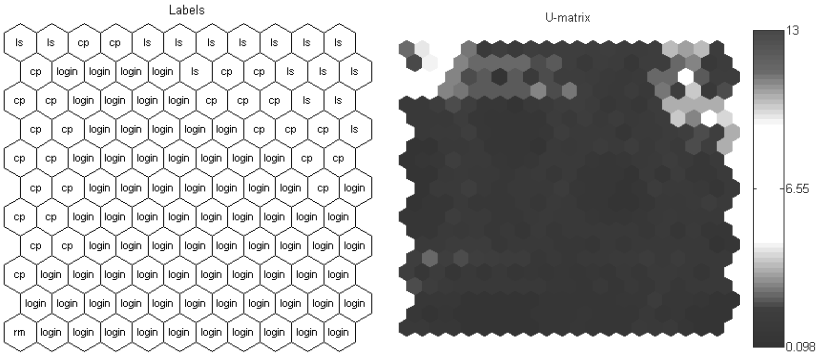


Рис. 8. Результаты обучения сети 11×11

Таким образом, результаты можно представить в табл. 2.

Таблица 2

Итоговые результаты классификации

Наименование процесса	Количество входных векторов	Сеть 9×9	
		Верно классифицированные, %	Ошибочно классифицированные, %
cp	44	92,68	7,32
rm	9	78	22
ls	18	89	11
login	139	100	0
Наименование процесса	Количество входных векторов	Сеть 10×10	
		Верно классифицированные, %	Ошибочно классифицированные, %
cp	44	90,9	9,1
rm	9	88	12
ls	18	94,5	5,5
login	139	100	0
Наименование процесса	Количество входных векторов	Сеть 11×11	
		Верно классифицированные, %	Ошибочно классифицированные, %
cp	44	93,2	6,8
rm	9	88	12
ls	18	94,5	5,5
login	139	100	0

Из таблицы можно сделать вывод, что при достаточном объеме статистики поведения процессов (login, ls) результаты классификации оказываются весьма неплохими.

Выводы. В результате проведения исследований был создан исследовательский прототип в ОС Minix3, позволяющий эффективно осуществлять сбор статистики поведения процессов на уровне ядра ОС. Проведено обучение сети на примере поведения нескольких процессов. Результат классификации сетью показал достаточно эффективную работоспособность данного метода.

Основными преимуществами подхода являются: отсутствие необходимости обновления сигнатурных баз; отсутствие каких-либо эмпирических правил для обнаружения аномального поведения; высокая эффективность защиты, связанная со встраиванием системы в ядро ОС.

Основными недостатками на данном этапе являются: для обучения сети требуется достаточно большой объем статистики поведения процессов; обучение нейросетевого классификатора необходимо производить в режиме off-line.

ЛИТЕРАТУРА

1. Anderson D., Lunt T., Javitz H., Tamaru A., Valdes A. Detecting unusual program behavior using statistical component of next-generation intrusion detection expert system (NIDES), SRI-CSL-95-06. May 1995.
2. Forrest S., Hofmeyr S.A., Somayaji A., Longstaff T.A. A sense of self for UNIX processes // *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, Los Alamitos, CA, IEEE Computer Society Press. 1996. P. 120–128.
3. Warrender C., Forrest S., Pearlmutter B. Detecting Intrusions Using System Calls: Alternative Data Models // *IEEE Symposium on Security and Privacy*. 1999. P. 133–145.
4. Feng H., Kolesnikov O., Fogla P. et al. Anomaly detection using call stack information // IEEE Symposium on Security and Privacy, Berkley, California, IEEE Computer Society, 2003.
5. Cho S., Park H. «Efficient anomaly detection by modeling privilege flows with hidden Markov model», Computers&Security. 2003. Vol. 22. № 1. P. 45–55.
6. Han S., Cho S. Rule-based integration of multiple measure-models for effective intrusion detection // IEEE International Conference on Systems, Man and Cybernatics. 2003.Vol. 1. P. 120–135.
7. Gao D., Reiter M., Song D. Gray-box extraction of execution graphs for anomaly detection // ACM Conference on Computer and Communications Security. 2004. P. 318–329.
8. Vigna G., Mutz D., Valeur F., Krugel C. On the detection of Anomalous System Call Arguments // Proceeding of the 8th European Symposium on Research in Computer Security, ESORICS-03, Gjovik, Norway. P. 101–118.
9. Vigna G., Krugel C., Robertson W. A multi-model approach to the detection of web-based attacks // International Journal of Computer and Telecommunication Networking. 2005. August. Vol. 48. № 5. P. 717–738.
10. Sekar R., Bhatkar S., Chatuverdi A. Dataflow Anomaly Detection // IEEE Symposium on Security and Privacy. May 2006.
11. Таненбаум Э., Вудхалл А. Операционные системы. Разработка и реализация (+CD). Классика CS. 3-е изд. СПб.: Питер, 2007. 704 с.
12. http://www.cis.hut.fi/projects/somtoolbox/

РАЗРАБОТКА МЕТОДА СИНТЕЗА ГЛАВНЫХ КОМПОНЕНТ ДЛЯ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ

А.В. Мокеев, аспирант каф. ТГСВ

г. Челябинск, ТГСВ, т. 8-952-506-73-33, gr.smk@mail.ru

В работе рассматривается задача распознавания изображений, которая базируется на методе главных компонент. Рассматриваемая задача включает несколько этапов: предварительная обработка изображения, построение матрицы изображений/ковариационной матрицы, вычисление собственных значений матрицы, редуцирование исходной матрицы изображений. Основное внимание уделяется решению задачи

редуцирования пространства признаков изображений методом главных компонент. Предлагаются новый метод нахождения главных компонент, базирующийся на решении задачи по частям. Матрица изображений представляется в виде набора матриц, каждая из которых имеет небольшой ранг. Полное решение получается путем синтеза частных решений.

В настоящее время активно развиваются биометрические технологии, направленные на получение и использование биометрических данных человека в целях его идентификации. Системы, использующие такие технологии, могут применяться в различных областях информационной безопасности: системах паспортного контроля в аэропортах и других крупных транспортных узлах, системах электронной торговли, системах наблюдения для снижения террористических угроз и розыска людей [1, 2]. Существенным преимуществом распознавания по лицу перед другими биометрическими методами является возможность идентификации на расстоянии.

Эффективным направлением развития технологий анализа изображений является комбинирование различных методов, таких как линейный дискриминантный анализ, метод главных компонент и нейросетевые методы. Основной задачей такого синтеза является развитие и построение интеллектуальных технологий, позволяющих построить модель, при помощи которой можно быстро распознавать изображения, осуществлять их поиск в базе изображений, и т.п. В настоящее время одним из наиболее мощных и универсальных средств анализа является метод главных компонент, который позволяет, не отбрасывая конкретные признаки, учитывать лишь наиболее значимые комбинации их значений [1, 3].

В случае большого числа изображений получение главных компонент на базе ковариационной матрицы всех изображений представляет существенные трудности. Это связано с тем, что матрица изображений (ковариационная матрица) может иметь большой ранг, и методы нахождения собственных векторов оказываются неэффективными. Поэтому в качестве главных компонент используется набор собственных векторов, полученный на основе обучающей выборки, которая имеет небольшой ранг. Учитывая тот факт, что выбранное изображение сначала раскладывалось по главным компонентам, а затем по ним производился поиск, ошибка распознавания прямо зависит от погрешности разложения как выбранного, так и хранящихся в базе изображений. На основе вышесказанного можно отметить, что хотя алгоритм распознавания изображений, представленных комбинацией собственных векторов, и является относительно быстрым и практичным, но при

его работе с большими базами данных могут появиться проблемы с точностью.

Для устранения этих недостатков в работе особое внимание уделяется решению задачи нахождения собственных значений больших матриц. Среди методов решения проблемы собственных значений можно выделить следующие группы: итерационные и преобразования подобия [4]. Методы преобразований подобия применяется с целью получить из исходной матрицы новую с теми же собственными значениями, но более простого вида. Наиболее известными являются методы Якоби, Гивенса и Хаусхолдера. Метод Хаусхолдера позволяет получить требуемый результат быстрее, чем метод Гивенса, так как связан с выполнением меньшего числа хотя и более сложных преобразований. Эффективным методом определения небольшого числа наибольших собственных значений является степенной метод, или метод прямых итераций. Однако на быстроту сходимости решения влияет отношение величины искомого собственного значения к ближайшему собственному значению. Если это отношение близко к единице, то сходимость оказывается медленной. Также скорость сходимости итерационного процесса зависит от того, насколько удачно выбран начальный вектор.

В данной работе рассматривается новый метод нахождения собственных векторов больших матриц, базирующийся на решении задачи собственных значений по частям. Предлагается разбивать матрицу отцентрированных изображений на подматрицы, каждая из которых имеет небольшой ранг. Это позволяет быстро находить частные решения. Полное решение получается путем синтеза частных решений.

Метод главных компонент. Пусть имеется набор образов, каждый из которых описывается вектором x_i, где i – номер образа (i = 1, 2, 3,..., m). Размерность вектора x_i равняется числу пикселей образа (n). Таким образом, все образы можно представить в виде матрицы $\mathbf{X}$, строками которого являются векторы x_i. Размерность пространства образов определяется произведением $n \times m$. Основная проблема анализа такого пространства заключается в его высокой размерности для реальных задач. Например, для набора из 10 000 черно-белых образов, каждый из которых 100×100 пикселей, размерность пространства равна 10 000×10 000.

Пространство образов центрируется относительно среднеарифметического вектора, который вычисляется по формуле

$$\bar{x} = \frac{1}{M} \sum_{i}^{M} x_i \ . \qquad (1)$$

При этом приходим к новому пространству векторов $\mathbf{X}^0$, строками которого являются векторы $x_i^0 = x_i - \bar{x}$.

Основная формулировка метода главных компонент предполагает вычисление ковариационной матрицы $\mathbf{A} = \frac{1}{m}\mathbf{X}^0(\mathbf{X}^0)^T$ и нахождение собственных значений и собственных векторов уравнения

$$(\mathbf{A} - \lambda\mathbf{I})v_0 = 0, \quad (2)$$

где $\mathbf{I}$ – единичная матрица; v_{0i} – собственный вектор; λ_i – собственное значение; индекс «Т» означает транспонирование матрицы. Матрица $\mathbf{A}$ имеет порядок $n \times n$. Матрица собственных векторов формируется из r собственных векторов, которым соответствуют наибольшие собственные значения:

$$\mathbf{V} = [v_{01} v_{02} ... v_{0r}]. \quad (3)$$

В связи с тем, что порядок матрицы $\mathbf{A}$ высокий, его решение представляет существенные трудности. Поэтому, как правило, используется дуальная формулировка метода главных компонент, в соответствии с которой вычисляется матрица Грамма $\mathbf{A}^* = \frac{1}{m}(\mathbf{X}^0)^T\mathbf{X}^0$. Матрица $\mathbf{A}^*$ имеет порядок $m \times m$, при этом m существенно меньше n. Для вычисления главных компонент необходимо найти собственные значения и соответствующие им собственные векторы матричного уравнения

$$(\mathbf{A}^* - \lambda\mathbf{I})u_0 = 0, \quad (4)$$

где u_{0i} – собственный вектор; λ_i – собственное значение. Следует отметить, что собственные значения уравнений (2) и (4) совпадают. После сортировки собственных значений формируется матрица собственных векторов, которым соответствуют r первых наибольших собственных значений:

$$\mathbf{U} = [u_{01} u_{02} ... u_{0r}]. \quad (5)$$

Известно, что матрицу $\mathbf{X}^0$ можно представить в виде сингулярного разложения

$$\mathbf{X}^0 = \mathbf{U}\mathbf{T}\mathbf{V}^T, \quad (6)$$

где $\mathbf{V}$ – матрица собственных векторов уравнения (2), столбцы которой ортонормированны, т.е. $\mathbf{V}^T\mathbf{V} = \mathbf{I}$; $\mathbf{U}$ – матрица собственных векторов уравнения (4) с ортонормированными столбцами, т.е. $\mathbf{U}^T\mathbf{U} = \mathbf{I}$; $\mathbf{T}$ – диагональная матрица порядка $r \times r$, диагональные

элементы которой $\eta_1,\eta_2,...,\eta_r$ называются сингулярными числами матрицы $\mathbf{X}^0$. Здесь r – ранг матрицы $\mathbf{X}^0$. Чаще всего $r=m$, но приводимый ниже результат охватывает общий случай, он справедлив и при условии $r<m$. Собственные значения матрицы $\mathbf{X}^0$ связаны с собственными значениями матрицы $\mathbf{A}$ соотношением

$$\eta_i=(m\lambda_i)^{1/2}.$$

Вычисляем матрицу собственных векторов $\mathbf{V}$. Для этого выражение (6) умножим справа на транспонированную матрицу $\mathbf{U}$ и матрицу T^{-1}. Далее, используя свойство ортогональности матрицы $\mathbf{U}$, получим

$$\mathbf{V}^T=\mathbf{T}^{-1}\mathbf{U}^T\mathbf{X}^0. \qquad (7)$$

Каждый вектор пространства $\mathbf{X}^0$ теперь может быть представлен в редуцированном пространстве, т.е.

$$x_i^0=\mathbf{V}z_i, \qquad (8)$$

где z_i – векторы главных факторов образа x_i^0 в новом редуцированном пространстве состояний. Векторы z_i образуют матрицу $\mathbf{Z}$, которая может быть вычислена по следующей формуле:

$$\mathbf{Z}=\mathbf{X}^0\mathbf{V}, \qquad (9)$$

где $\mathbf{Z}$ – матрица главных факторов пространства $\mathbf{X}^0$.

Метод синтеза главных компонент. Пусть ставится задача найти l наибольших собственных значений и соответствующих им собственных векторов уравнения (2). Полагается, что $l<m$. Для решения этой задачи предлагается матрицу $\mathbf{X}^0$ представить в виде набора подматриц, каждая из которых имеет ранг $s<<m$. Таким образом:

$$\mathbf{X}^0=\begin{vmatrix}\mathbf{X}_1^0\\ \mathbf{X}_2^0\\ \vdots\\ \mathbf{X}_p^0\end{vmatrix}. \qquad (10)$$

Для каждой из подматриц вычисляем ковариационную матрицу $\mathbf{A}_{ii}^*=\frac{1}{m}(\mathbf{X}_i^0)^T\mathbf{X}_i^0$. Далее вычисляем собственные значения и собственные векторы матричного уравнения

$$(\mathbf{A}_{ii}^*-\lambda\mathbf{I})u_i=0, \qquad (11)$$

где u_i – собственный вектор. Формируется матрица из собственных векторов, которым соответствуют l первых наибольших собственных значений.

$$\mathbf{U}_i = [u_{i1} u_{i2} ... u_{il}] . \quad (12)$$

Далее выполняется процедура синтеза главных компонент. Она может выполняться в одношаговом и многошаговом варианте. Ниже представлена одношаговая процедура синтеза главных компонент.

Вычисляем матрицу собственных векторов $\mathbf{V}_i$:

$$\mathbf{V}_i^T = \mathbf{T}_i^{-1} \mathbf{U}_i^T \mathbf{X}_i^0 . \quad (13)$$

Формируется матрица $\mathbf{V}^* = [\mathbf{V}_1 \mathbf{V}_2 \cdots \mathbf{V}_p]$. Затем вычисляется приведенная матрица $\mathbf{A}_r = \mathbf{V}^{*T} \mathbf{A} \mathbf{V}^*$ и определяются собственные значения и собственные векторы уравнения

$$(\mathbf{A}_r - \lambda \mathbf{I}_r) q_r = 0 . \quad (14)$$

Получается матрица синтезированных главных компонент

$$\mathbf{V} = \mathbf{V}^* \mathbf{Q}_r . \quad (15)$$

Программная реализация. Разработан программный инструмент, предназначенный для исследования в области распознавания изображений. Система позволяет накапливать изображения в базе данных WFile, подсистема импорта изображений поддерживает все стандартные графические форматы файлов (bmp, gif, jpg), а также специализированный формат базы данных FERET (ppm). База данных WFile предназначается для ввода, хранения, обработки и вывода цифровых изображений, главных компонент, главных факторов. Используется страничная группировка записей, что позволяет уменьшить число обращений к жесткому диску.

Разработанная программа допускает выполнение операций не только над импортированными изображениями, но и над результатами промежуточных вычислений (например, ковариационная матрица). Исходные изображения, как и результаты промежуточных вычислений, могут отображаться в графическом или числовом виде.

Над данными (изображениями) могут производятся следующие операции:

1) перевод графических файлов в различные цветовые схемы (RGB, HSL, XYZ);

2) стандартные операции над матрицами и векторами (умножение, сложение, транспонирование и т.п.);

3) вычисление главных компонент:

- метод Хаусхолдера,
- итерационный метод,
- метод синтеза;

4) операции восстановления исходных изображений из *N*-главных компонент.

Исследование точности метода. Важным критерием любого численного метода является точность получаемых с его помощью результатов. Исследование точности метода синтеза демонстрируется на задаче обработки 72 изображений. Решение задачи выполняется методом синтеза. Точность метода исследуется для задачи нахождения первых восьми собственных значений и собственных векторов. Рассматривается четыре варианта синтеза главных компонент, отличающихся друг от друга количеством собственных векторов частных решений. В первом варианте вычисляются собственные векторы, сумма собственных значений которых составляет 75% суммы всех собственных значений, во втором варианте – 85%, в третьем варианте – 90%, в четвертом варианте – 95% В качестве эталонного решения используются собственные значения и собственные векторы, полученные методом Хаусхолдера.

Погрешность собственных значений, вычисленных методом блочно-линейной конденсации, вычисляется по формуле $\varepsilon_i = |\lambda_i^* - \lambda_i| / \lambda_i$, где λ_i^* – собственные значения, вычисленные методом блочно-линейной конденсации; λ_i – собственные значения, полученные методом Хаусхолдера. В таблице представлена погрешность восьми наибольших собственных значений, вычисленных для четырех вариантов синтеза главных компонент. Как видно из таблицы, чем больше собственных векторов частных решений используется в процедуре синтеза, тем выше точность решения.

Погрешность собственных значений, %

Вариант	Номер тона							
	1	2	3	4	5	6	7	8
1	0,013	0,073	1,273	7,943	7,711	12,86	16,72	15,75
2	0,005	0,013	0,261	0,609	1,163	1,648	2,17	4,407
3	0,004	0,010	0,132	0,281	0,566	1,145	0,897	2,442
4	0,002	0,002	0,018	0,076	0,299	0,099	0,243	0,825

Для изучения точности на больших объемах данных предполагается в дальнейшем использовать базу данных FERET, которая сегодня широко применяется для тестовой проверки коммерческих систем распознавания лиц.

Выводы. Рассмотрена задача распознавания изображений лиц на базе метода главных компонент. Основное внимание уделено решению задачи собственных значений больших матриц.

1. Разработана программная система, предназначенная для исследования в области распознавания изображений лиц.

2. Предложен новый метод нахождения главных компонент, базирующийся на делении исходной задачи на части, получении частных

решений и синтезе полного решения. Достоинство предлагаемого метода связано с тем, что он позволяет распараллелировать вычисления.

3. Исследована точность получаемых решений методом синтеза. Показано, что метод позволяет получать решения с приемлемой точностью.

ЛИТЕРАТУРА

1. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. СПб.: Политехника, 2001. 240 с.

2. Zhao W., Chellappa R., Rosenfeld A., Phillips P.J. Face recognition: a literature survey // National Institute of Standards and Technology. Technical Report #7478. USA. 2001. P. 66.

3. Ту Дж., Гонсалес Р. Принципы распознавания образов. М.: Мир, 1978. 411 с.

4. Парлетт В. Симметричная проблема собственных значений. Численные методы. М.: Мир, 1983. 384 с.

РЕАЛИЗАЦИЯ МОДЕЛИ РАСПРОСТРАНЕНИЯ ПРАВ ДОСТУПА TAKE-GRANT КОНЕЧНЫМИ АВТОМАТАМИ

Д.М. Мурин, студент 5-го курса, каф. компьютерной безопасности и математическх методов обработки информации

г. Ярославль, ЯрГУ, т. 8-902-330-73-28, nirum87@mail.ru

Рассматривается модель распространения прав доступа Take-Grant. Предложен алгоритм решения задачи Take-Grant путем сведения ее к задаче пересечения двух детерминированных автоматов. Алгоритм имеет в большинстве практических случаев полиномиальную оценку сложности от числа внутренних состояний автоматов.

Модель распространения прав доступа Take-Grant используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа в таких системах. Обычно данную модель описывают в терминах графов доступа. В данной работе предложен метод перехода от графов доступа к детерминированным автоматам, а также показано, что задача Take-Grant может быть сведена к задаче пересечения двух детерминированных автоматов. Один из этих автоматов строится на основе графа доступа, в работе приведен алгоритм его построения, другой является универсальным графом для модели Take-Grant, то есть не зависит от графа доступа.

Описание модели секретности TAKE-GRANT. U – множество сущностей (универсальных сущностей); O – множество объектов – пассивных сущностей (ими могут являться файлы, папки, документы,

области памяти); S – множество субъектов – активных сущностей (ими, например, будут пользователи или процессы).

Причем для введенных множеств справедливы следующие соотношения:

$$U = O \cup S, \qquad S \cap O = \varnothing,$$

$R = \{r_1, r_2, \ldots r_m\} \cup \{t, g\}$ – множество прав доступа, где t(take) – право «брать права доступа»; g(grant) – право «отдавать права доступа».

Пусть G = (U, E) – конечный помеченный ориентированный граф без петель, представляющий текущие доступы в системе.

Элементы множества $E \subseteq U \times U \times R$ представляют дуги графа, помеченные правами доступа.

Определим предикат «возможен доступ» ВД(α, *x*, *y*, G_0), который будет истинным тогда и только тогда, когда существуют графы $G_1 = (U_1, E_1), \ldots, G_n = (U_n, E_n)$ такие, что

$$G_0 \vdash_{op1} G_1 \vdash_{op2} G_2 \vdash_{op3} \ldots \vdash_{opn} Gn \wedge (x, y, \alpha) \in E_n,$$

где $G \vdash_{op} G^*$ – преобразование графа доступа по одному из четырех определенных в модели правил (take, grant, create и remove).

Задача Take-Grant состоит в том, чтобы для графа доступов G = (U, E) по заданным $\alpha \in R$, x, y $\in$ U определить истенен ли предикат ВД(α, x, y, G).

Более подробное описание модели секретности Take-Grant содержится в [1–4].

Алгоритм преобразования графа доступов в автомат доступов

Напомним определение конечного недетерминированного автомата.

Определение. Недетерминированный конечный автомат – это пятерка

$$M = (\Sigma_M, Q_M, \Delta_M, s_M, F_M),$$

где Σ_M – входной (внешний) алфавит автомата M; Q_M – внутренний алфавит автомата M, его элементы называются внутренними состояниями; $s_M \in Q_M$ – начальное состояние автомата M; $F_M \subseteq Q_M$ – множество конечных (заключительных, допускающих) состояний автомата M; Δ_M – отношение переходов автомата M, $\Delta_M \subseteq Q_M \times (\Sigma \cup \{\varepsilon\}) \times Q_M$.

Напомним, что у нас есть ориентированный, помеченный граф $G_0 = (U_0, E_0)$ и предикат ВД(α, x, y, G_0). Пусть $|\alpha| = 1$, т.е. α состоит из одного права и $(\alpha \neq t)$ & $(\alpha \neq g)$ (эти предположения несколько упрощают описание).

Предикат ВД(α, x, y, G_0) дает нам информацию о начальном и заключительном состояниях автомата TG: $s_{TG} = x$, $f_{TG} = y$.

$\Sigma_{TG} = \{\alpha\} \cup \{s\vec{t}o, o\vec{t}s, o\vec{t}o, s\vec{t}o, o\vec{t}s, o\vec{t}o, s\vec{g}o, o\vec{g}s, o\vec{g}o, s\vec{g}o, o\vec{g}s, o\vec{g}o\}$.

Сопоставим внутренним состояниям автомата TG вершины графа доступа G_0, примем $Q_{TG} = U$.

Зададим Δ_{TG}:

1) $<q, \alpha, p> \in \Delta_{TG} \Leftrightarrow (q, p, \alpha) \in G_0$;
2) $<q, \vec{s}to, p> \in \Delta_{TG} \Leftrightarrow ((q, p, t) \in G_0) \& (q \in S) \& (p \in O)$;
3) $<q, \vec{o}ts, p> \in \Delta_{TG} \Leftrightarrow ((q, p, t) \in G_0) \& (q \in O) \& (p \in S)$;
4) $<q, \vec{o}to, p> \in \Delta_{TG} \Leftrightarrow ((q, p, t) \in G_0) \& (q \in O) \& (p \in O)$;
5) $<q, \overleftarrow{s}to, p> \in \Delta_{TG} \Leftrightarrow ((p, q, t) \in G_0) \& (q \in S) \& (p \in O)$;
6) $<q, \overleftarrow{o}ts, p> \in \Delta_{TG} \Leftrightarrow ((p, q, t) \in G_0) \& (q \in O) \& (p \in S)$;
7) $<q, \overleftarrow{o}to, p> \in \Delta_{TG} \Leftrightarrow ((p, q, t) \in G_0) \& (q \in O) \& (p \in O)$;
8) $<q, s\vec{g}o, p> \in \Delta_{TG} \Leftrightarrow ((q, p, g) \in G_0) \& (q \in S) \& (p \in O)$;
9) $<q, o\vec{g}s, p> \in \Delta_{TG} \Leftrightarrow ((q, p, g) \in G_0) \& (q \in O) \& (p \in S)$;
10) $<q, o\vec{g}o, p> \in \Delta_{TG} \Leftrightarrow ((q, p, g) \in G_0) \& (q \in O) \& (p \in O)$;
11) $<q, s\overleftarrow{g}o, p> \in \Delta_{TG} \Leftrightarrow ((p, q, g) \in G_0) \& (q \in S) \& (p \in O)$;
12) $<q, o\overleftarrow{g}s, p> \in \Delta_{TG} \Leftrightarrow ((p, q, g) \in G_0) \& (q \in O) \& (p \in S)$;
13) $<q, o\overleftarrow{g}o, p> \in \Delta_{TG} \Leftrightarrow ((p, q, g) \in G_0) \& (q \in O) \& (p \in O)$.

Таким образом, мы определили автомат TAKE-GRANT. Автомат недетерминирован, так как в общем случае у графа доступа из одной вершины могут выходить несколько ребер с одинаковой меткой, а следовательно, для автомата возможен переход из одной конфигурации в несколько. В автомате TAKE-GRANT переходов в шесть раз больше, чем ребер графа доступа, помеченных правами t и g, однако это плата за то, что наш автомат может различать субъекты и объекты.

Можно показать, что все пути утечки прав описываются автоматом, схема которого представлена на рис. 1.

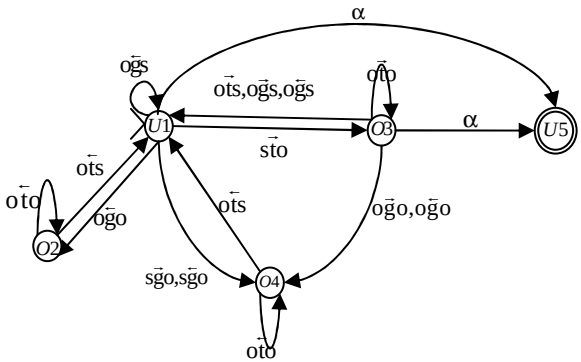


Рис. 1. Автомат, описывающий пути утечки прав (автомат ПУ)

Задача обнаружения путей утечки прав доступа (задача Take-Grant) сводится к задаче пересечения построенных в работе автоматов ПУ и TAKE-GRANT.

Поскольку автомат TAKE-GRANT недетерминированный, необходимо построить эквивалентный ему детерминированный автомат. В худшем случае полученный из НКА ДКА может иметь 2^n внутренних состояний, где n – число состояний НКА. Следовательно, в общем случае сложность найденного алгоритма решения задачи обнаружения путей утечки прав доступа экспоненциальная. Однако, как отмечается в [5], в большинстве практических случаев подобная экспоненциальная зависимость встречается крайне редко, обычно число внутренних состояний ДКА не намного превышает число внутренних состояний исходного НКА, поэтому изложенный в работе подход может быть применим не только в теории, но и на практике. Причем сложность алгоритма, составляющая в худшем случае $O(K^2 + 2^N)$, в большинстве практических случаев может быть оценена как $O(K^2 + N)$, где K – число субъектов графа; N – мощность множества U (число сущностей).

ЛИТЕРАТУРА

1. Bishop M. Theft of Information in the Take-Grant Protection Model // Computer Security. 1994/1995. № 3(4).

2. Bishop M. Conspiracy and Information Flow in the Take-Grant // Computer Security. 1996. № 4(4).

3. Девянин П.Н. Модели безопасности компьютерных систем. М.: Академия, 2005.

4. Корт С.С. Теоретические основы защиты информации. М.: Гелиос АРВ, 2004.

5. Ахо А., Сети Р., Ульман Дж. Компиляторы: Принципы, технологии, инструменты. М.: Вильямс, 2003.

ОБ ЭФФЕКТИВНОЙ РЕАЛИЗАЦИИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

В.В. Перевощиков, А.А. Гриценко, студенты 4-го курса,
каф. компьютерной безопасности и прикладной алгебры
г. Калининград, РГУ им. И. Канта, т. 8-962-252-81-37,
roadrunner39@rambler.ru

NP-полнота задачи дискретного логарифмирования на эллиптических кривых (ECDLP) не доказана. Но и алгоритмов, способных ее решить за полиномиальное время, пока не было найдено. Наиболее эффективным общим методом решения задачи ECDLP на сегодня является ρ-метод Полларда, но и он требует достаточно большого време-

ни работы. Поэтому важно уметь уменьшать время решения задачи за счет ускорения элементарных операций.

Данная работа посвящена созданию комплекса программ для решения ECDLP над полем $GF(2^n)$. В ней собрана статистическая информация о времени решения ECDLP, кратко описаны приемы, алгоритмы и их модификации, использованные в разработанном комплексе. В этом комплексе был использован алгоритм Поллига–Хеллмана для сведения задачи дискретного логарифмирования к аналогичным задачам в подгруппах простого порядка, где они решались ρ-методом Полларда.

I. Алгоритмическое представление поля $GF(2^n)$

Современные компьютеры построены на двоичной арифметике, что дает возможность ускорить выполнение операций над элементами поля $GF(2^n)$. Опишем особенности программной реализации операций в этом поле.

Если многочлен $f(x) \in GF(2^n)\ f(x) \in GF$ (2) представлен последовательностью бит $a_0, a_1, \ldots, a_{n-1}$, то мы можем разбить ее на $m = \lceil n/s \rceil$ группы по $s = 32$ бита, начиная с коэффициента при нулевой степени, т.е. представить в виде последовательности $A^{(0)}, A^{(1)}, ..., A^{(m-1)}$. Каждую из таких последовательностей $A^{(j)}$ можно интерпретировать как элементарный многочлен $\tilde{a}_j(x)$: $\deg \tilde{a}_j(x) \le s-1$. Тогда $f(x) = \sum_{j=0}^{m-1} \tilde{a}_j(x) \cdot (x^s)^j$. При этом также важно, что каждую последовательность бит $A^{(j)}$ можно интерпретировать, как двоичную запись некоторого 32-разрядного неотрицательного целого числа, которое в языке C/C++ представляется типом unsigned int. Рассмотрим алгоритмы выполнения некоторых операций в поле $GF(2^n)$.

1. Сложение и вычитание.

Эти операции являются базовыми операциями, и быстрота их выполнения во многом влияет на эффективность алгоритмов, использующих эти операции. Пусть $f, g \in GF(2^n)$, $\deg f(x) = k \le m = \deg g(x) < n$, $f(x) = \sum_{i=0}^{l_k} f_i(x) \cdot (x^s)^i$, $g(x) = \sum_{i=0}^{l_m} g_i(x) \cdot (x^s)^i$, где $f_i(x)$ и $g_i(x)$ – элементарные многочлены степени не больше $s-1$, тогда $f(x) + g(x) = \sum_{i=0}^{l_k} (f_i(x) + g_i(x)) \cdot (x^s)^i + \sum_{i=l_k+1}^{l_m} g_i(x)(x^s)^i$.

Если элементарные многочлены $a(x) = \sum_{i=0}^{s} a_i x^i$ и $b(x) = \sum_{i=0}^{s} b_i x^i$ интерпретировать как числа $\tilde{a} = \sum_{i=0}^{s} a_i 2^i$ и

$\tilde{b} = \sum_{i=0}^{s} b_i 2^i$, то сумма их интерпретируется как число $\tilde{c} = \sum_{i=0}^{s} c_i 2^i$, где $c_i = (a_i + b_i) \bmod 2$, т.е. $\tilde{c} = \tilde{a} \oplus \tilde{b}$. Вычитание многочленов в рассматриваемом поле равносильно их сложению.

2. Умножение.

Рассмотрим алгоритм умножения многочленов $u(x) = \sum_{i=0}^{r} u_i(x) \cdot (x^s)^i$ и $v(x) = \sum_{i=0}^{p} v_i(x) \cdot (x^s)^i$, т.е. нахождения многочлена $z(x) = u(x) \cdot v(x) = \sum_{i=0}^{r+p} z_i(x) \cdot (x^s)^i$. Положим, что мы знаем, как перемножать элементарные многочлены степени $s-1$. Заметим, что произведение двух элементарных многочленов $a(x)$ и $b(x)$ есть некоторый многочлен $q(x)$ степени $2s-2$: $v(x) = \sum_{i=0}^{1} q_i(x) \cdot (x^s)^i$, где $q_i(x)$ – элементарные многочлены. Через $\{a \times b\}_i$ будем обозначать многочлен q_i , $i = 0,1$.

ВХОД: $\{u_i\}_{i=0...r}$, $\{v_i\}_{i=0...p}$

ВЫХОД: $\{z_i\}_{i=0...r+p}$

1. **for** $i \leftarrow 0$ **to** $r+p$ **do** $z_i \leftarrow 0$

2. **for** $i \leftarrow 0$ **to** r **do**

2.1. **for** $j \leftarrow 0$ **to** p **do**

2.1.1. $z_{i+j} \leftarrow z_{i+j} + \{u_i \times v_j\}_0$

2.1.2. $z_{i+j+1} \leftarrow z_{i+j+1} + \{u_i \times v_j\}_1$

Алгоритм 1. Сведение умножения многочленов к умножению элементарных многочленов

Каждый элементарный многочлен можно представить четырьмя однобайтовыми числами и свести при помощи декомпозиционных схем Карацубы умножение двух четырехбайтовых чисел к умножению однобайтовых. А произведение однобайтовых чисел можно хранить в предвычисленной таблице *M*.

Пусть $a(x)$ и $b(x)$ – элементарные многочлены, многочлен $a(x)$ представлен последовательностью байт $A[0]\,A[1]\,A[2]\,A[3]$, $b(x)$ представлен как $B[0]\,B[1]\,B[2]\,B[3]$, тогда их произведение $p(x) = a(x) \cdot b(x)$ можно представить в виде последовательности байт $P[0]\,P[1] \ldots P[7]$.

Используя построенную таблицу *M*, вычислим следующие многочлены:

$$O_i = A[i] \times B[i] , \; i = 0...4 , \; T_{0,1} = (A[0] + A[1]) \times (B[0] + B[1]) ,$$

$$T_{1,1} = (A[2] + A[3]) \times (B[2] + B[3]),$$

$$T_{0,2} = (A[0] + A[2]) \times (B[0] + B[2]),$$

$$T_{1,2} = (A[1] + A[3]) \times (B[1] + B[3]),\ F = \sum_{i=0}^{3} A[i] \times \sum_{i=0}^{3} B[i].$$

Используя эти многочлены, находим следующие величины:

$D[i] = O_{i(\mathrm{mod}\,4)}[0] + O_{i-1(\mathrm{mod}\,4)}[1]$, $\quad i = 1...6$, $\quad S[1] = O_0[0] + D[1]$,

$S[i] = S[i-1] + D[i]$, $i = 2...6$.

Тогда однобайтовые элементы многочлена $p(x)$ вычисляются по формулам:

$$P[0] = O_0[0],\ P[1] = S[1] + T_{0,1}[0],\ P[2] = S[2] + T_{0,1}[1] + T_{0,2}[0],$$

$$P[3] = S[3] + T_{0,1}[0] + T_{1,1}[0] + T_{0,2}[0] + T_{0,2}[1] + T_{1,2}[0] + F[0],$$

$$P[4] = S[4] + T_{0,1}[1] + T_{1,1}[1] + T_{0,2}[0] + T_{1,2}[0] + T_{1,2}[1] + F[1],$$

$$P[5] = S[5] + T_{1,1}[0] + T_{1,2}[1],\ P[6] = S[6] + T_{1,1}[1],\ P[7] = O_3[1].$$

Описанный алгоритм дает существенное ускорение работы с разумными требованиями к используемой памяти для хранения таблицы M – всего 128 Кб.

3. Приведение по модулю неприводимого многочлена.

Эта операция, наряду со сложением и вычитанием, является базовой, и очень важно уметь выполнять ее быстро. Рассмотрим модификацию наивного алгоритма деления. Пусть $d_u = \deg u(x)$, $d_v = \deg v(x)$, тогда, пока $d_u \geq d_v$, возможно 2 случая:

1) $d_u - d_v \geq s$, в этом случае мы выделяем из многочлена $u(x)$ не одночлен $x^{d_u - d_v}$, а многочлен $q(x) \cdot x^{d_u - d_v - s + 1}$, где $q(x)$ – элементарный многочлен степени $s-1$. Это значит, что мы представляем $u(x) = q(x) \cdot x^{d_u - d_v - s + 1} v(x) + h(x)$, $\deg h(x) \leq d_u - s$. Если $\deg u(x) \geq s$, то с $u(x)$ мы можем связать элементарный многочлен $\tilde{u}(x)$ степени $s-1$, составленный из его старших коэффициентов. В противном случае имеем элементарный многочлен $\tilde{u}(x) = u(x)$. Аналогичным образом с многочленом $v(x)$ связываем элементарный многочлен $\tilde{v}(x)$. Далее мы полагаем $u(x) = h(x)$.

2) $d_u - d_v < s$, в этом случае сводим ситуацию к использованию 1-го случая за счет уменьшения s.

Нетрудно заметить, что $q(x)$ однозначно определяется многочленами $\tilde{u}(x)$ и $\tilde{v}(x)$. Это позволяет нам ускорить алгоритм, заранее ус-

тановив и записав в соответствующую таблицу, какой многочлен $q(x)$ соответствует каждой паре элементарных многочленов $\tilde{u}(x)$ и $\tilde{v}(x)$.

4. Деление многочленов в поле.

Эта операция осуществляется с использованием модификации расширенного алгоритма Евклида для многочленов.

II. ρ-метод Полларда

Для того чтобы решать ECDLP в циклических подгруппах простого порядка, в общем случае удобнее всего пользоваться ρ-методом Полларда. Это вероятностный метод, использующий случайное блуждание. Преимущество данного метода состоит в том, что он не требует для работы большого количества памяти. Опишем суть метода.

Пусть $E(GF(q))$ – эллиптическая кривая, заданная над конечным полем $GF(q)$, и $P \in E(GF(q))$. Обозначим через G_P циклическую подгруппу точек $E(GF(q))$, порожденную точкой P, пусть n – порядок этой группы, $Q \in G_P$. Будем полагать, что n – простое число. В группе G_P будем решать задачу дискретного логарифма, т.е. будем искать такое натуральное $0 \le x < n : x \cdot P = Q$.

Зададим легко вычислимую функцию $f : G_P \to \{1...k\}$, где k невелико (порядка 20). Далее случайным образом определим числа a_i и b_i из отрезка $[0, n-1]$, $i = 1...k$ и вычислим $M_i = a_i P + b_i Q$. Берем произвольную пару чисел s_0, t_0 из отрезка $[0, n-1]$ и вычислим $A_0 = s_0 P + t_0 Q$. Каждый член последовательности $A_i = s_i P + t_i Q$ вычисляется рекуррентно: $A_{i+1} = A_i + M_{f(A_i)}$, $s_{i+1} = s_i + a_{f(A_i)} (\mathrm{mod} n)$, $t_{i+1} = t_i + b_{f(A_i)} (\mathrm{mod} n)$.

Поскольку группа G_P конечна, то существуют такие индексы $i \neq j$, что $A_i = A_j$. Тогда $A_{i+1} = f(A_i) = f(A_j) = A_{j+1}$, т.е. последовательность, начиная с некоторого члена, будет вести себя циклическим образом. Так как n – очень большое число, то согласно парадоксу дней рождений повторение членов последовательности ожидается через $\sqrt{\pi n / 2}$ шагов. Однако чтобы обнаружить первое повторение, нам потребуется хранить $O(\sqrt{n})$ членов последовательности, что не очень эффективно. Удобнее воспользоваться алгоритмом Флойда поиска циклов. Берем пару элементов (A_1, A_2), по ней вычисляем пару (A_2, A_4), по этой паре вычисляем (A_3, A_6) и т.д., т.е. на i-м шаге по

паре (A_i, A_{2i}) мы вычисляем пару $(A_{i+1}, A_{2(i+1)}) = (f(A_i), f(f(A_{2i})))$. Процесс продолжаем до тех пор, пока $A_i \neq A_{2i}$. Таким образом на выходе мы получаем число m такое, что $A_m = A_{2m}$. Доказано, что совпадение членов ожидается через $O(\sqrt{n})$ шагов. При этом нам практически не требуется памяти для хранения данных. Так как $A_i = s_i P + t_i Q = s_i P + t_i xP = (s_i + t_i x)P$, то $(s_m + t_m x)P = (s_{2m} + t_{2m} x)P$, т.е. $s_m + t_m x = s_{2m} + t_{2m} x \pmod{n}$, откуда $x = (s_{2m} - s_m)/(t_m - t_{2m}) \pmod{n}$. Так как n очень велико, то возможность того, что $t_m = t_{2m}$, можно игнорировать. Заметим, что числа s_i, t_i, x могут иметь большое количество десятичных знаков, поэтому необходимо уделить внимание скорости выполнения операций с этими числами.

III. Алгоритм Поллига–Хеллмана

Алгоритм Поллига–Хеллмана успешно сводит задачу вычисления $l = \log_P Q$ к задаче вычисления дискретных логарифмов в подгруппе простого порядка группы G_P. Отсюда следует, что ECDLP в группе G_P не сложнее, чем ECDLP в её подгруппах. Поэтому для повышения стойкости криптосистемы к данному виду атаки необходимо выбирать параметры криптосистемы таким образом, чтобы $n = |G_P|$ делилось на большое простое число. Эта тенденция прослеживается и в результатах, полученных в данной работе. Опишем сам алгоритм.

Предположим, что мы знаем разложение порядка группы n на простые множители: $n = \sum_{i=1}^{r} p_i^{e_i}$. Стратегия алгоритма Поллига–Хеллмана заключается в том, чтобы подсчитать $l_i = l \bmod p_i^{e_i}$ для $i = 1...r$ и решить систему линейных сравнений

$$l_i = l \bmod p_i^{e_i}, \; i = 1...r, \qquad (1)$$

где $0 \le l < n$. Эта система может быть решена при помощи китайской теоремы об остатках (Chinese Remainder Theorem или CRT), которая гарантирует существование единственного решения системы (1) в данных условиях.

Покажем, как подсчёт l_i может быть сведён к вычислению e_i дискретных логарифмов в подгруппе порядка p_i группы G_P. Далее, для каждого i пусть $l_i = \sum_{j=0}^{e_j - 1} z_{i,j} p_i^j$, где $0 \le z_{i,j} < p_i$ – представление числа l_i в системе счисления с основанием p_i. Числа $z_{i,0}, z_{i,1}, \ldots, z_{i,e_i - 1}$ вычисляются одно за другим следующим образом:

ВХОД. Точки $P, Q \in G_P$, порядок группы n, числа $p = p_i$, $e = e_i$.

ВЫХОД. Число l_i.

1. $P_0 \leftarrow (np^{-1}) \cdot P$. (Порядок точки P_0 равен p).
2. $\tilde{Q} \leftarrow Q$.
3. **for** $j \leftarrow 0$ **to** $e-1$ **do**.

3.1. $Q_j \leftarrow (n / p^{j+1}) \cdot \tilde{Q}$.

3.2.Решить ECDLP ρ-методом Полларда для точек Q_j и P_0, $z_j \leftarrow \log_{P_0} Q_j$.

3.3. $\tilde{Q} \leftarrow \tilde{Q} - (z_j \cdot p^j) \cdot P$.

4. **return** $l_i = \sum_{j=0}^{e-1} z_j p^j$.

Алгоритм 2. Вычисление чисел l_i системы линейных сравнений (1).

Путём применения этого алгоритма ко всем l_i, $i = 1...r$ определяется система линейных сравнений (1), в ходе решения которой алгоритмом CRT вычисляется $l = \log_P Q$.

Таким образом, в ходе работы авторы сумели реализовать описанные в данной статье алгоритмы в виде комплекса программ по решению ECDLP. В процессе тестирования этого комплекса была собрана статистическая информация о времени работы алгоритма, позволяющая оценить его быстродействие (под размером задачи мы понимаем максимум из порядков простых циклических подгрупп группы G_P). В таблице приведены результаты – среднее время работы алгоритма для подгруппы размера n.

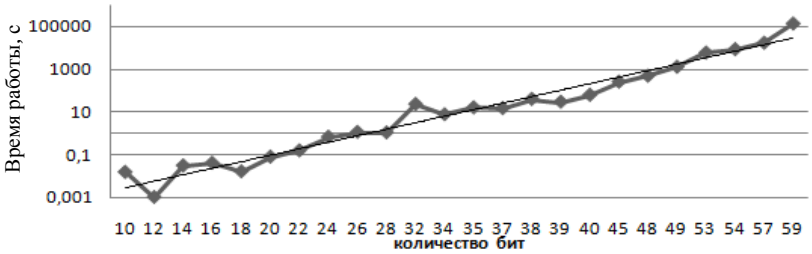


Рис. 1. Зависимость времени работы программы от размера задачи

Время работы реализованного алгоритма

№	Размер задачи (n)	Кол-во бит	Среднее время работы, с
1	2	3	4
1	541	10	0,015
2	2377	12	0,001
3	10837	14	0,03
4	42457	16	0,04
5	225611	18	0,016
6	633257	20	0,078
7	2693237	22	0,153
8	11127041	24	0,669
9	62699333	26	1,129
10	230603167	28	1,066
11	4265677249	32	22,916
12	10063074221	34	7,563
13	17192986687	35	15,958
14	106781081677	37	14,813
15	166456142911	38	39,531
16	275295876199	39	29,368
17	549756390943	40	61,645
18	21044858204113	45	256,159
19	162888033982417	48	486,772
20	418616258967271	49	1278,4655
21	5513228015079457	53	5889,234
22	14351744671810121	54	8496,802
23	86020738150056119	57	17051,172
24	440512026877326167	59	135373,979

На рис. 1 отражена зависимость времени работы от размера задачи. По оси времени используется логарифмическая шкала.

Авторы ставят перед собой задачу расширения созданного программного комплекса для распределенного вычисления дискретного логарифма ρ-методом Полларда и ускорения последнего за счет использования подходящей структуры данных для быстрого доступа к точкам эллиптической кривой, хранимым на центральном сервере. Планируется оценить сложность параллельного алгоритма и сравнить быстродействие последовательного и параллельного вариантов комплекса.

ЛИТЕРАТУРА

1. Алешников С.И., Болтнев Ю.Ф. Математические методы защиты информации. Ч. 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых: практ. пособие. Калининград, 2007.

2. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига/URSS, 2006.

3. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига/URSS, 2006.

4. Вельшенбах М. Криптография на Си и С++ в действии: учеб. пособие. М.: Триумф, 2004.

5. Cohen H., Frey G. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, 2005.

6. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. New-York: Springer-Verlag Inc., 2004.

7. Menezes A. et al. Handbook of applied cryptography. CRC Press Inc., 1997.

8. Применко Э.А., Винокуров А.Ю. Эллиптические кривые: новый этап развития современной криптографии // Системы безопасности. 2004. № 1.

9. Teske E. Speeding up Pollard's Rho Method for Computing Descrete Logarithms. Algorithmic Number Theory // Third International Symposium, ANTS-III, Portland, Oregon, USA, June 1998 Proceedings, Springer-Verlag, 1998.

10. Certicom ECC Challenge. November, 1997.

11. Arndt J. Algorithms for programmers: ideas and source code, 2008.

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

А.А. Пономерев

г. Ижевск, Удмуртский государственный университет,
т. 8-904-832-50-16, ponart@mail.ru

Методами функционального моделирования, используя стандарт [1], построена функциональная модель деятельности службы защиты информации. В данной модели отражены основные направления деятельности службы защиты информации для любой коммерческой организации.

Под функциональной оптимизацией СЗИ будем понимать процесс описания и выбора структуры службы защиты информации (СлЗИ), обеспечивающей защиту информации организации от наиболее полного множества угроз. Для описания деятельности СлЗИ будем представлять её как обеспечивающий бизнес-процесс и опишем её с помощью стандарта [1] (который является аналогом нотации IDEF0).

Деятельность по выявлению и описанию существующих бизнес-процессов (анализ бизнес-процессов), а также проектированию новых (проектирование бизнес-процессов) называется бизнес-моделированием. Каждый бизнес-процесс состоит из набора функций.

Описание бизнес-процессов предприятия, используя стандарт [1], будем называть функциональным моделированием. Стандарт [1] предназначен для использования при анализе и синтезе производственно-

технических и организационно-экономических систем. Рекомендации содержат описание комплекса средств для наглядного представления широкого спектра деловых, производственных и других процессов и операций предприятия на любом уровне детализации, а также организационные и методические приемы применения этих средств [1].

Одной из важнейших целей при подготовке проекта системы защиты информации является четкая и правильно понимаемая постановка задачи СЗИ. Для достижения этой цели необходимо исследовать все происходящие финансово-хозяйственные процессы и соответствующие им потоки информации на предприятии, выявить те из них, которые должны быть защищены в первую очередь. Для построения эффективной системы защиты информации недостаточно знать организационно-штатную структуру организации. Дело в том, что кроме собственно организационно-штатной структуры важнейшее значение имеет система взаимодействия между ее элементами. Такая система взаимодействия имеет пять основных аспектов:

– административный;
– финансовый;
– материальный (товарный);
– информационный;
– коммуникационный.

Существование любого предприятия связано с выполнением на предприятии бизнес-процессов. Бизнес-процесс – структурированный набор действий, охватывающий различные сущности предприятия и подчиненный определенной цели. Целью любого коммерческого предприятия в конечном итоге является получение прибыли. Прибыль же извлекается из бизнес-процессов, происходящих на предприятии. Бизнес-процессы охватывают собой всю структурированную деятельность предприятия. По сути, коммерческое предприятие нуждается в защите своих бизнес-процессов. Исходя из этого и должна быть построена система защиты информации на предприятии. Такой подход позволяет более детально поставить приоритеты в защите той или иной информации.

Деятельность предприятия можно представить в виде трех групп высокоуровневых процессов [2]:

– процессы управления организацией;
– основные процессы (процессы основной деятельности);
– вспомогательные процессы (процессы, связанные с ресурсообеспечением).

Характерными признаками трех перечисленных групп процессов являются:

• процессы управления организацией предназначены для координации и управления деятельностью всей организации. Данные процессы предназначены для формирования целей деятельности для основных процессов, а также синхронизации основных, вспомогательных и управленческих процессов внутри организации. Другой важной задачей является синхронизация материальных средств, людских ресурсов, финансовых средств, различных видов информации внутри и вне организации. Важно также отметить, что по своей сути управленческие процессы являются процессами информационными, т.е. получают информацию от объекта управления, преобразуют её, проводят анализ информации, принимают решение, доводят решение до объекта управления;

• основные процессы предназначены для создания основного продукта производства (услуги). Данные процессы добавляют к продукту ценность для потребителя;

• вспомогательные процессы обеспечивают деятельность основных процессов. Результатом их деятельности являются ресурсы и сервисы для основных процессов. Деятельность вспомогательных процессов не касается основных продуктов, поэтому они добавляют продукту стоимость.

Приоритетами СЗИ должны стать, в первую очередь, защита основных бизнес-процессов организации, во-вторых, защита процессов управления, в-третьих, участие во вспомогательных процессах (работа с персоналом, участие в деятельности служб информатизации и др.). При этом сама деятельность службы защиты информации или специалиста по защите информации может быть представлена и как вспомогательный бизнес-процесс, так как данная деятельность не участвует в выпуске продукции и по своей сути является затратной для предприятия. Также деятельность СлЗИ может быть представлена как основной бизнес-процесс, так как создаёт экономию при возможных потерях, т.е. формирует прибыль.

Важнейшими исходными данными для построения СЗИ являются информационные модели (описание реализованных бизнес-процессов, реализуемых технологий и т.п.). Данные модели определяют приоритеты деятельности СлЗИ, так как они позволяют понять, где в структуре деятельности предприятия имеются уязвимые места для потенциальных злоумышленников, какие меры (организационные, технические и др.) могут потребоваться и какие будут наиболее эффективны. Наличие или отсутствие в организации формализованной модели ее управленческой, основной или вспомогательной деятельности не является препятствием к организации деятельности по обеспечению информационной безопасности на базе процессного подхода.

Описание бизнес-процессов предприятия. Существует множество нотаций для описания бизнес-процессов. Самыми авторитетными стали нотации IDEF, которые были приняты как стандарты, в частности, в России (см. [1]). Стандарт [1] предназначен для использования при анализе и синтезе производственно-технических и организационно-экономических систем методами функционального моделирования. Рекомендации содержат описание комплекса средств для наглядного представления широкого спектра деловых, производственных и других процессов и операций предприятия на любом уровне детализации, а также организационные и методические приемы применения этих средств [1]. На основе данных стандартов выпущено множество программных продуктов, позволяющих представить деятельность организации с помощью бизнес-процессов.

Семантика языка IDEF0. Поскольку IDEF0 есть методология функционального моделирования, имя блока, описывающее функцию, должно быть глаголом или глагольным оборотом. Каждая сторона функционального блока имеет назначение с точки зрения связи блок/стрелки. Стрелка (и), входящая (ие) в левую сторону блока, – вход (ы). Входы преобразуются или расходуются функцией, чтобы создать то, что появится на ее выходе. Стрелка (и), входящая (ие) в блок сверху, – управление (я). Управление определяет условия, необходимые функции, чтобы произвести правильный выход. Стрелка, покидающая блок справа, – выход, то есть данные или материальные объекты, произведенные функцией. Стрелки, входящие в нижнюю сторону блока, представляют механизмы, то есть все то, с помощью чего осуществляется преобразование входов в выходы. Стрелки, выходящие из нижней стороны блока, представляют вызовы. Стрелки вызова обозначают обращение из данной модели или данной части модели к блоку, входящему в состав другой модели или другой части модели. Стандартное расположение стрелок показано на рис. 1.

Рис. 1. Семантика языка IDEF0

Функциональная модель СЗИ. Разработанная модель деятельности СлЗИ написана в нотации IDEF0. Данная модель показывает не конкретную организацию с её службой защиты информации, а деятельность абстрактной службы защиты информации (как должно быть). На основе полученной модели должна строиться деятельность реальных служб ЗИ в организациях.

Объемы статьи позволяют разобрать только несколько диаграмм модели, которые представлены в приложении. На первой диаграмме (рис. 2) деятельность службы ЗИ отображена в общем виде с отображением основных механизмов и ограничений на деятельность. Далее на диаграмме А0 (рис. 3) произведена декомпозиция деятельности СлЗИ на основные процессы. В отдельный процесс выделен анализ рисков, так как его выполнение является наиважнейшей задачей СлЗИ. И на его основе принимаются дальнейшие управленческие решения по совершенствованию СЗИ. На диаграмме А1 (рис. 4) анализ рисков разбит на ряд операций, после проведения которых у собственника информационных ресурсов должно возникнуть понимание, какая информация циркулирует на предприятии, какова её цена и каков риск появления угроз. Таким образом, удалось описать деятельность СлЗИ по обеспечению информационной безопасности организации с использованием функционального моделирования. В результате получена функциональная модель деятельности СлЗИ, которая может являться шаблоном в организации деятельности реальных подразделений, занимающихся обеспечением информационной безопасности организации. Защита информации является процессом (что, в частности, показано в модели в виде обратной связи) и нуждается в постоянном совершенствовании. Целью разработки функциональной модели деятельности службы защиты информации является функциональная оптимизация службы под потребности организации.

Функциональная оптимизация СЗИ. Функциональная оптимизация СЗИ будет заключаться в декомпозиции приведенных диаграмм до конкретных функций, которые должны выполнять конкретные исполнители. Следует отметить, что СЗИ строятся под конкретную организацию и функции СЗИ должны соответствовать целям функционирования организации. Построение функциональной модели СлЗИ позволяет оптимизировать деятельность путем четкого распределения обязанностей и ответственности между исполнителями. В случае рассмотрения уже существующей СлЗИ рекомендуется построить её функциональную модель, а затем сравнить её с оптимальной путем индукции, т.е. подниматься от обязанности существующих сотрудников до направлений защиты и следить за тем, что бы за все направления были ответственные. Таким образом, удастся достигнуть оптимальной структуры СлЗИ.

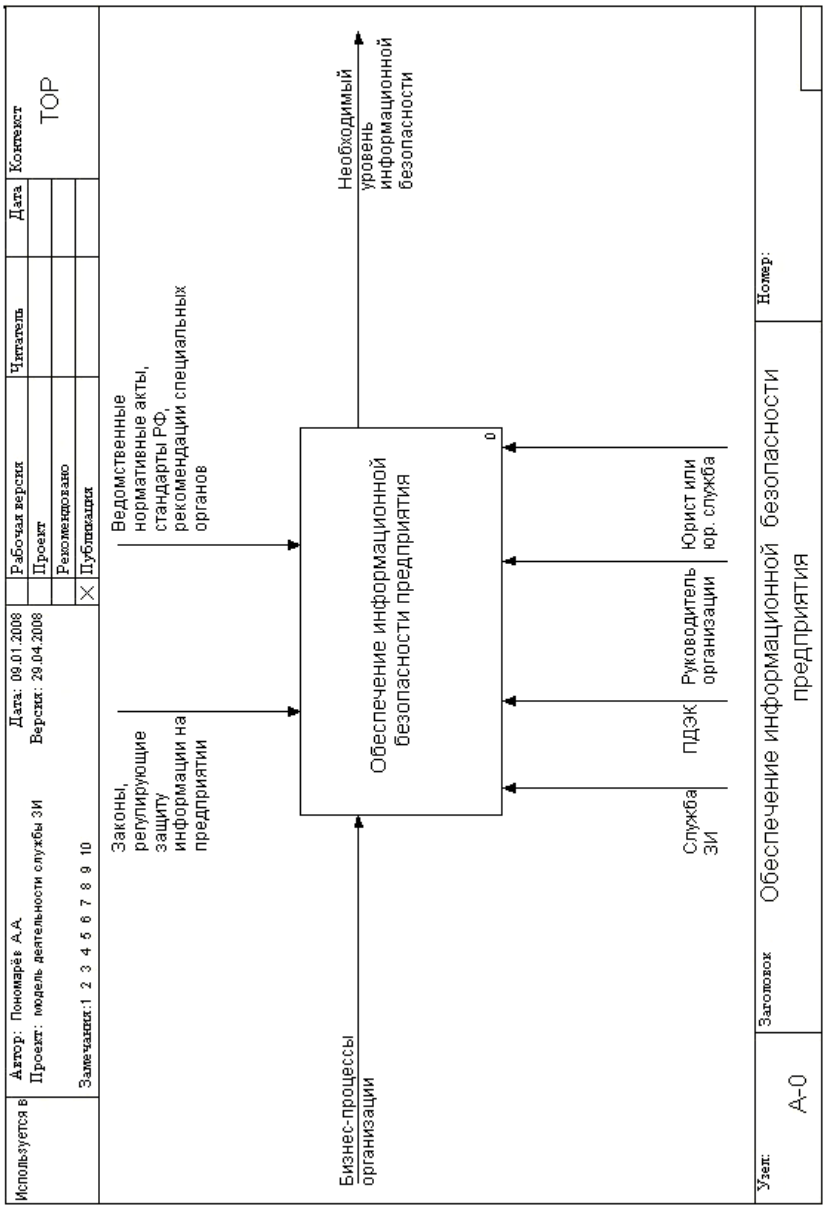


Рис. 2. Диаграмма A-0

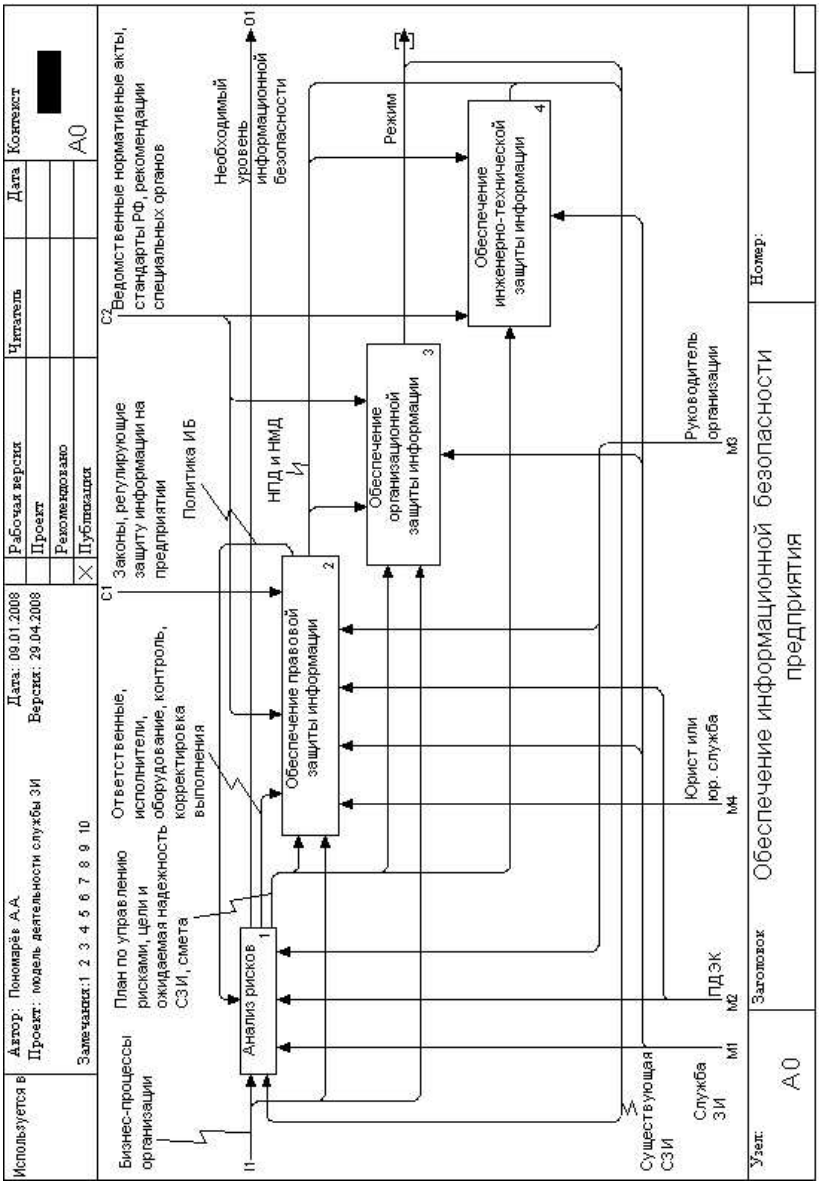


Рис. 3. Диаграмма A0

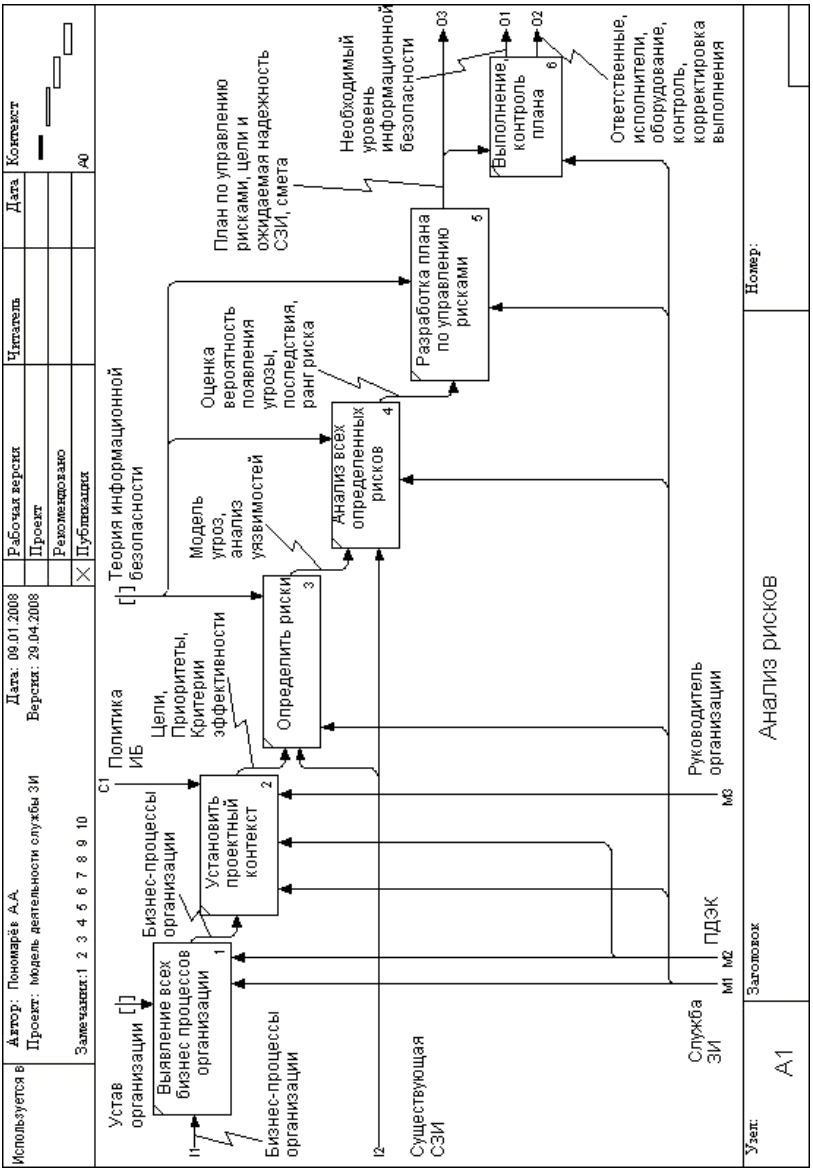


Рис. 4. Диаграмма A1

Выявление бизнес-процессов организации является важной задачей для руководства компании, так как позволяет оптимизировать деятельность предприятия, исключив дублирование функций, лишние связи и другие проблемы в организации деятельности. Построение эффективной системы защиты информации должно начинаться с выявления основных бизнес-процессов организации, так как именно они обычно нуждаются в защите их информационной составляющей.

Функциональная модель позволяет описать функции службы защиты информации, которые должны быть реализованы. Функциональная модель представляет функции не просто их набором, а упорядочивает, вводя входные данные (или материальные объекты), ограничения, исполнителя, результат выполнения. Конкретная организация может строить деятельность своего органа защиты информации, используя полученную модель.

ЛИТЕРАТУРА

1. Р 50.1.028-2001 Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования. М.: Госстандарт России, 2001.

2. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. М.: Издательская группа «БДЦ-пресс», 2006. 304 с.

РАЗРАБОТКА МЕТОДИК АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Пономарев

г. Ижевск, Удмуртский государственный университет,
т. 8-904-832-50-16, ponart@mail.ru

Проанализирован опыт анализа рисков. Разработаны методики анализа рисков. Суть первой заключается в анализе рисков со стороны злоумышленника и ранжирования угроз, исходя из этого параметра. Суть второй заключается в совмещении количественного и качественного анализа рисков. То есть количественно риски предлагается оценивать только после этапа их качественной оценки по заданному множеству параметров.

Основой методологии анализа рисков на сегодня является американский стандарт NIST [1], где приводится общая методология анализа рисков для организаций. В настоящее время существуют коммерческие программные продукты, которые также оценивают риски для организаций и выдают некоторые рекомендации по усовершенствованию существующих систем.

Методики анализа рисков

Можно выделить три сформировавшихся направления анализа рисков [3, 4]:

• Качественная оценка рисков.

• Количественная оценка рисков.

• Именные методики (Модель обобщенного стоимостного результата Миоры (англ. Miora Generalized Cost Consequence Model)) и коммерческие программные продукты, в которых может быть реализована как количественная и качественная оценка рисков, так и оба подхода сразу.

Модель качественной оценки

Качественная оценка обычно сводится к введению некоторых качественных шкал оценки показателей для оценки важности информации (например, важная, критичная, жизненная) и оценки риска угрозы (низкий, средний, высокий). Далее выбираются ресурсы с наибольшими показателями риска, они и подвергаются дополнительной защите (например, защищаются ресурсы с показателями важности информации – жизненная и риском угрозы – высоким).

Достоинством качественной оценки рисков являются:

• ускоряется и упрощается анализ рисков;

• нет необходимости оценивать в денежных единицах стоимость ресурса;

• нет необходимости вычислять вероятности проявления угрозы;

• нет необходимости вычислять соответствие применяемых мер угрозам.

Модель количественной оценки рисков.

Количественная модель рисков оперирует такими понятиями, как [4]:

• годовая частота происшествия (англ. Annualized Rate of Occurrence – ARO);

• ожидаемый единичный ущерб (англ. Single Loss Expectancy – SLE);

• ожидаемый годовой ущерб (англ. Annualized Loss Expectancy – ALE), величина, равная произведению ARO на SLE.

$$ALE = ARO \times SLE. \quad (1)$$

ARO – это частота появления события, приносящего ущерб в год. Данный показатель также можно назвать интенсивностью события.

SLE – показатель, который рассчитывается как произведение стоимости информации (Asset Value – AV) на фактор воздействия (англ. Exposure Factor – EF). Фактор воздействия – это размер ущерба или влияния на значение актива (от 0 до 1), т.е. часть значения, которую актив потеряет в результате события:

$$SLE=AV \times EF \quad (2)$$

Управление рисками считается эффективным, если расходы на безопасность в год не превышают ожидаемый годовой ущерб.

Отечественный опыт оценки рисков.

После того как в коммерческой фирме выявлены все носители конфиденциальной информации КИ, по каждому (группам однотипных) носителю должен быть произведен анализ рисков с целью выявления слабых мест существующей СЗИ и более правильного распределения выделенных на защиту материальных средств.

В [2] приводится двухфакторный и трехфакторный анализ рисков, который производится по следующим формулам:

$$R = P_{\text{происшествия}} C_{\text{потери}}, \quad (3)$$

$$R = P_{\text{угрозы}} P_{\text{уязвимости}} C_{\text{потери}}, \quad (4)$$

где R – риск; $P_{\text{происшествия}}$ – вероятность происшествия; $P_{\text{угрозы}}$ – вероятность возникновения угрозы; $P_{\text{уязвимости}}$ – вероятность потери информации (потеря трактуется широко: уничтожение, разглашение, уничтожение, модификации); $C_{\text{потери}}$ – стоимость информации (цена потери). Данная методика является шагом назад по сравнению с приведенной выше методикой количественной оценки рисков, так как последняя позволяет рекомендовать, сколько средств нужно тратить на защиту информации, а методология, указанная в [2], лишь позволяет ранжировать риски.

При этом в обоих случаях количественная оценка рисков осложняется тем, что не приводится никаких методик по вычислениям вероятностей (или частоты появления события) и цены информации. Но непонятно, чем должны руководствоваться привлекаемые эксперты. Поэтому методика нуждается в объяснении, желательно близком к математическому, каждого показателя вероятности и стоимости информации.

Отдельно рассмотрим формулу (4), в которой автор разложил $P_{\text{происшествия}}$ на $P_{\text{угрозы}}$ и $P_{\text{уязвимости}}$. Однако вероятности возникновения преднамеренных угроз в формуле (4) будут зависеть от вероятности уязвимости. Поэтому данную формулу не всегда правильно применять, так как $P_{\text{угрозы}}$ будет зависеть от $P_{\text{уязвимости}}$. Поэтому следует более подробно подойти к анализу рисков, исходя из характера возникающих угроз. Таким образом можно будет избежать ошибок, которые будут происходить по причине того, что вероятность происшествия и вероятность уязвимости будут не независимыми событиями. Например, рассмотрим случай – две организации одна применяет эффективную систему контроля персонала, периодически проверяет наличие

носителей конфиденциальных документов, в другой организации такого контроля не ведется. Однако, исходя из формулы (4), вероятность возникновения угрозы выноса материальных носителей, хранящих конфиденциальную информацию, будет одинаковой. Это неправильно, так как злоумышленник всегда оценивает свои силы и возможности перед совершением преступления. Поэтому оценивать вероятность угрозы можно только для угроз, не зависящих от человека.

Предлагаемая методика оценки рисков.

Для оценки вероятности возникновения угрозы сначала приведем удобную для дальнейшего рассмотрения классификацию угроз информации. Поскольку конечной целью оценки является (в идеальном случае) определение вероятности возникновения угрозы, выделим следующие источники угроз:

Естественные – это стихийные бедствия, аварии, сбои и отказы технических средств, другие события, вызванные объективными физическими явлениями, не подконтрольными человеку.

Искусственные – угрозы, вызванные деятельностью человека. Эти угрозы разделяются на:

• непреднамеренные (неумышленные, случайные), вызванные ошибками в проектировании систем и элементов, ошибки в программном обеспечении, ошибки в действиях персонала и т.п.;

• преднамеренные (умышленные), связанные с сознательным причинением вреда.

При этом естественные и непреднамеренные искусственные угрозы будем считать случайными. Оценить вероятность возникновения (и частоты появления) случайных угроз возможно при накоплении достаточной статистики их возникновения. Случайные угрозы можно оценить, например, с помощью простого потока событий (Пуассона). На этом этапе можно полностью отбросить угрозы, вероятность возникновения которых пренебрежимо мала (падение метеорита), и воспользоваться приведенной выше методикой количественной оценки рисков.

Отдельно рассмотрим вопрос выхода из строя оборудования. Данный вопрос хорошо разработан в теории надежности, которая для анализа в данной области пользуется математическим аппаратом теории массового обслуживания.

Также отметим, что большинство случайно возникающих угроз – это угрозы целостности и доступности информации.

Анализ рисков для систем обработки информации на основе анализа рисков злоумышленника.

Вероятность возникновения угрозы ($P_{\text{угрозы}}$) также тяжело оценивать в случае, когда идет речь о преднамеренных действиях людей

(например, несанкционированный доступ), потому что действия будут зависеть от существующей СЗИ на предприятии. А давать оценку возникновения преднамеренной угрозы, не учитывая систему защиты информации, является неверным, так как злоумышленник будет оценивать свои силы, и если в плохо защищенной организации он попытается произвести действия, приводящие к ущербу для организации, то в хорошо защищенной организации, осуществляющей пристальный контроль действий сотрудников фирмы, он не решится.

Можем разделить злоумышленников на категории несколькими способами, приняв за основу классификации цели, доступ, ресурсы, квалификацию и риск.

Цели злоумышленников могут быть различны: причинение ущерба, финансовая выгода, информация и т.д. Цели промышленного шпиона отличаются от целей синдиката организованной преступности, и контрмеры, которые способны остановить первого, могут даже не побеспокоить второй. Понимание целей вероятных злоумышленников – это первый шаг к выяснению контрмер, которые будут эффективными.

Злоумышленники имеют различный уровень доступа: возможности члена какой-либо организации, например, намного больше, чем любого одиночки. Злоумышленники также сильно различаются по своим финансовым возможностям: некоторые хорошо финансируются, другие нет. Одни имеют достаточную техническую квалификацию, у других ее нет. В [6] нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Различные классы злоумышленников по-разному относятся к риску. Террористы часто бывают счастливы умереть за свои убеждения. Преступники смиряются с риском оказаться в тюрьме, но, вероятно, не захотят иметь неприятности сверх тех, которыми может обернуться грабеж банка. Ищущие славы вовсе не хотят попасть в тюрьму. Злоумышленник с практически неограниченным бюджетом (например, государственные структуры) наиболее гибок в решениях, так как он может использовать свои средства для различных целей. Он может получить доступ, подкупив посвященных лиц, и повысить свой технический уровень, купив технологию или наняв экспертов (возможно, посвятив их в свои намерения, возможно, нанимая их под ложными предлогами). Он может также использовать деньги для снижения риска, совершая более подготовленные и поэтому более дорогостоящие атаки.

Рациональный злоумышленник (большинство) выбирает нападение, которое с лихвой окупит понесенные расходы с учетом всех издержек: квалификации, получения доступа, трудовых ресурсов, времени и риска. Некоторые нападения требуют хорошей квалификации, но

не требуют никакого специального доступа: взлом алгоритма кодирования, например. Каждый злоумышленник старается использовать набор приемлемых для него видов атак, отбросив те, которые ему не подходят. Конечно же, он выберет такое нападение, которое уменьшает затраты и увеличивает выгоды. Поэтому вероятность угрозы выше 0 тогда, когда выгода от полученной информации превышает затраты на её добывание. Она резко возрастает при существенном увеличении отношения цены информации к затратам на ее добывание – $С_И/С_Д$ (рис. 1).

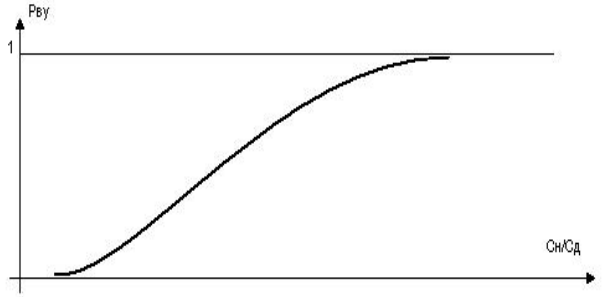


Рис. 1. Зависимость вероятности возникновения преднамеренной угрозы от соотношения цены информации и затрат на её добывание

Уровень защищенности информации определяет затраты на добывание информации. Его рост уменьшает отношение $С_И/С_Д$ и, следовательно, вероятность угрозы.

Вероятность возникновения угрозы зависит от многих факторов, основными из которых являются [2, 5]:

• цена защищаемой информации;

• уровень информационной безопасности организации;

• квалификация злоумышленника, его ресурсы и затраты на добывание им информации;

• криминогенная обстановка в месте нахождения организации.

В большинстве случаев, если речь идет о преднамеренных действиях людей, имеет место их материальная заинтересованность. В этом случае проще перейти на позиции злоумышленника и оценивать риски с его позиции. Тогда заменим вероятность угрозы $P_{\text{угрозы}}$ на риск злоумышленника $R_{\text{зл}}$. В этом случае $R_{\text{зл}}$ можно записать следующим образом:

$$R_{\text{зл}} = \frac{C_{\text{доход}}}{C_{\text{орг}}} P_{\text{необн}} P_{\text{получ}}, \qquad (5)$$

где $C_{орг}$ – стоимость организации канала получения информации; $C_{доход}$ – доход, получаемый от добытой информации (не всегда равен стоимости информации для владельца); $P_{необн}$ – вероятность необнаружения действий злоумышленника (зависит от частоты проверок действий собственных сотрудников, ошибок первого рода охранной сигнализации и др.); $P_{получ}$ – вероятность получения информации (или какой-то выгоды). Данный подход может объяснить действия злоумышленника, однако не может сказать, сколько денег следует потратить на предотвращение (уменьшение) риска атаки. Подход исходит из того, что злоумышленник будет осуществлять свои действия (атаки, НСД) на наименее защищенные объекты, которые и следует защищать.

Методика оценки рисков для преднамеренных угроз.

Анализ рисков предлагается осуществлять по схеме, показанной на рис. 2.

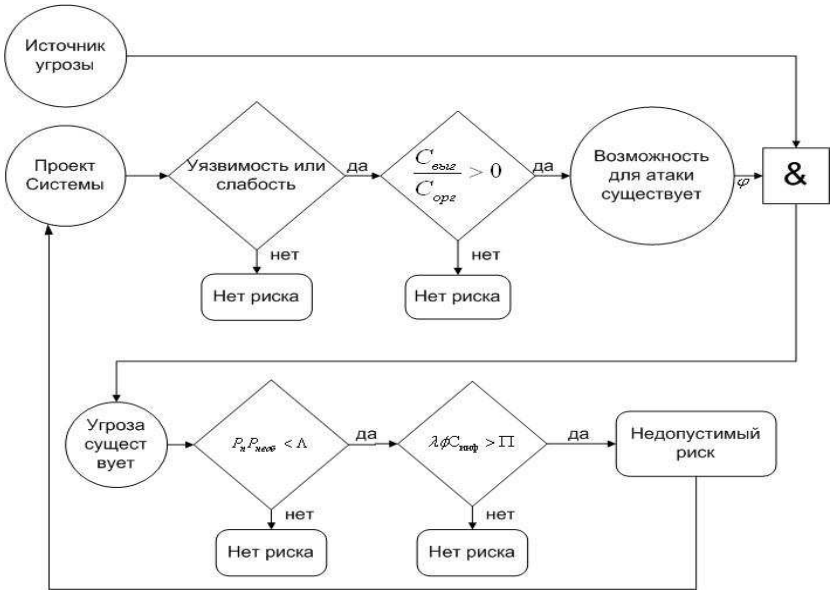


Рис. 2. Анализ рисков для преднамеренных угроз

Анализ рисков рассматривается для проекта системы защиты информации, та же методика применима и к существующей в организации системе защиты информации. В проекте (существующей системе) могут быть уязвимости и слабости реализации, которые должны быть

найдены. Далее следует рассмотреть вопрос о том, могут ли найденные уязвимости эксплуатироваться злоумышленником. Считается, что злоумышленник действует экономически целесообразно, а значит, отношение стоимости получаемой им выгоды к стоимости организации атаки будет больше нуля $\frac{C_{\text{выг}}}{C_{\text{орг}}}>0$. Далее также следует рассмотреть, имеется ли у данной организации источник рассматриваемой угрозы. Если источник угрозы существует, то угроза существует и проявится, если произведение вероятности получения информации $P_{\text{п}}$ и вероятности необнаружения действий злоумышленника $P_{\text{необ}}$ меньше, какого-то порогового значения (страх злоумышленника перед наказанием) Λ: $P_{\text{п}}P_{\text{необ}}<\Lambda$. Далее собственник информационных ресурсов применяет меры, если ежегодные потери больше порогового значения: $\lambda\phi C_{\text{инф}}>\Pi$, где λ – интенсивность происшествия в год; ϕ – фактор утраты; $C_{\text{инф}}$ – цена информационного ресурса (или процесса); Π – пороговое значение. Данное пороговое значение рассматривается применительно к конкретной угрозе, так как уменьшить некоторые угрозы – очень дорогое мероприятие, и собственнику следует перераспределить средства на защиту от других угроз. Исходить следует из того, что защита информации не должна быть дороже ежегодных потерь. Приведенная выше методика должна быть применена в отношении всех угроз безопасности информации, целью является минимизация общего риска для информационных ресурсов организации.

Источники угроз безопасности информации.

В процессе анализа рисков по каждой угрозе важно понимать, что для осуществления некоторых угроз требуется применение специальной дорогостоящей техники. Поэтому по некоторым угрозам источника угрозы для рассматриваемой организации может не быть.

В общем случае источниками преднамеренных угроз являются [2, 4, 5]:

- органы зарубежной разведки;
- органы разведки коммерческих структур;
- криминальные структуры;
- персонал организации (завербованные или не довольные своим положением сотрудники организации);
- психически больные;
- преступники-одиночки;
- террористы;
- пресса;

• государственные органы власти (полиция, милиция, прокуратура, налоговая полиция и др.).

Каждая группа характеризуется своими характеристиками. К примеру органы зарубежной разведки хорошо финансируются, имеют высокую квалификацию и все необходимое оборудование, однако боятся быть разоблаченными, что может привести к международному скандалу и нагнетании напряженности между государствами. Террористы финансируются менее хорошо, однако, напротив, не ставят цель скрыть свои действия, желают своими действиями привлечь общественное внимание.

Выводы. Предложены методики анализа рисков. Первая заключается в рассмотрении системы защиты информации со стороны злоумышленника и классификации самих злоумышленников по группам (от одиночки до террористов), различающихся профессиональными знаниями, намерениями, отношением к риску и финансовыми возможностями. Вторая заключается в объединении количественной и качественной оценки рисков. Позволяет существенно сократить количественные вычисления за счет угроз, которые были отсеяны на этапе качественной оценки рисков по заданному множеству параметров в частности, по отношению к риску злоумышленника.

ЛИТЕРАТУРА

1. 3. NIST Special Publication 800-30 Rev A. Risk management Guide for information Technology Systems, Gary Stoneburner, Alice Goguen, and Alexis Feringa.

2. Симонов С.В. Методология и технологии анализа рисков // Вопросы защиты информации: науч.-практ. ж. 2003. № 1. С. 25–33.

3. Методы и средства анализа рисков и управление ими в ИС. BYTE / Россия № 12. 2005 – http://www.bytemag.ru/?ID=605155.

4. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб.: БХВ-Петербург, 2003. 752 с.

5. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. СПб.: Питер, 2003. 368 с. (Сер. «Классика computerscience»).

6. Руководящий документа Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» –
http://www.gtk.lissi.ru/doc.phtml?DocumentID=1

ПОЛИГРАФ НА ОСНОВЕ РЕЧЕВОГО ВВОДА

М.Э. Раисов, студент 5-го курса, каф. РЗИ,
Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС
г. Томск, ТУСУР, т. 8-923-421-68-28, ramax@sibmail.com

Проблема обнаружения лжи существует столько же, сколько существует и сам человек. С целью выявить и зафиксировать обман и был разработан прибор **полиграф**, получивший в 20-х годах двадцатого века название «**детектор лжи**». Современный полиграф фиксирует сигналы, поступающие с датчиков, которые прикреплены к различным участкам тела. Они могут фиксировать до 50 физиологических параметров: покраснение лица или его отдельных частей, подрагивание губ, расширение или сужение зрачков, учащенное моргание, речь и другие изменения, которые могут свидетельствовать о лжи. В этой работе рассматривается модель полиграфа, позволяющего анализировать человеческую речь. Считается, что если подозреваемый сообщает заведомую ложь, у него изменяется состояние голосовых связок, которые производят несколько искаженный звук за счет нерегулярного изменения основной частоты вибрации. Оно не контролируется силой воли так, как можно контролировать дыхание [6].

Судебные психофизиологические экспертизы с использованием полиграфа проводятся в рамках уголовного и гражданского процессов, а также по делам об административных правонарушениях. Данный вид экспертизы назначается при наличии неустранимых противоречий в показаниях участников процесса или в случае противоречия между показаниями и другими доказательствами по делу.

Заключения психофизиологической экспертизы признаются в качестве доказательств по уголовным делам, и выводы экспертов используются судами при постановке приговора – как обвинительного, так и оправдательного [2–5].

Очень важно, чтобы испытуемые не отвлекались во время тестирования на полиграфе, так как это может оказать влияние на результат. Также экспериментатор и оборудование должны находиться позади испытуемого. Более того, испытуемым запрещается двигаться и позволено отвечать на вопросы только «да» или «нет», поскольку движения и речь могут привести к нежелательным физиологическим реакциям. Становится очевидным, что сотрудничество с испытуемым является необходимым условием проведения тестирования. Поэтому участие возможно только на добровольной основе, причем у испытуемых есть право прекратить тест в любое время. Однако прекращение тестирования выглядит нежелательным, поскольку может навлечь на испытуемого еще большие подозрения [6].

Типичный тест контрольных вопросов состоит из четырех этапов.

На первом этапе экзаменатор формулирует и обсуждает с испытуемым те вопросы, которые будут задаваться во время тестирования на полиграфе. Существует три типа вопросов, а именно: нейтральные, значимые и контрольные.

Нейтральные вопросы относятся к разряду общих и не должны вызывать возбуждения. Значимые вопросы – это специальные вопросы, касающиеся преступления. Контрольные вопросы имеют отношение к поступкам, которые связаны с расследуемым преступлением, но непосредственно на него не указывают.

У невиновного подозреваемого контрольные вопросы будут приводить к более сильному возбуждению, а у виновного значимые.

Второй этап – стимулирующий тест. Цель стимулирующего теста – убедить испытуемого в точности техники.

Третий этап – основной тест.

Точная формулировка контрольных вопросов зависит от конкретных обстоятельств. Одинаковая последовательность вопросов задается по крайней мере три раза, для того чтобы исключить случайные различия в физиологических реакциях между контрольными и значимыми вопросами. То есть может так произойти, что невиновный испытуемый случайно даст очень сильную реакцию на один из значимых вопросов. Чем больше вопросов задает экзаменатор, тем меньше будет влияние случайных реакций на окончательный результат.

Для оценки параметров голоса использовалось программное обеспечение «Полиграф», которое выполняет со звуковыми файлами операции «Фильтрация», «Сегментация» и «Графики». При этом звуковые файлы должны отвечать следующим требованиям: тип файла – wav, частота дискретизации – 12 кГц, 16 бит, моно. Сначала wav-файл вводится в модуле «Фильтрация» программы sr. После фильтрации в папке с wav-файлом (например, 1.wav) появляется 3 файла с именами: 1.y2, 1Freq.y2, 1Mask.y2. Затем в модуле «Сегментация» выбирается файл 1Mask.y2. После сегментации появляется файл 1Mask.y2.ff. Затем в модуле «Графики» выбирается файл 1.y2. После прорисовки графиков появляется папка с именем wav-файла, где расположены сохранённые рисунки.

После проведения оценки параметров голоса с использованием теста контрольных вопросов и программного обеспечения «Полиграф» были получены следующие результаты.

Последний, четвертый, этап теста заключается в интерпретации диаграмм полиграфа. Существует два метода интерпретации данных, а именно, общий подход и подход числового выражения.

В рамках общего подхода полиграфолог составляет впечатление о физиологических реакциях испытуемого на тест. В рамках метода числового выражения проводятся сравнения между реакциями на значимые вопросы и последующие контрольные вопросы (З–1 сравнивается с К-1, З–2 сравнивается с К-2, а З–3 – с К-3). Возможны четыре варианта. Если различий в физиологической реакции нет, присваивается значение 0. Если различия заметные, ставится 1 балл, тогда как 2–3 балла присваиваются, соответственно, сильным и очень выраженным различиям. Итак, мы видим, что реакция на К1 намного сильнее, чем на З1, следовательно, присваиваем «+3». Реакция на З2 сильнее, чем на К2, присваиваем «–1». Реакция на К3 намного сильнее, чем на З3, присваиваем «+3». Реакция на К4 сильнее, чем на З4, присваиваем «+2». В итоге получаем 3 – 1 + 3 + 2 = +7, что позволяет нам считать тест пройденным [1].

Делаем заключение – подозреваемый не виновен.

Все зависит от навыков специалиста проводить серьезный критический разбор тестирования, а также его опыт. К сожалению, многим не хватает соответствующей подготовки в области психодиагностики, и они не знакомы с базовыми концепциями и требованиями стандартизированного психологического теста. Эти проблемы усиливаются, когда экзаменатор формулирует и предъявляет контрольные вопросы испытуемому, поскольку очень трудно стандартизировать формулировку и процедуру обсуждения вопросов для всех испытуемых. Многое зависит от того, каким образом испытуемый воспринимает контрольные вопросы и реагирует на них по ходу предварительного интервью.

ЛИТЕРАТУРА

1. Vrij A. Detecting Lies and Deceit. New York, 2000. 270 с.
2. Уголовно-процессуальный кодекс Российской Федерации.
3. Гражданско-процессуальный кодекс Российской Федерации.
4. Кодекс Российской Федерации об административных правонарушениях.
5. Информационный бюллетень Следственного Комитета при МВД России. 2006. № 2(128).
6. http://psyfactor.org

РАЗРАБОТКА ТЕКСТОЗАВИСИМОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ ДИКТОРА ПО ГОЛОСУ

А.Н. Ручай
г. Челябинск, ЧелГУ, т. 8-351-799-72-92, ruchai@pochta.ru

За последние несколько десятилетий можно отметить возросший интерес к проблеме идентификации по голосу, в основном он связан как с успехами, достигнутыми в последнее время, так и с большим спектром практических применений данной задачи, а также обусловлен преимуществами установления и проверки подлинности личности по голосу.

В связи с существованием разнообразных методов идентификации личности по голосу, в основном связанных с выбором пространства наблюдений и решающего правила, возникает важность анализа существующих методов с целью выявления наиболее надежных.

Определим центральные понятия классической постановки задачи идентификации диктора по голосу.

Гипотетическим множеством Ω будем называть множество объектов распознавания $\omega \in \Omega$.

Индикаторной функцией будем называть функцию $g(\omega):\Omega \to M$, разбивающую множество Ω на m непересекающихся классов $\Omega_1,\ldots,\Omega_m$, где $M = \{1,\ldots,m\}$.

Пусть $x(\omega):\Omega \to X$ функция, которая ставит в соответствие каждому объекту $\omega \in \Omega$ его образ $x(\omega) \in X$, непосредственно воспринимаемый наблюдателем. Тогда множество X будем называть пространством наблюдения.

Решающее правило $\tilde{g}(x): X \to M$ позволяет наблюдателю распознать класс $g(\omega)$ скрытого объекта $\omega \in \Omega$, опираясь на его образ $x(\omega)$ в пространстве наблюдений X.

Задача идентификации состоит в выделении одного диктора по наблюдаемому голосу из множества известных системе (наблюдателю) дикторов (множество Ω), основываясь на векторе значений признаков, вычисленных по данному речевому сигналу.

Текстозависимые системы идентификации – это системы, которые используют грамматически один и тот же речевой сигнал, другими словами, при обучении и при идентификации диктор должен произносить одно и то же предложение (фразу).

Исходя из формулировки задачи идентификации, выпишем отдельно список алгоритмов и данных, которые необходимо описать, чтобы

метод идентификации диктора по голосу считался описанным полностью.

Пространство наблюдений X описывает векторы признаков, вычисляемых на основе речевого сигнала. Для описания временной структуры речевого сообщения была выбрана динамическая модель, в соответствии с которой исходный речевой сигнал сегментируется на перекрывающиеся сегменты длительностью 1/16 с и с шагом 1/32 с. На каждом из сегментов вычисляются коэффициенты линейного предсказания. По полученным коэффициентам с помощью дискретного преобразования Фурье вычисляется спектр мощности сигнала, который является сглаженным спектром. В вычисленном спектре мощности на каждом из сегментов находят максимум по амплитуде, значение которого будет формировать вектор признаков.

Получаемый спектр не является тем же спектром, что и полученный с помощью преобразования Фурье, потому что для вычисления КЛП используют сотни входных отсчетов, а самих коэффициентов вычисляют не более двух десятков. Тем не менее полученный из КЛП спектр с некоторой точностью совпадает со спектром, полученным с помощью преобразовании Фурье.

Были изучены другие методы обработки речевого сигнала, используемые в текстозависимых системах идентификации для извлечения из сигнала высокоинформативных характеристик. И был сделан вывод о том, что самую высокую надежность в идентификации диктора по голосу дают только робастные характеристики речи. Например, робастными характеристиками являются форманты, которые полагаются частотами и амплитудами максимумов в сглаженном спектре речевого сигнала.

Если признаки объектов обозначить через x^i, где $i=1,\ldots,n$, то каждый объект в n-мерном пространстве признаков может быть представлен в виде вектора, координаты которого характеризуют свойства объекта.

Решающее правило. $\tilde{g}(x)$ обычно задается критерием минимального расстояния от поступившего на вход вектора до всех векторов всех моделей дикторов.

Пусть в результате классификации все множество объектов $\Omega=\{\omega\}$ разбито на непересекающиеся подмножества $\Omega_1,\ldots,\Omega_m$, каждое из которых и будет составлять соответствующий класс. Обозначим объекты, относящиеся к каждому классу, следующим образом: $\Omega_1=\{\omega_{11},\omega_{12},\ldots,\omega_{1k_1}\}$, …, $\Omega_m=\{\omega_{m1},\omega_{m2},\ldots,\omega_{mk_m}\}$.

Для определения меры близости или подобия необходимо ввести метрику. Выбор метрики произволен, необходимо лишь, чтобы она удовлетворяла обычным аксиомам расстояний:

1. $d(a,b)=d(b,a)$;
2. $d(a,c)\le d(a,b)+d(a,c)$;
3. $d(a,b)\ge 0$;
4. $d(a,b)=0\Leftrightarrow a=b$.

В качестве такой метрики можно взять Евклидову метрику

$$d^2(\omega_{pk},\omega_{ql})=\sum_{j=1}^{n}\left(x_{pk}^{j}-x_{ql}^{j}\right)^2,$$

$$p,q=1,\ldots,m;k=1,\ldots,k_p;l=1,\ldots,k_q,$$

где x_{pk}^{j} есть значение j-го признака k-го объекта p-го класса, то есть объекта ω_{pk}; x_{ql}^{j} – значение j-го признака l-го объекта q-го класса, то есть объекта ω_{ql}.

Также можно взять взвешенную Евклидову меру

$$d^2(\omega_{pk},\omega_{ql})=\sum_{j=1}^{n}\lambda_j\left(\tilde{x}_{pk}^{j}-\tilde{x}_{ql}^{j}\right)^2,$$

где λ_j – характеристические числа положительно определенной квадратной матрицы, которая описывает взаимосвязь координат и ортогональных проекций на оси неортогональной системы координат, и $\tilde{x}^j$ – новые значения вектора признаков в новой ортогональной системе координат, полученные с помощью матрицы ортогонализующего преобразования.

Также можно использовать меру Махалонобиса

$$d^2(\omega_{pk},\omega_{ql})=\sum_{j=1}^{n}\mu_j\left(x_{pk}^{j}-x_{ql}^{j}\right)^2,$$

где μ_j – характеристические числа симметрической положительно определенной квадратной обратной ковариационной матрицы, которая описывает взаимное влияние параметров вектора друг на друга.

Также можно использовать меру Хемминга

$$d^2(\omega_{pk},\omega_{ql})=\sum_{j=1}^{n}y_j,$$

где

$$y_j = \begin{cases} 0, & \text{если } x_{pk}^j \in \left[\min\limits_{i=1,..,n} (x_{ql}^i), \max\limits_{i=1,..,n} (x_{ql}^i) \right]. \\ 1, & \text{иначе.} \end{cases}$$

В качестве меры также можно взять меру Чебышева

$$d^2(\omega_{pk}, \omega_{ql}) = \max_{j=1,..,n} \left(x_{pk}^j - x_{ql}^j \right).$$

Рассмотрим величину $S(\omega, \{\omega_g\})$ – меру близости между распознаваемым объектом ω и классом Ω_g, $g = 1,2,\ldots,m$, заданным своими объектами $\{\omega_g\}$:

$$S(\omega, \{\omega_g\}) = \sqrt{\frac{1}{k_g} \sum_{g=1}^{k_g} d^2(\omega, \omega_g)}.$$

Решающим правилом тогда будет

$$\tilde{g}(x(\omega)) = \arg \min_{g=1,..,m} S(\omega, \{\omega_g\}).$$

Выбор метрики в задаче идентификации обусловлен факторами простоты, быстродействия и качества работы системы. Например, вычисление собственных значений матрицы – это сложная задача, поэтому на практике приходится отказываться от прямого поиска собственных чисел матрицы. Также для обеспечения высокой надежности идентификации возникает требование большой обучающей выборки, порядка 30–100 примеров, что осложняет применение таких метрик, как Хемминга и Чебышева. В настоящее время широко используются решающие правила, которые используют нейронные сети с линейными и нелинейными разделяющими функциями.

В рамках данной работы была разработана и реализована открытая текстозависимая система идентификации диктора по голосу. Данная система поддерживает два основных режима работы: обучение системы и идентификацию (рис. 1).

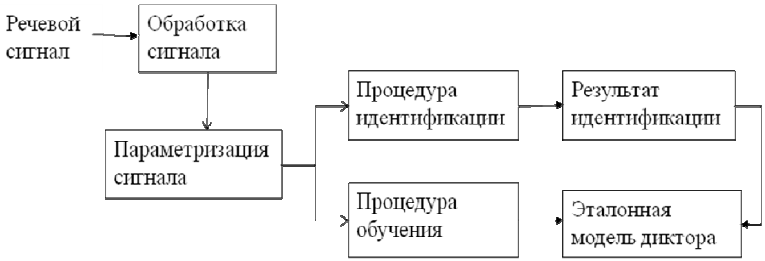


Рис. 1. Схема системы идентификации диктора по голосу

Обработка речевого сигнала заключается в следующих этапах: запись выходных данных с микрофона, дискретизация и квантование сигнала. В связи с тем, что качество распознавания диктора по голосу сильно зависит от качества сигнала, так как системы идентификации чувствительны к фоновому шуму, канальному шуму и искажениям, создаваемым различными микрофонами, то была применена шумоочистка сигнала с помощью вейвлет-преобразования. Нормализация речевого сигнала по времени использовалась для удаления из записанной ключевой фразы слабовыраженных речевых участков, таких как начальные и конечные паузы. Также была реализована процедура сравнения речевых сигналов на временное сходство, которое основывается на том, что длительность произношения одной и той же фразы диктором должна оставаться практически одинаковой.

Параметризация сигнала представляет собой задание индикаторной функции и пространства наблюдений.

Процедура обучения представляет и сохраняет обучающую совокупность как эталонную модель диктора. Для этого пользователю предлагается 3 раза произнести ключевую фразу, ограниченную по длительности 3 с.

Процедура идентификации задается как простое применение решающего правила к данному речевому сигналу. Также стоит отметить то, что система является самообучающейся.

Было проведено тестирование надежности системы. Тестирование проводилось в соответствии с правилами тестирования систем идентификации, установленными в стандарте ИСО/МЭК 19795-1 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии» [9]. Полученные результаты являются независимой оценкой данных систем. Для проведения тестирования была собрана собственная база голосов разных дикторов. В результате качество работы можно оценить ошибкой 1-го рода, равной 0,32, и ошибкой 2-го рода, равной 0,009. В сравнении с другими аналогичными системами эти показатели практически совпадают, и отличие состоит только в том, что разработанная и реализованная система построена с оптимальным выбором ее параметров и представляет собой открытую систему, что позволяет ее использовать для последующих исследований, а также для демонстрации подобных систем.

Таким образом, автором статьи были проанализированы методы и модели текстозависимой идентификации диктора по голосу. Были изучены математические методы обработки речевого сигнала, используемые в системах идентификации для извлечения из сигнала высокоинформативных характеристик. Были проведены исследования по выбо-

ру параметров шумоочистки с помощью вейвлет-преобразования, а также различных оптимальных уровней пороговых значений для временного сходства, минимального уровня спектральной мощности речевого сигнала, длительности сегментации и шага сегментации. Были применены различные метрики для построения решающего правила и сформулированы критерии по выбору метрики в задаче текстозависимой идентификации диктора по голосу. Была разработана и реализована система текстозависимой идентификации диктора по голосу, проведено тестирование надежности реализованной системы.

ЛИТЕРАТУРА

1. Болл Р.М., Коннел Дж.Х., Панканти Ш. и др. Руководство по биометрии / Пер. с англ. Н.Е. Агаповой. М.: Техносфера, 2007. 368 с.

2. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. Пенза: Пенз. гос. ун-т, 2000. 188 с.

3. Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. М.: Радиотехника, 2004. 144 с.

4. Рамишвили Г.С. Автоматическое опознавание говорящего по голосу. М: Радио и связь, 1981. 224 с.

5. Ручай А.Н. Биометрика как метод идентификации диктора по голосовым данным // Студент и научно-технический прогресс: тезисы докладов XXXI студенческой научной и межвузовской научно-практической конференции для студентов классических вузов. Челябинск: ЧелГУ, 2007. С. 97–98.

6. Ручай А.Н. Построение двухфакторной модели идентификации диктора по его речи // Безопасность информационного пространства VI: сборник трудов межвузовской научно-практической конференции студентов, аспирантов и молодых ученых. Тюмень: ТюмГУ, 2007. С. 57–59.

7. Ручай А.Н. Реализация системы текстозависимой верификации диктора по голосу. Безопасность информационного пространства: труды VII региональной научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург: УрГУПС, 2008. С. 83–84.

8. Ручай А.Н. Анализ и реализация методов идентификации диктора по голосу // Студент и научно-технический прогресс: тезисы докладов XXXII студенческой научной конференции. Челябинск: ЧелГУ, 2008. С. 103–105.

9. ГОСТ Р ИСО/МЭК 19795-1. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. М.: ИПК Издательство стандартов, 2006. 97 с.

УПРАВЛЕНИЕ ОПЕРАЦИОННЫМИ РИСКАМИ БАНКОВСКОГО ПЛАТЕЖНОГО ПРОЦЕССА

А.Ф. Саляхов, аспирант, д.т.н., А.И. Фрид, проф., Д.И. Кардаш, к.т.н., доцент

Уфимский государственный авиационный технический университет, т. 8-917-494-20-02, olmik@bk.ru

В современных условиях в процессе взаимодействия информационной системы и человека возникают события, процессы или явления, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации [1]. Указанные явления присутствуют при организации взаимодействия в банковском платежном технологическом процессе (БПТП) [2]. Особенности функционирования БПТП на сегодня таковы, что он представляет определенный операционный риск, связанный с нечетким определением зон ответственности участников БПТП, возможностью участников БПТП бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, отсутствием контроля результатов технологических операций по обработке платежной информации [3, 4]. Описанные проблемы связаны с отсутствием систем управления информационной безопасностью для данного класса технологических процессов, что, в свою очередь, следует из отсутствия моделей угроз и нарушителя информационной безопасности (ИБ) при осуществлении БПТП [5].

Разработка этих моделей для организаций банковской системы рекомендуется Стандартом Банка России (СБР) СТО БР ИББС–1.0–2006 [2]. Необходимо отметить, что на данный момент не существует моделей БПТП, но существует модель электронного документооборота, например, описанная в работах [6, 7]. В качестве недостатков этой модели можно указать то, что она, во-первых, не учитывает требования СБР, во-вторых, не рассматривает модели угроз и нарушителя, а следовательно, не пригодна для моделирования БПТП.

Построение данных моделей позволит использовать их для минимизации операционных рисков при проведении БПТП, прогнозировать ситуации в системе «человек – информационная система», ускорить процесс исследования информационной системы на наличие конкретных угроз и повысить эффективность применения средств обеспечения информационной безопасности БПТП.

Таким образом, для построения указанных выше моделей необходимо разработать методику оценки рисков нарушения ИБ БПТП, построенную с учетом требований СБР и предназначенную для обоснованного выбора средств обеспечения ИБ. Исходной предпосылкой при разработке указанных моделей (используемых в системах управления

информационной безопасностью (СУИБ)), является достижение области минимальных суммарных затрат (рис. 1) при обеспечении информационной безопасности БПТП.

Рис. 1. Соотношение между уровнем защищенности и стоимостью защиты;

C_Σ – суммарная величина затрат при осуществлении ИБ БПТП;

$C_{пот}$ – величина ущерба от нарушения технологического процесса;

$C_{ЗИ}$ – затраты на обеспечение ИБ

Далее предлагается методика оценки рисков нарушения ИБ БПТП. Методика иллюстрируется примерами создания моделей БПТП, угроз и нарушителя информационной безопасности при осуществлении операций над электронным платежным документом (ЭПД).

Методика оценки рисков нарушения ИБ БПТП

1. Выделение операций банковского платежного технологического процесса. Основные операции БПТП и их взаимосвязи, полученные в ходе выполнения данного шага методики, представлены на рис. 2.

2. Выделение требований СБР по обеспечению информационной безопасности банковских платежных технологических процессов.

3. Построение многосвязного ориентированного графа «каждый с каждым», вершины которого соответствуют операциям банковского платежного технологического процесса. Ребра графа обозначают возможность перехода из одной вершины в другую (перехода между операциями банковского платежного технологического процесса). Под входной вершиной будем понимать операцию, с которой начинается БПТП, под выходной вершиной – операцию, на которой заканчивается технологический процесс.

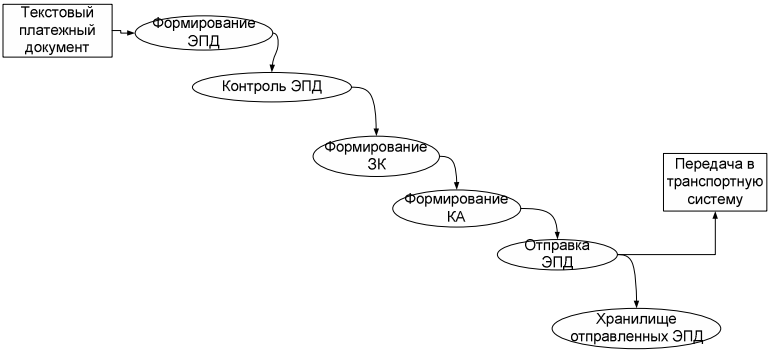


Рис. 2. Основные операции банковского платежного технологического процесса

4. Выполнение усечения графа путем отбрасывания тех ребер, которые не соответствуют логике функционирования процесса – считаются невозможными для осуществления, или вероятность перехода по которым ничтожно мала.

5. Анализируются связи между вершинами графа на предмет соответствия данного перехода требованиям СБР. В разрыв каждого ребра вводится условная вершина с двумя выходами: условие выполнено или нет. Если условие выполняется, то выходное ребро ведет в вершину, соответствующую следующей операции технологического процесса, а если же условие не выполнено, то выходное ребро ведет в специально вводимую вершину, являющуюся результатом нарушения. При этом существующая связь между вершинами убирается. В результате формируется модель угроз ИБ для БПТП, представленная на рис. 3.

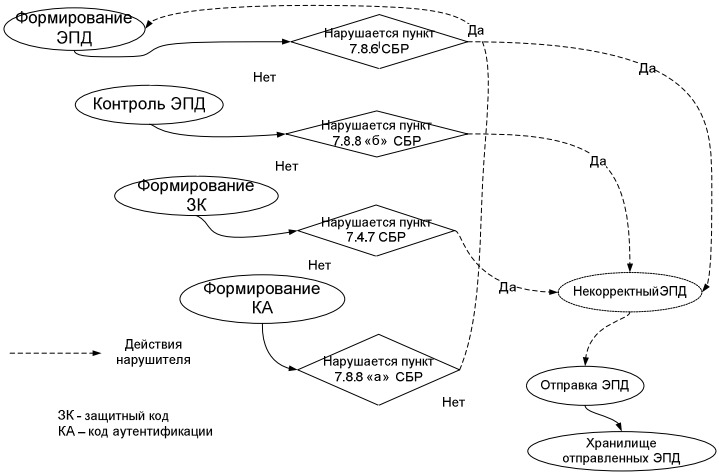


Рис. 3. Модель угроз банковского платежного технологического процесса

6. На основе модели угроз ИБ БПТП делается оценка риска информационной безопасности. Пусть $W=\{w_1;w_1;...w_n\}$ – некоторое пространство элементарных событий, соответствующее дугам модели. Каждому элементу w_i из W поставим в соответствие значение вероятности осуществления соответствующего ему перехода в технологическом процессе – p_i. События активизации каждого из двух выходов вершины условия будут несовместными. Последовательность случайных независимых элементарных событий определим как сложное событие. События обозначим заглавными буквами латинского алфавита A, B, C,... Будем считать, что сложное событие произошло тогда, когда произошла цепочка случайных независимых элементарных событий, соответствующих выполнению переходов от входной до выходной вершины, описанных в п. 3 данной методики. Обозначим вероятности элементарных событий, как показано на рис. 4.

Тогда вероятность сложного события определится как вероятность одновременного наступления нескольких элементарных событий, заключающихся в выполнении вершин графа, определенного в п. 3 данной методики. Примерами вероятности сложных неблагоприятных событий, возможных в ходе осуществления банковского платежного технологического процесса, представленного на рис. 4, являются:

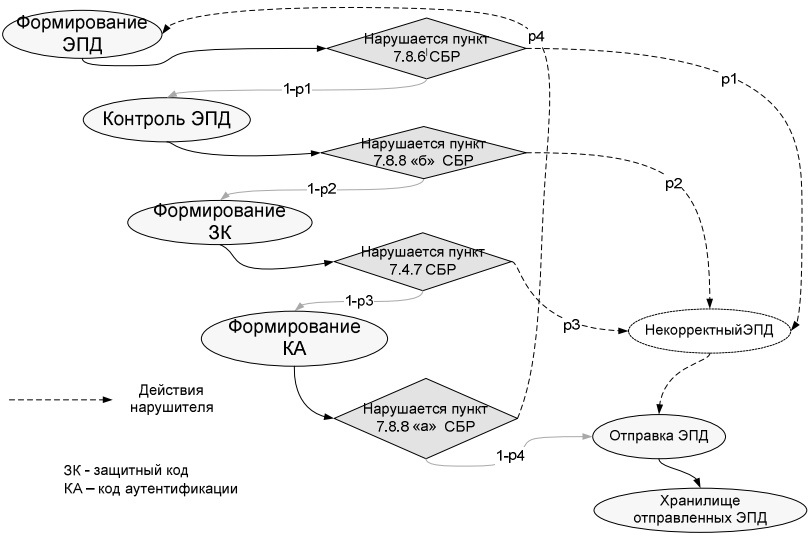


Рис. 4. Вероятности реализации различных угроз БПТП

- $P(A) = p1$ – вероятность попадания ЭПД в «Хранилище отправленных ЭПД» с нарушением п. 7.8.6. СБР, который подразумевает, что операции обработки платежной информации должны контролироваться;
- $P(B) = (1 - p1) * p2$ – вероятность попадания ЭПД в «Хранилище отправленных ЭПД» с нарушением п. 7.8.8 «б» СБР, который подразумевает, что отправляемые ЭПД должны быть защищены от искажения;
- $P(C) = (1 - p1) * (1 - p2) * p3$ – вероятность попадания ЭПД в «Хранилище отправленных ЭПД» с нарушением п. 7.4.7 СБР, который подразумевает невозможность отказа от авторства ЭПД;
- $P(D) = (1 - p1) * (1 - p2) * (1 - p3) * p4 * p1$ – вероятность попадания ЭПД в «Хранилище отправленных ЭПД» с нарушением п. 7.8.8 «а» и 7.8.6 СБР.

Из графа видно, что сложное событие может происходить по различным сценариям. Примем следующие вероятности элементарных событий:

1) Нарушение п. 7.8.6 СБР происходит в 15% случаев;
2) Нарушение п. 7.8.8 «б» СБР происходит в 45% случаев;
3) Нарушение п. 7.4.7 СБР происходит в 40% случаев.

Можно определить значения вероятностей сложных событий: $P(A) = 0{,}15$, $P(B) = 0{,}3825$, $P(C) = 0{,}187$ и $P(D) = 0{,}0021$.

Высчитывается сумма ущерба по каждому сложному событию. Обозначим за X сумму общего ресурса банка, который тратится, в том числе и в ходе выполнения БПТП. Если обратиться к рис. 4, то значения величины ущерба при возникновении сложных событий A, B, C, D окажутся различными. Реализация события A ведет к ущербу $S(A)$ в размере суммы, указанной при формировании ЭПД. Максимальный риск при реализации события A $S(A) = X$. Тогда риск события A можно вычислить по формуле

$$R(A) = p1 * X,$$

где X – общий ресурс банка.

Реализация событий B и C ведет к ущербам $S(B)$ и $S(C)$ соответственно, которые заключаются в наложении штрафных санкций надзорным органом (например, Центром проведения расчетов). Если предположить, что размер штрафа составляет 0,01*X, тогда ущерб $S(B) = 0{,}01 * X$, а $S(C) = 0{,}01 * X$. Риск события B можно вычислить по формуле

$$R(B)=(1-p1)*p2*0{,}01*X\ .$$

Риск события C можно вычислить по формуле:

$$R(C)=(1-p1)*(1-p2)*p3*0{,}01*X\ .$$

Реализация события D ведет к ущербу $S(D)$ который заключается в возможности изменения значения суммы, указанной в ЭПД. Можно предположить, что максимальный риск при реализации события D случается, когда $S(D)=X$. Тогда риск события D можно высчислить по формуле

$$R(D)=(1-p1)*(1-p2)*(1-p3)*p4*p1*X\ .$$

Из методики также можно выделить модель нарушителя, которая может использоваться в комплексе с моделью угроз при дальнейшем построении СУИБ. Модель нарушителя представляет собой множество вероятностей неисполнения требований СБР, множество путей реализации угроз, выделенных в построенной модели угроз. На основании анализа выделенных путей реализации угроз может быть получена классификация нарушителей ИБ БПТП с учетом их мотиваций, включающая описание их опыта и доступных средств реализации угроз [8].

Таким образом предложена методика оценки рисков нарушения информационной безопасности банковского платежного технологического процесса, позволяющая построить модели угроз и нарушителя ИБ БПТП в рамках требований СБР. Построенные модели пригодны для вычислительной реализации и компьютерного моделирования. В дальнейшем предполагается, что разработанные модели будут использованы при построении СУИБ.

ЛИТЕРАТУРА

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

2. Стандарт Банка России СТО БР ИББС–1.0–2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

3. Письмо ЦБ РФ от 24.05.2005 № 76-Т «Об организации управления операционным риском в кредитных организациях» // Вестник Банка России. 2005. № 28.

4. Криворучко С.В. Операционные риски платежных систем: уровни ответственности // Расчеты и операционная работа в коммерческом банке. 2007. № 2.

5. Лямин Л.В. Три составные части и три источника информационной безопасности в кредитных организациях // Управление в кредитной организации. 2006. № 4.

6. Круковский М.Ю. Графовая модель композитного документооборота // Математичні машини і системи. 2005. № 1.

7. Круковский М.Ю. Методология построения композитных систем документооборота // Математичні машини і системи. 2004. № 1. С. 101–114.

8. Саляхов А.Ф., Кардаш Д.И. Модель целенаправленного поведения злоумышленника // Вопросы защиты информации: Научно-практический журнал. М.: ФГУП «ВИМИ». 2007. № 1. С. 8–10.

КОМБИНАТОРНО-ГЕОМЕТРИЧЕСКИЙ МЕТОД ИССЛЕДОВАНИЯ СОВЕРШЕННЫХ ШИФРОВ И ИХ СОВРЕМЕННЫХ АНАЛОГОВ

С.С. Коновалова, аспирант каф. прикладной математики

г. Екатеринбург, УрГУПС, т. (343) 358-55-50, svetlanak@e1.ru

В современном мире для сокрытия информации от злоумышленника активно применяются симметричные блочные шифры, такие как DES и Rijndael=AES, а также асимметричные (RSA). Но они не являются абсолютно стойкими к дешифрованию: их стойкость определяется достаточно большими временными и вычислительными затратами злоумышленника на нахождение ключа. С созданием намного более мощных компьютеров в будущем, в чем не стоит сомневаться, они будут взламываться очень быстро. Выходом может стать применение совершенных шифров, которые являются теоретически стойкими. Это понятие ввел Клод Шеннон в 40-х гг. XX в. [1] как шифра, обеспечивающего наилучшую защиту. В 80–90-е гг. XX в. это понятие было обобщено на шифры, обеспечивающие стойкость к активным криптоатакам. Например, уменьшают вероятность подмены или имитации сообщения так называемые $U(L)$- и $O(L)$-стойкие шифры. На сегодня известно мало о существовании массивов, соответствующих таким шифрам с определенными параметрами. Для применения на практике необходимо стремиться строить массивы с лучшими параметрами стойкости, в том числе с большим значением L.

При исследовании совершенных шифров встает проблема их построения. Чтобы построить совершенные шифры, необходимо применять математические конструкции, комбинаторные конфигурации, формулы зашифрования, которые этим условиям бы удовлетворяли. К числу таких структур могут быть отнесены конечные группы, конечные графы, множества, поля, плоскости, функции и так далее. Такие понятия на интуитивном уровне хорошо понимаются, так как соотносятся с нашими геометрическими и комбинаторными представлениями, но, с другой стороны, эти понятия намного шире и обладают большим набором свойств. И такие комбинаторные конфигурации не-

обходимо использовать для построения новых примеров совершенных шифров.

Так, известны три конструкции [2], позволяющие строить линейные совершенные шифры, каждая из которых определяет свое правило зашифрования. Первая конструкция: $y = xM_k$, где M_k – матрица, построенная на основе линейной рекуррентной последовательности (ЛРП); y, x и k – векторы зашифрованного, открытого текста и ключа соответственно; для зашифрования применяется операция умножения вектора на матрицу. Вторая конструкция: $y = x \cdot k$, где y, x и k – ненулевые элементы поля $GF(q^n)$, а «·» – операция умножения в этом поле. Вторую конструкцию можно обобщить до третьей: $y' = x' \cdot k'$, где $x' = xA$, $k' = kB$, $y' = yC$; A, B, C – невырожденные матрицы. Она дает мультипликативный шифр.

Цель работы – решить конкретные давно поставленные проблемы, тем самым получить новые знания о классических эндоморфных совершенных шифрах и их современных аналогах.

Объект исследования – классические эндоморфные совершенные шифры, $U(L)$-стойкие шифры, $O(L)$-стойкие шифры.

Предмет исследования – комбинаторные конструкции данных шифров.

Используемые методы – математические и криптографические преобразования, геометрические построения, алгебраическая и дискретно-геометрическая методика исследования конструкций совершенных шифров, комбинаторные вычисления, построение аналогий и проведение сравнений.

1. Решение трех задач о трех конструкциях совершенных шифров. О классических линейных эндоморфных совершенных шифрах, описанных в 1987 г. западными криптологами [3], в том числе классиком криптологиии J. Massey, в книге [2] (которая в данной работе была взята за основу), были поставлены следующие задачи:

1. Является ли шифр конструкции 1 мультипликативным шифром?

2. Является ли любой совершенный билинейный шифр мультипликативным шифром?

3. Является ли любой совершенный линейный шифр билинейным шифром?

Для решения *первой задачи* была доказана

Теорема 1. *Конструкция* 1 *задает мультипликативный шифр вида* $y = u \cdot k$, $u = xM_e$.

Таким образом, был осуществлен переход от умножения вектора на матрицу конструкции 1 к умножению элементов в конечном поле. Поэтому попытка западных криптографов выйти за рамки мультипли-

кативных совершенных шифров с помощью конструкции ЛРП не увенчалась успехом и дополнительное усложнение шифра при помощи матриц *A*, *B*, C на самом деле может быть достаточно легко раскрыто злоумышленником.

Заметим, что изотопия, указанная в теореме 1, приводит конструкцию 1 к мультипликативному шифру не только для примитивного, но и для любого неприводимого многочлена. Примитивность многочлена не столь существенна, важно лишь наличие таблицы перекодирующего изоморфизма, а это очевидно имеет место для любого неприводимого многочлена.

Для решения *второй задачи* была использована теорема Алберта для коммутативной квазигруппы и абелевой группы. Было доказано, что билинейные немультипликативные совершенные шифры строятся в недезарговых конечных плоскостях, к которым в том числе относится частный случай системы Веблена–Веддерберна – полуполе, не сводящееся к полю. Примерами таких полуполей является полуполе Алберта и полуполе Дональда Кнута [4]. Значит, доказана

Теорема 2. *Существуют билинейные немультипликативные совершенные шифры*.

Наблюдение 1. *Набор матриц* M_k *приводит к совершенному шифру тогда и только тогда, когда* $\det [M(k') - M(k)] = 0$ *для любых различных ненулевых* k' *и* k.

Утверждение 1. *Все билинейные двумерные и трехмерные совершенные шифры над полем из двух элементов мультипликативны*.

Итак, в ходе решения второй задачи удалось расширить класс линейных совершенных шифров и была получена возможность эффективной проверки шифра на мультипликативность. Пусть злоумышленник перехватывает сообщение и хочет выяснить наличие этого свойства у шифра, чтобы правильно найти ключ. Он знает таблицу умножения (в силу второго правила Керкхгоффса). Если известна только часть циклической таблицы, то можно всю ее восстановить. Затем смотрим наличие единицы в ней. Если квазигруппа ассоциативна, то шифр мультипликативный. Если есть единица, по теореме Алберта квазигруппа изоморфна мультипликативной группе поля, и злоумышленник может одним преобразованием расшифровать шифр, полученный путем трех преобразований. Найдя изоморфизм, получим умножение в поле, которое хорошо известно. Если единицы нет, то находим изотопию, которая превращает квазигруппу в квазигруппу с единицей и осуществляем аналогичные действия. Таким образом, расширение линейных совершенных шифров при помощи мультипликативных несущественно усложняет первые, лучше использовать недезарговы плоскости.

Для решения *третьей задачи* докажем, что не любой совершенный линейный шифр является билинейным шифром. Очевидно, что для построения такого шифра достаточно подвергнуть ключ k билинейного шифра нелинейному обратимому преобразованию, которых над конечным полем гораздо больше, чем линейных [5].

Например, $y = x \cdot k^h$, $h = 1$, $h \in Z$. При $h = -1$ происходит не зашифрование, а расшифрование текста – явление парастрофии в квазигруппах. Это преобразование, рассматриваемое как оператор зашифрования, линейно по x, но не линейно по k, т.е. это – пример линейного, но не билинейного шифра. Над полем характеристики два можно брать только нечетные h. Очевидно, что при условии взаимной простоты h с $2^m - 1$ возможно построение шифра, который будет линейным, но не билинейным.

Итак, справедлива

Теорема 3. *Любая нелинейная по ключу k изотопия мультипликативной группы поля дает пример линейного, но не билинейного совершенного шифра*.

Решением третьей задачи является и система Холла [4], преимущество которой перед рассмотренной выше (где отсутствует левая единица) в том, что в ней есть двусторонняя единица.

Теорема 4. *Система Холла дает пример двумерного над данным полем линейного, но не билинейного совершенного шифра на основе квазигруппы с двусторонней единицей*.

Таким образом, теорема 3 открывает большие перспективы построения более стойких совершенных шифров, так как существование линейных, но не билинейных шифров расширяет область перебора злоумышленнику.

Обобщая результаты решения всех трех задач [6], можно уточнить классификацию линейных шифров, которая в окончательном варианте показана на рис. 1.

Воспользуемся теперь выявленной связью совершенных шифров с конечными плоскостями для изучения имитостойких совершенных шифров.

2. Конструкции совершенных шифров, стойких к другим видам криптоатак. Перейдем к рассмотрению $U(L)$- и $O(L)$-стойких шифров и соответствующих им массивов $PA_1(L, \lambda, \mu)$ (или $CPA_1(L, \lambda, \mu)$) и $A_1(L, \lambda, \mu)$ (или $CA_1(L, \lambda, \mu)$) [2].

Перенесем область их рассмотрения в область дискретной геометрии – конечные плоскости. Это становится возможным благодаря следующей теореме.

Теорема 5. *Построение эндоморфного O* (2)*-стойкого шифра с минимальным числом ключей равносильно построению конечной аффинной плоскости*.

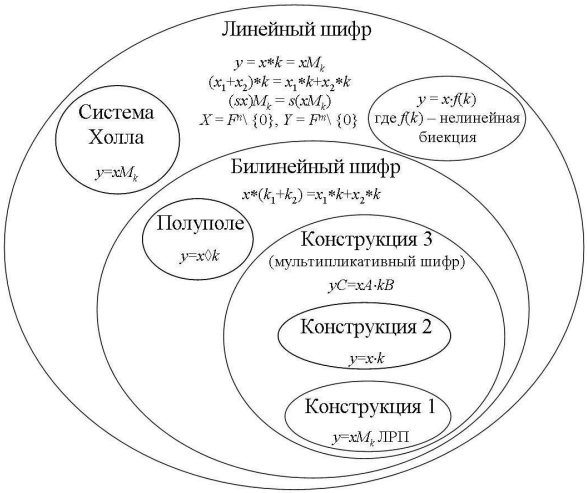


Рис. 1. Классификация линейных совершенных шифров

Утверждение 2. *Построение $O(L)$-стойкого шифра приводит к пороговой схеме разделения секрета* $(L, 2L–1)$.

Если массивы построены по системам Веблена–Веддерберна, не сводящимся к полям, то они дают примеры линейных $O(2)$-стойких шифров со свойствами, отличающимися от привычных свойств дезарговых плоскостей.

При исследовании эндоморфных $U(2)$- и $O(2)$-стойких шифров с минимальным числом ключей в системах Веблена-Веддерберна была установлена взаимосвязь между ними, которую можно сформулировать через следующую теорему.

Теорема 6. *Если имеется эндоморфный $U(2)$-стойкий шифр, то существует конечная плоскость, соответствующая O (2)-стойкому шифру, которая допускает инволюцию $m \mapsto –m$. Обратно: если имеется $O(2)$-стойкий эндоморфный шифр, представляющий собой набор прямых в системе Веблена–Веддерберна, то в нем можно выделить $U(2)$-стойкий подшифр только тогда, когда квазигруппа по умножению допускает такой набор инволюций m_a, что при $m \in M$ имеем $(((m_{a_1})_{a_2})_{a_s}) \in M$ в том и только том случае, когда s четно.*

Заметим, что для общего случая произвольной тернарной операции результат может и не иметь места. Итак, полное изучение взаимосвязи эндоморфных $U(2)$- и $O(2)$-стойких шифров приводит к изучению групп, порожденных инволюциями.

Также были получены условия для проверки линейных шифров на совершенность, а линейных и циклических шифров – на $O(2)$- и $U(2)$-стойкость.

Далее были исследованы различные типы конечных плоскостей для возможности построения $O(L)$- и $U(L)$-стойких шифров на их основе: система Холла (являющаяся решением второй задачи); почти-поля, не сводящиеся к полям, вместе с исключительными случаями; плоскости Мёбиуса, а также группы Матьё, задаваемые некоторыми подстановками элементов конечного множества [2, 4, 7–9]. В ходе анализа были получены некоторые результаты по таким системам, в том числе конкретизованы связи между ними (рис. 2).

Были построены следующие массивы $O(L)$- и $U(L)$-стойких шифров:

− $CPA_1(2, 7, 7)$, соответствующий $U(2)$-, и $CA_1(2, 7, 7)$, соответствующий $O(2)$-стойкому шифру, на основе известной из [2] формулы зашифрования $y = ix + j$.

− $A_1(2, 9, 9)$ по формуле $y = xM_k + \ell$, где векторы x, y, k, ℓ – элементы поля $GF(9)$, а M_k – матрица зашифрования Холла, $f(x) = x^2 + 1$. Из него выделен массив $PA_1(2, 9, 9)$.

Рис. 2. Тернарная операция

− $A_1(2, 9, 9)$, используя ту же формулу, но с $f(x) = x^2 + 2x + 2$.

− $PA_1(3, 8,8) = A_1(2, 8, 8)$ на основе конечной плоскости по формуле $y = x \cdot k + \ell$, где умножение производится в поле $GF(8)$ по таблице

степеней корня $f(x)=x^3+x+1$ или $f(x)=x^3+x^2+1$. Приводит к $U(3)$- или $O(2)$-стойкому шифру.

− $A_1(3, 6, 6)$ на основе группы PGL(2, 5) в виде дробно-линейной функции $f(x) = (ax + b)/(cx + d)$ с элементом ∞: $f(\infty) = a/c$, $f(-d/c) = \infty$. a, b, c, d – элементы поля $GF(5)$. Приводит к $O(3)$-стойкому шифру.

− $PA_1(3, 32, 32)$ в поле $GF(32)$ по формуле $y = x^{\sigma} \cdot k + \ell$, где $\sigma = 2^j$, $j=\{0...4\}$.

− $A_1(2, 9, 9)$ по формуле $y = x \circ k + \ell$, где x, y, k, ℓ – элементы поля $GF(3^2)$, операция «о» – умножение в почти-поле $K(9)$, $f(x) = x^2 + 2x + 2$.

Найден целый класс $O(3)$-стойких шифров на основе дробно-линейных подстановок в почти-полях.

Отметим, что в ходе исследования плоскостей Мёбиуса была установлена возможность построения неэндоморфных $U(3)$-стойких шифров на основе данного типа инверсной конечной геометрии и соответствующих эндоморфных $U(3)$-стойких шифров.

Таким образом в работе получены результаты как по классическим совершенным шифрам, так и по их современным аналогам.

Результатом исследования первых стало решение трех классических задач о трех конструкциях совершенных шифров, выявившее возможности практического применения известных конструкций таких шифров. При решении второй задачи была разработана геометрическая методика исследования конструкций совершенных шифров. Она состоит в том, что для построения линейных совершенных шифров можно использовать не только алгебраические, но и геометрические конструкции. Данная методика была успешно применена на $O(L)$- и U(L)-стойкие шифры благодаря установлению связи $O(2)$-стойких шифров с конечными плоскостями.

Результатом исследования современных аналогов совершенных шифров стало построение таких шифров для $L = 2$ и $L = 3$ в различных системах. Также была установлена связь между $O(2)$- и $U(2)$-стойкими шифрами, что позволит не искать новые конструкции таких шифров, а выделять их из существующих при определенных условиях, или, наоборот, дополнять до необходимых.

Полученные в работе результаты позволили расширить существующую теорию совершенных шифров, а также изучить свойства различных типов конечных плоскостей.

Развитие существующих методов и привлечение более тонких комбинаторных, алгебраических, геометрических свойств и приемов не может не привести к эффективным критериям существования совершенных шифров и их современных аналогов, применимых в теоретических исследованиях и на практике, а также к исследованию современных аналогов совершенных шифров с лучшими параметрами стой-

кости. Для получения в дальнейшем новых результатов в этой области следует расширить обычные рамки, в пределах которых исследуются применяемые математические структуры для установления новых связей между понятиями.

ЛИТЕРАТУРА

1. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 333–369.

2. Зубов А.Ю. Совершенные шифры. М. : Гелиос АРВ, 2003. 160 с.

3. Massey J., Maurer U., Wang M. Non-expanding, key minimal, robustly-perfect, linear and bilinear ciphers // Proceedings «Advances in Cryptology». Crypto'87. 1987. P. 237–247.

4. Холл М. Комбинаторика. М.: Мир, 1970. 424 с.

5. Артин Э. Геометрическая алгебра. М.: Наука, 1969. 284 с.

6. Коновалова С.С., Титов С.С. О конструкциях эндоморфных совершенных шифров // Материалы междунар. науч. конф. по проблемам безопасности и противодействия терроризму / Интеллектуальный центр МГУ, 2–3 ноября 2005 г. М.: МЦНМО, 2006. С. 168–180.

7. Картеси Ф. Введение в конечные геометрии: Пер. с англ. М.: Наука. Гл. ред. физ.-мат. лит., 1980. 320 с.

8. Коновалова С.С., Титов С.С. Построение $O(L)$- и $U(L)$-стойких шифров в конечных плоскостях // Материалы междунар. науч. конф. по проблемам безопасности и противодействия терроризму / Интеллектуальный центр МГУ. М.: МЦНМО, 2008.

9. Коновалова С.С., Титов С.С. Изучение свойств системы Холла для построения совершенных шифров // Сборник научных трудов «Проблемы прикладной математики и механики»: под общ. ред. С.Л. Дерябина. Екатеринбург: УрГУПС. 2008. Вып. 65(148). С. 202–211.

О ЗАДАЧЕ КРИПТОГРАФИЧЕСКОГО СЖАТИЯ ИЗОБРАЖЕНИЙ В ТЕЛЕМЕДИЦИНЕ

А.В. Ветлов, аспирант каф. БИС

г. Самара, СамГУ, т. 8-846-278-09-41, fonesquire@inbox.ru

Постановка проблемы криптографического сжатия изображений актуальна для приложений телемедицины. С одной стороны, необходимо обеспечить конфиденциальность хранимой и передаваемой информации, а с другой – эффективность ее хранения и передачи. При этом для задач медицины зачастую недопустимы искажения информации, свойственные широко используемым алгоритмам сжатия изображений «с потерями». Работа фокусируется на анализе некоторых существующих подходов к криптографическому сжатию изображений, целесообразности их практического применения в области телемедицины, а также на критике отдельных разработок.

Тривиальным решением задачи устранения избыточности и обеспечения конфиденциальности передаваемых (хранимых) изображений видится последовательное применение к исходному изображению сжимающего и криптографического преобразований. Такая последовательность позволит, с одной стороны, сжать изображение, а с другой – очевидным образом улучшить статистические характеристики зашифрованного сообщения за счет уменьшения избыточности открытого сообщения. Обратная последовательность нецелесообразна, поскольку криптографическое преобразование увеличивает энтропию сообщения, т.е. зашифрованное изображение окажется практически несжимаемым.

Однако описанный подход (будем называть его «сжатие + шифрование») на практике имеет ряд недостатков, а именно:

− время на обработку информации тратится неэффективно, поскольку последовательно применяется пара не связанных между собой алгоритмов;

− применение универсальных алгоритмов сжатия информации может раскрыть криптоаналитику некоторые элементы открытого сообщения вследствие повторяемости структуры сжатых файлов.

Под термином «криптографическое сжатие» понимают некоторое единое преобразование, не сводимое к схеме «сжатие + шифрование» и не обладающее указанными недостатками.

Имеющее место разделение алгоритмов сжатия и шифрования обусловлено существованием определенной «конкуренции целей» этих преобразований. Сжатие – это процесс устранения избыточности представления информации. Шифрование стремится увеличить энтропию выходных данных с тем, чтобы криптоаналитик не имел возможности использовать статистические зависимости шифртекста для проведения успешного криптоанализа.

В связи с указанными особенностями сжимающего и шифрующего преобразований вопрос о нахождении единого алгоритма «криптосжатия» (*crypto-compression*), решающего обе указанные задачи сразу, является весьма актуальным.

Ниже анализируются имеющиеся работы в обозначенной области с точки зрения применения и развития их результатов для решения задач криптографического сжатия медицинских изображений.

Анализ подходов к криптографическому сжатию изображений с потерями. Основная идея, на которой базируются подходы к криптографическому сжатию изображений с потерями, заключается в (частичном) шифровании коэффициентов матриц преобразований, используемых в существующих алгоритмах сжатия изображений с потерями, которые распространены довольно широко.

Наиболее разработанными направлениями являются:

− частичное шифрование квадротомического представления;

− частичное шифрование коэффициентов дискретного косинусного преобразования (ДКП);

− частичное шифрование коэффициентов дискретного вейвлет-преобразования (ДВП).

В рамках первого направления интерес представляют работы [1–3]. Второму направлению посвящены работы [4–7]. В [4] предложен собственный метод «зигзагообразного перемешивания» коэффициентов ДКП, однако тенденцией является использование стандартных алгоритмов шифрования. В частности, работа [7] посвящена применению блочного алгоритма *AES* для шифрования изображений в формате *JPEG*. Указанная тенденция характерна для всех трех направлений. Третье направление развивается в работах [8, 9].

В качестве общего недостатка работ по криптографическому сжатию изображений с потерями можно указать тот факт, что стойкость разрабатываемых схем авторами зачастую не исследуется, либо приводимые в работах исследования недостаточны. Само по себе использование стандартных алгоритмов шифрования не означает, что стойкость всей схемы определяется стойкостью этих алгоритмов (чаще на практике наблюдается обратное), и не гарантирует обеспечение конфиденциальности, поскольку шифрованию подвергаются не сами произвольные данные, а результат их обработки при помощи некоторого осредняющего преобразования.

Следует также отметить, что для задач медицины сжатие изображений с потерями обычно не применяется. Это обусловлено сложностью формализации критерия определения допустимого уровня искажений. При этом искажение какой-нибудь «незначительной» детали может повлиять на здоровье и жизнь пациента. Уместно предположить, что криптографическое сжатие с потерями пока неприменимо в области телемедицины по схожим причинам.

Анализ подходов к криптографическому сжатию изображению без потерь. Подходы к криптографическому сжатию можно разделить, как и алгоритмы сжатия, на универсальные и специализированные. К наиболее разработанным универсальным подходам можно отнести криптографическую модификацию алгоритма сжатия Хаффмана.

В частности, в [10] показывается, что проблема декодирования кодов Хаффмана является *NP*-полной для некоторых способов кодирования. Работа [11] посвящена криптоанализу текста, сжатого по Хаффману, в предположении, что использованное дерево Хаффмана аналитику неизвестно. В этой работе Ривест делает вывод, что в такой ситуации криптоанализ является невозможным в некоторых случаях.

В простейшем случае, согласно [12], для получения алгоритма криптографического сжатия из алгоритма сжатия по Хаффману достаточно ассоциировать с каждым уровнем дерева Хаффмана один бит секретного ключа. В этом случае каждый код Хаффмана складывается по модулю два с соответствующей позицией секретного ключа.

В работе [13] показана возможность эффективной реализации кодов ограниченной длины с незначительным ухудшением степени сжатия. В работах [14, 15] указанный подход развивается. Для улучшения криптографических характеристик предлагается использовать гомофоническую подстановку, «канонические» коды Хаффмана и перемешивание открытого текста.

Важной особенностью упомянутых подходов является тот факт, что взлом таких систем криптографического сжатия сводится к решению *NP*-полной задачи. Это показано в [16].

Универсальные алгоритмы криптографического сжатия без потерь не рассчитаны на использование особенностей данных, с которыми оперируют, что неизбежно сказывается на сжимающих характеристиках этих алгоритмов. С точки зрения практического применения криптографического сжатия в области телемедицины предпочтительным сценарием является разработка специализированных методов.

О создании специализированного метода криптографического сжатия, ориентированного непосредственно на медицинские изображения, заявляют авторы работы [17].

Основной упор в [17] сделан на шифровании медицинских изображений. Авторы рассматривают три варианта шифрования:

− применение алгоритма блочного шифрования TEA в режиме электронной кодовой книги (ЭКК) к несжатому изображению;

− применение авторской модификации шифра Виженера к несжатому изображению;

− сочетание сжатия изображения при помощи модификации *RLE*-алгоритма, ориентированной на размер блока алгоритма *TEA*, с блочным шифрованием при помощи *TEA* в режиме ЭКК.

Авторы делают справедливый вывод о том, что первый способ не обеспечивает достаточной стойкости. Однако другие режимы блочного шифрования ими не рассматриваются.

Последний вариант кодирования изображений авторы называют «криптосжатием», делая акцент на том, что оба преобразования выполняются одной и той же программой.

Следует отметить, что, несмотря на выбранное название и особенности программной реализации, схема, предложенная авторами [17], полностью совпадает со схемой «сжатие + шифрование» и обла-

дает всеми ее недостатками, т.е. криптографическим сжатием в описанном в настоящей работе смысле не является.

Рассмотренные подходы к криптографическому сжатию изображений с потерями для приложений телемедицины практически неприменимы, поскольку отсутствие искажений в изображениях является жестким требованием этой области, необходимым для уменьшения вероятности врачебной ошибки.

Среди существующих подходов к криптографическому сжатию без потерь следует выделить подход на основе случайных префиксных кодов. Однако указанный подход является универсальным методом криптографического сжатия, не использующим специфику изображений как исходных данных. Возможно, разработка специализированного метода, ориентированного непосредственно на обработку изображений, относящихся к некоторому определенному классу, позволит существенно улучшить характеристики криптографического сжатия.

В целом можно заключить, что направление криптографического сжатия изображений без потерь на сегодня разработано недостаточно. Вместе с тем это направление является практически значимым в связи с бурным развитием и внедрением телемедицины. Поэтому разработка подходов к криптографическому сжатию изображений, обладающих высокой эффективностью, криптостойкостью и сжимающими характеристиками, является актуальной.

ЛИТЕРАТУРА

1. Chang H.K.C., Liu J.L. A linear quadtree compression scheme for image encryption // Signal Processing: Image Communication. 1997. Vol. 10. № 4. P. 279–290. September.

2. Li X.B., Knipe J., Cheng H. Image Compression and Encryption Using Tree Structures // Pattern Recognition Letters. 1997. Vol. 18. № 11–13. P. 1253–1259. November.

3. Fterich S., Ben Amar C. Crypto-compression d'images fixes par la méthode de quadtree optimisée et AES // CORESA'04, ENIC Télécom, Lille-France, 25–26, p. 169–173, Mai 2004.

4. Lei Tang, Methods for Encrypting and Decrypting MPEG Video Data Efficiently // Proc. of the Forth ACM International Conference on Multimedia '96, Boston, MA, ACM Press, p. 219–229, November 1996.

5. Fisch M., Stogner H. Layered encryption techniques fot DCT-coded visual data // Proc. of the European Signal Processing Conference EUSIPCO'04, vol. 1, Austria, Vienna, p. 821–825, September 2004.

6. Droogenbroeck M., Van and Benedett R. Techniques for a selective encryption of uncompressed and compressed images // ACIVS Advanced Concepts for Intelligent Vision Systems, Ghent, Belgium, p. 90–97, September 2002.

7. Puech W., Rodrigues J.M. Crypto-Compression of Medical Images by Selective Encryption of DCT // Proc. of the European Signal Processing Conference EUSIPCO'05, Antalya, Turkey, September 2005.

8. Benabdellah M., Himmi M.M., Zahid N., Regragui F., Bouyakhf El.H. Encryption-compression of images based on FMT and AES algorithm // Applied Mathematical Sciences. 2007. Vol. 1. № 45. P. 2203–2219.

9. Benabdellah M., Himmi M.M., Zahid N., Regragui F., Bouyakhf El.H. Encryption-Compression of still images using the FMT transformation and the DES algorithm // International Journal of Computer Sciences and Telecommunications. 2006. № 4 (11). P. 22–31. August.

10. Klein S.T., Fraenkel A.S. Complexity Aspects of Guessing Prefix Codes // Algorithmica. 1989. № 12. P. 409–419.

11. Gillman D.W., Mohtashemi M., Ronald L. Rivest: On breaking a Huffman code // IEEE Transactions on Information Theory. 1996. Vol. 42. № 3. P. 972–976.

12. Wayner P.A. Redundancy Reducing Cipher // Cryptologia. 1988. Vol. 12. № 2. P. 107–112.

13. Milidiu R.L., Laber E.S. Improved Bounds on the Inefficient of Length-Restricted Prefix Codes, SPIRE – String Processing and Information Retrieval, 1997.

14. Milidiu R.L., Mello C.G. Fernandes J.R. Adding security to compressed information retrieval systems – SPIRE – String Processing and Information Retrieval. Chile, 2001.

15. Milidiu R.L., Mello C.G. Randomized Huffman codes // PUC-RioInf. Monografias em Ciência da Computação 49/04, December 2004.

16. Milidiu R.L., Mello C.G. A provably secure crypto-compression algorithm – CIBSI 05 – 30. Congreso Iberoamericano de Seguridad Informratica. Chile, 2005.

17. Borie J.C., Puech W., Dumas M. Crypto-Compression Using TEA's Algorithm and a RLC Compression // Proc. of the Intelligent Access to the Multimedia Documents on the Internet (MediaNet'04), Tozeur, Tunisia, p. 5–16, November 2004.

СИСТЕМА ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ

В.Д. Котов, студент 4-го курса, каф. ВТ и ЗИ
г. Уфа, УГАТУ, kotov.v.d@gmail.com

Методы, используемые в современных системах обнаружения атак, делятся на сигнатурные методы и методы обнаружения аномалий. Первая группа методов, несмотря на их высокую эффективность при известных атаках, обладает следующими недостатками:

– необходимость в постоянном обновлении сигнатур;

– разрастание баз данных сигнатур;

– низкая эффективность обнаружения неизвестных атак.

Что касается методов обнаружения аномалий, то и здесь существуют свои минусы, такие как:

– сложность настройки;

– сложность алгоритмов обучения, а также сложности до- и переобучения;

– большое количество ложных срабатываний.

В последнее время перспективным направлением в области защиты информационных систем от вторжения являются технологии искусственных иммунных систем [1, 2]. Принцип их работы основан на моделировании процессов, протекающих в организме при иммунном ответе. Системы обнаружения атак (СОА) на основе технологий искусственных иммунных систем обладают следующими преимуществами:

– способность эффективно реагировать на неизвестные атаки;

– отсутствие сигнатур;

– способность адаптироваться;

– простой алгоритм обучения.

Вместе с тем реализация данных систем требует дополнительного исследования таких вопросов, как:

1) выбор способа построения адекватной математической модели информационной системы;

2) применение иммунологических алгоритмов для выявления расхождений поведения информационной системы (ИС) с нормальным поведением;

3) разработка алгоритмов обучения СОА, а также методов составления обучающей выборки;

4) создание алгоритмов мониторинга, позволяющих СОА обучаться в процессе аудита ИС.

Решаемая задача. Метод, реализуемый в разрабатываемой интеллектуальной системе обнаружения атак, относится к методам обнаружения аномалий. При таком подходе решаются следующие задачи:

1) создание модели нормального поведения информационной системы;

2) разработка способа выявления аномалий.

Существует ряд работ [3–5], в которых показано, что запись последовательностей системных вызовов в операционной системе UNIX, выполняемых различными приложениями, является информативным и приемлемым источником для составления модели поведения информационной системы. Подобный подход, в частности, справедлив и для системных вызовов ОС Windows [6]. Для проведения экспериментов при мониторинге ИС было выбрано 133 системных вызова. Каждый вызов кодируется целым числом (рис. 1), а мониторинг осуществляется путем непрерывного наблюдения за активностью каждого приложения. На рис. 2 приведены графики активности программ svchost.exe и

explorer.exe. Из рисунка видно, что каждое приложение проявляет свойственную лишь ему активность. При длительном наблюдении в активности приложения можно обнаружить повторения, что позволяет судить о том, что при нормальной работе та или иная программа осуществляет конечное число различных последовательностей системных вызовов.

CancelRemoveDevice	1
CancelStopDevice	2
CloseFile	3
……	…
WriteFile	133

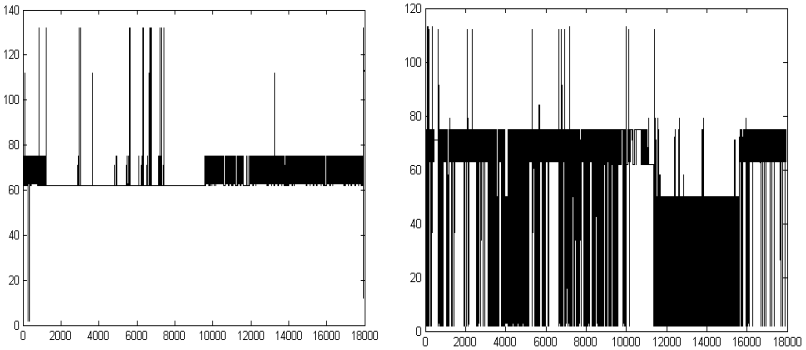
Рис. 1. Способ кодирования системных вызовов

В предлагаемой СОА за основу принят метод представления данных, описанный в [4]:

1) записывается последовательность системных вызовов за некоторый интервал времени;

2) выбираются размер временного окна W_{size} и сдвиг временного окна W_{shift};

3) создается набор строк длины W_{size}, который описывает нормальное поведение системы (рис. 3).



svchost.exe explorer.exe

Рис. 2. Графическое представление активностей процессов svchost.exe и explorer.exe

В исследуемой СОА размер окна $W_{size} = 6$, а размер сдвига $W_{shift} = 1$. Такие параметры позволяют, согласно [4, 6], составить адекватную модель поведения информационной системы. Основная задача системы обнаружения атак состоит в разработке способа мониторинга ак-

тивностей приложений с целью выявления аномального поведения ИС. Для решения задач подобного рода перспективным направлением исследований являются искусственные иммунные системы.

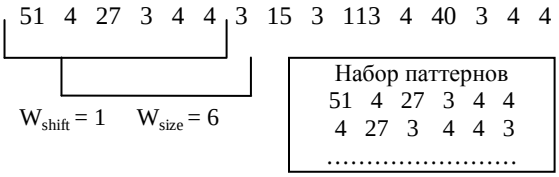


Рис. 3. Способ формирования набора строк для описания поведения системы

Идея построения искусственной иммунной системы. В организме при попадании вредоносных микроорганизмов (антигенов) возникает иммунный ответ. Главными участниками иммунного ответа являются лимфоциты, способные узнавать антигены и уничтожать их, а также при определенных условиях претерпевать мутации, чтобы приобрести способность быстрее распознавать враждебные клетки. Особенностью лимфоцитов является то, что они способны узнавать только инородные клетки. Такую способность они приобретают при созревании, когда популяция лимфоцитов сравнивается с клетками организма и те лимфоциты, которые реагируют на собственные клетки организма, отвергаются. Данный процесс называется отрицательным отбором.

На основе данного процесса разработан алгоритм отрицательного отбора, описанный в [7] (рис. 4). В данном случае S – массив паттернов нормальной активности, полученных в результате наблюдения за системными вызовами. В результате выполнения алгоритма будет получен набор детекторов R, каждый из которых не совпадает ни с одной из строк в S.

Считается, что совпадение происходит только тогда, когда две строки совпадают в *r* смежных позициях.

В исходной статье [5] детекторы генерируются случайным образом, что приводит к большим аппаратным затратам. В предлагаемой СОА детекторы генерируются на основе алгоритма клональной селекции [6]. Работа алгоритма сводится к следующим шагам:

1) создание случайным образом массива строк над заданным алфавитом – потенциальных детекторов;

2) для каждого созданного детектора:

2.1) вычисление аффинности по формуле

$$Aff = \sum_{i=1}^{N_S} aff_i \,, \qquad (1)$$

где aff_i – аффинность данного детектора с i-й строкой (см. далее); N_S – число строк, характеризующих поведение системы;

2.2) каждый детектор копируется $(l*N - Aff)c$ раз, где l – длина строки, и каждая копия претерпевает мутацию в $Aff*c$ позициях; c – параметр, выбираемый в зависимости от решаемой задачи;

3) вычисляется аффинность для каждого детектора и выбирается n строк, аффинность которых минимальна.

Алгоритм завершается, когда будет получено необходимое число детекторов N_R.

Поиск аномалий заключается в непрерывном сравнении вновь поступающих паттернов в S с детекторами. Если происходит совпадение, то детектирована аномалия (рис. 5).

Как показывают исследования, данный подход к обнаружению аномалий позволяет эффективно выявлять отклонения в поведении системы при количестве детекторов во много раз меньшем, чем набор паттернов нормальной активности.

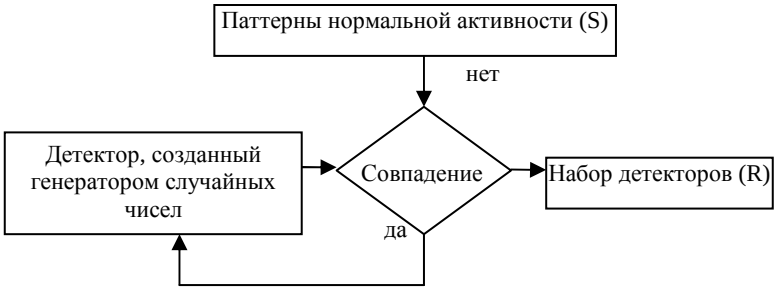


Рис. 4. Алгоритм отрицательного отбора

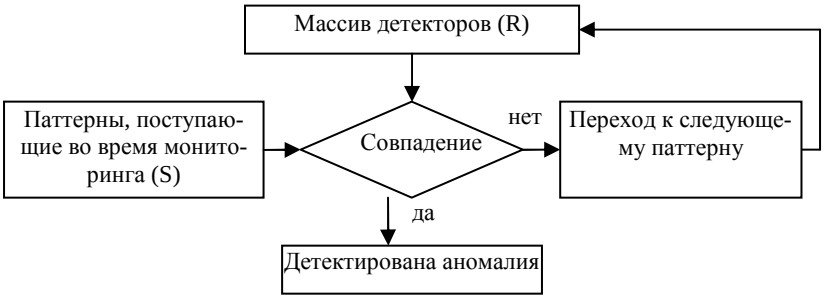


Рис. 5. Алгоритм обнаружения аномалий

Предлагаемая архитектура системы обнаружения атак. В предлагаемой интеллектуальной СОА, при сборе данных и мониторинге

отслеживаемые вызовы группируется по идентификаторам приложений. При обучении системы обучающая выборка также содержит строки данных, сгруппированных по приложениям. Для каждого приложения формируется набор уникальных вызовов, сделанных им за определенное время наблюдения, из которого впоследствии генерируются детекторы отдельно для каждого приложения (рис. 6).

Таким образом, этапы сбора и обработки обучающих данных для СОА – следующие:

1) провести наблюдение за процессами, записав последовательности системных вызовов;

2) сгруппировать полученные данные по идентификаторам процессов;

3) разбить данные на строки с помощью скользящего временного окна;

4) отфильтровать повторяющиеся строки;

5) сгенерировать для каждого из наборов паттернов массив детекторов.

Так как число возможных комбинаций системных вызовов гораздо больше паттернов нормальной активности, то необходимо, чтобы каждый детектор покрывал несколько возможных аномальных паттернов. Важным показателем при сравнении двух паттернов является аффинность, которая в данном случае определяется как количество совпадений в смежных позициях (см. рис. 6).

1	**23**	**35**	**13**	7
15	**23**	**35**	**13**	3
Аффинность *Aff* = 3				

Рис. 6. Схема вычисления аффинности двух паттернов

В том случае, если аффинность больше некоторого порогового значения ε, происходит активация детектора, что влечет за собой срабатывание СОА.

В предлагаемой системе выбрано $\varepsilon = 1$, т.е. для детектирования аномалии достаточно совпадение двух строк в одной позиции.

В процессе эксперимента использован набор паттернов, полученных в результате наблюдений за приложением expolrer.exe с применением разработанных автором программных модулей. Во время наблюдения было зафиксирован 41 уникальный вызов и получено 15 469 различных строк. Далее был проведен ряд экспериментов. Согласно графику на рис. 7 выбранное значение $\varepsilon = 1$ является оптимальным, так как при $\varepsilon = 2$ вероятность обнаружения аномалии резко снижается.

Как видно из графика, вероятность обнаружения одиночной аномалии возрастает с увеличением числа сгенерированных детекторов.

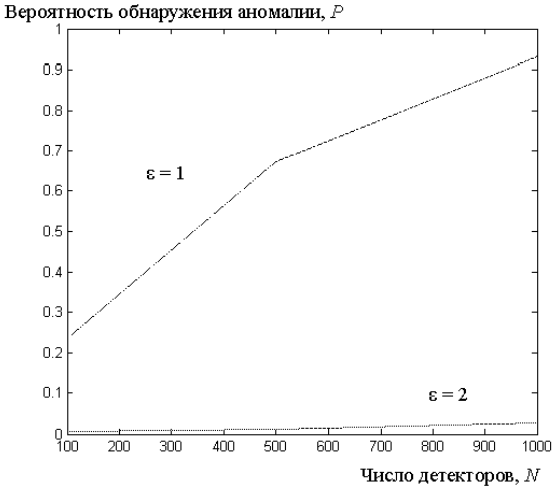


Рис. 7. Зависимость вероятности обнаружения аномалии от числа детекторов при различных значениях величины ε

В результате экспериментов при $N = 1000$ было получено число ложных срабатываний < 3%, в то время как число пропущенных аномалий < 9% (рис. 8).

В исследуемой СОА важную роль играет распределенный характер системы. Для различных рабочих станций в сети, несмотря на то, что используемые на них приложения могут различаться, существует ряд процессов, которые запускаются на каждом компьютере (explorer.exe, lsass.exe и т.д.). В таком случае СОА, построенная на основе технологий искусственных иммунных систем, будет работать намного эффективнее, если обеспечить взаимодействие между клиентами СОА по сети. Поскольку детекторы для каждой рабочей станции генерируются независимо, то система в целом будет обладать большей защищенностью при минимальном количестве детекторов на каждой станции. Если вероятность обнаружения аномалии на i-й станции обозначить через P_i, а число станций через n, то вероятность P сети среагировать на атаку определяется как:

$$P = 1 - \prod_{i=1}^{n} (1 - P_i). \qquad (2)$$

Из (2) следует, что с увеличением n требуемую вероятность P_i обнаружения атаки i-й рабочей станцией можно уменьшить при одном и

том же заданном значении P, а значит, сократить число детекторов на каждой станции.

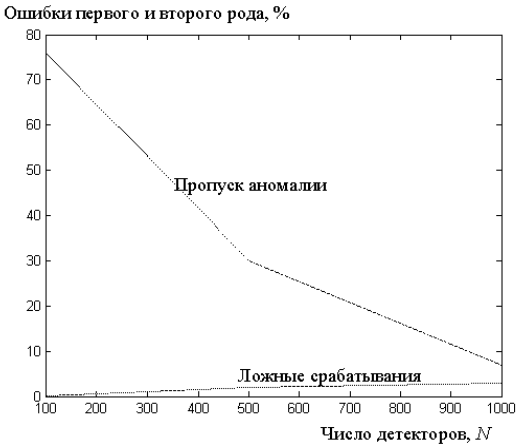


Рис. 8. Зависимость ошибок первого и второго рода от числа детекторов

Архитектура и принцип работы распределенной СОА, реализованной на основе технологий искусственных иммунных систем, изображены на рис. 9. В качестве примера предполагается, что происходит активация детектора *2* на рабочей станции *2*, после чего копия данного детектора добавляется в наборы детекторов остальных станций.

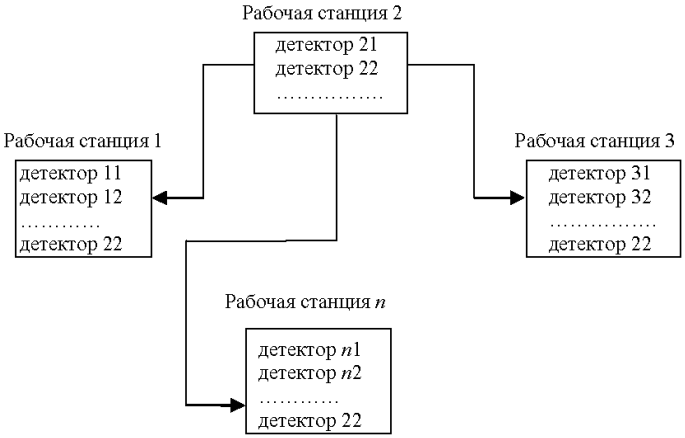


Рис. 9. Структура распределенной СОА

Эксперименты показывают, что чем больше рабочих станций в сети, на которых установлена разрабатываемая СОА, тем меньшие требования предъявляются к отдельно взятой рабочей станции. Графики на рис. 10 показывают зависимость вероятности обнаружения атаки сетью (P) от различных значений вероятности обнаружения аномалии одиночной рабочей станцией (P_i).

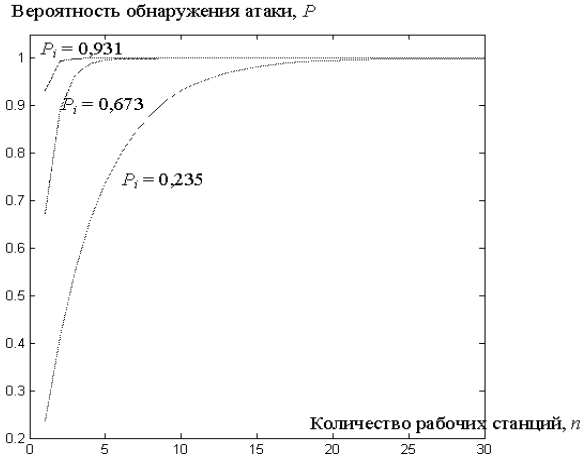


Рис. 10. Зависимость вероятности обнаружения атаки сетью от различных значений вероятности обнаружения аномалии одиночной рабочей станцией

В качестве эксперимента предлагаемая СОА была установлена на три компьютера (n = 3), объединенных в сеть. После обнаружения аномалии на одной из рабочих станций сработавший детектор копируется в базы данных детекторов остальных рабочих станций сети. График работы данного алгоритма адаптации искусственной иммунной системы изображен на рис. 11. Данные о начальных параметрах и параметрах после десяти обнаружений аномалий отражены в таблице, где число рабочих станций – 3.

Параметры СОА до и после адаптации

Наименование параметра	Параметры в начале работы системы	Параметры после десяти обнаружений аномалий
Вероятность обнаружения атаки одной станцией (P)	P1 = 0,931 P2 = 0,931 P3 = 0,931	P1 = 0,970 P2 = 0,955 P3 = 0,967
Число детекторов на одной станции (N)	N1 = 1000 N2 = 1000 N3 = 1000	N1 = 1004 N2 = 1005 N3 = 1003
Вероятность обнаружения атаки распределенной СОА (P*)	0,99967	0,99995

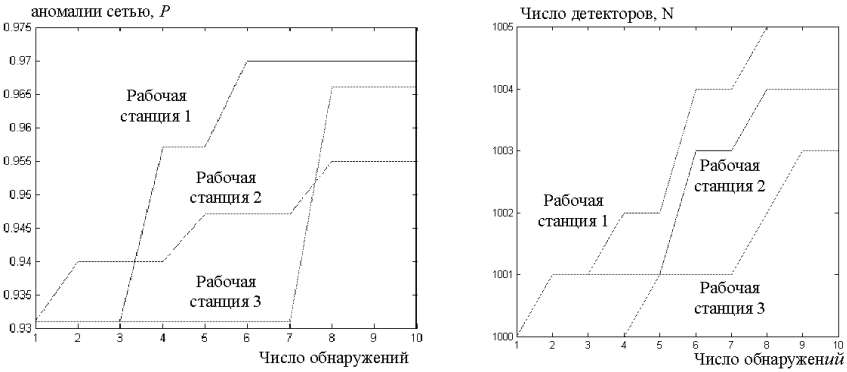


Рис. 11. Адаптация распределенной СОА

Предлагаемая интеллектуальная система обнаружения атак, основанная на технологиях искусственных иммунных систем, позволяет обнаруживать аномальное поведение приложений, что может быть полезным, если приложение модифицировано вирусом или подвергается какому-либо воздействию злоумышленника. Запись последовательностей системных вызовов при проделанных экспериментах является достаточно информативным источником для составления модели нормального поведения системы. Дальнейшие исследования по этой теме предполагают следующие этапы:

1) проведение более развернутых экспериментов с целью проверки эффективности в реальных условиях с большим количеством атак;

2) анализ полученных результатов с целью выяснить, насколько состоятельным является предложенный способ составления модели поведения системы;

3) создание альтернативных вариантов мониторинга системы, например анализ параметров, посылаемых приложениями вместе с вызовами, или число вызовов в дискретные интервалы времени.

В целом, можно сделать вывод о том, что в случае локальных вычислительных сетей, искусственные иммунные системы оказываются более эффективными, поскольку в процессе работы набор детекторов пополняется после каждой обнаруженной аномалии и распространяется на все рабочие станции сети, что позволяет добиться высоких показателей защищенности.

ЛИТЕРАТУРА

1. Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты. М.: Физматлит, 2006. 344 с.

2. De Castro L.N., Timmis J. Artificial Immune Systems: A New Computational Intelligence Approach, Springer-Verlag, 2002. 357 c.

3. Forrest S., Hofmeyr S.A., Somayaji A., Longstaff T.A. A sense of self for Unix processes // Proc. of 1996 IEEE Symposium on Security and Privacy. 1996. P. 120–128. May.

4. Hofmeyr S.A. Forrest S.A. Intrusion detection using sequences of system calls // Journal of Computer Security. 1998. Vol. 6. P. 151–180. August.

5. Warrender C., Forrest S., Pearlmutter B. Detecting Intrusions Using System Calls: Alternative Data Models // Proc. of 1999 IEEE Symposium on Security and Privacy. 1999. P. 133–145. May.

6. Wang M., Zhang C., Yu J. Native API Based Windows Anomaly Intrusion Detection Method Using SVM // Proc. of 2006 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. 2006. P. 514–519. June.

7. Forrest S., Perelson A.S., Allen L., Cherukuri R. Self-nonself discrimination in a computer // Proc. of 1994 IEEE Symposium on Research in Security and Privacy. 1994. P. 202–212, May.

СОДЕРЖАНИЕ

СЕКЦИЯ 11
АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

М.С. Агапов, Р.В. Мещеряков
ТРЕХМЕРНОЕ МОДЕЛИРОВАНИЕ ЛИЦА ЧЕЛОВЕКА 9

Р.Ф. Акчурин, Н.А. Новгородова
СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ДЛЯ РАБОТЫ С БАЗОЙ ДАННЫХ 11

Р.Ф. Акчурин
АВТОМАТИЗАЦИЯ РАБОТЫ ТОРГОВОГО ПРЕДПРИЯТИЯ С ПОМОЩЬЮ ТЕХНОЛОГИИ IDEF 14

Р.Ф. Акчурин, В.А. Трошин
СИСТЕМА КЛАССИФИКАЦИИ ДАННЫХ 16

А.А. Авдеев
МЕДИЦИНСКАЯ СИСТЕМА ВОССТАНОВЛЕНИЯ ГОЛОСОВОЙ ФУНКЦИИ 19

А.И. Балашов, М.И. Мельников
МОДУЛЬ ОПОВЕЩЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ РАСПРЕДЕЛЕННЫМ ЛИФТОВЫМ ХОЗЯЙСТВОМ 20

С.П. Берляков, Д.С. Бронников, Е.О. Воронина, Т.Р. Муксунов
ФУНКЦИОНАЛЬНАЯ СХЕМА ДЛЯ ПРОЕКТА «ИССЛЕДОВАТЕЛЬСКИЙ РОБОТ» 23

А.О. Битюцкая
БАЗА ДАННЫХ ПО ИНВЕНТАРИЗАЦИИ КОМПЬЮТЕРНОЙ ТЕХНИКИ ОРГАНИЗАЦИИ 25

А.О. Битюцкая
СТРУКТУРНЫЙ АНАЛИЗ СИСТЕМЫ УЧЕТА КОМПЬЮТЕРНОЙ ТЕХНИКИ 27

А.С. Бондаренко, А.И. Гуляев, А.С. Яценко
КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПОИСКА, АНАЛИЗА И ПРИНЯТИЯ РЕШЕНИЙ В СЕТИ ИНТЕРНЕТ (ПУАРО) 29

С.А. Чебатков
ОПТИМАЛЬНОЕ РАЗМЕЩЕНИЕ МОДУЛЕЙ ВТОРОГО УРОВНЯ В ПЕРФОРИРОВАННОМ БЛОКЕ ЭЛЕКТРОННОГО СРЕДСТВА 32

М.П. Чеплакова
АНАЛИЗ ПРОГРАММ ПО УЧЕТУ КОМПЬЮТЕРНОЙ ТЕХНИКИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 34

Д.О. Дмитриев
АВТОМАТИЗАЦИЯ ВВОДА ФОРМ 36

Д.О. Дмитриев, Н.А. Новгородова
АВТОМАТИЗАЦИЯ РАБОТЫ ПРИЕМНОЙ КОМИССИИ 38

Р.А. Добрынин
СИСТЕМА АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ВЫСШИМ УЧЕБНЫМ ЗАВЕДЕНИЕМ. ПОДСИСТЕМА СРАВНЕНИЯ УЧЕБНЫХ ПЛАНОВ 39
А.С. Фролов
ПОВЕРКА ПОГРУЖНЫХ ВИХРЕВЫХ РАСХОДОМЕРОВ ИМИТАЦИОННЫМ СПОСОБОМ 41
Д.О. Гайдай
МОНИТОРИНГ СОБЫТИЙ В КОМПЬЮТЕРНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ 44
С.В. Гавриш
ОПТИМАЛЬНОЕ РАЗМЕЩЕНИЕ МОДУЛЕЙ ВТОРОГО УРОВНЯ В ГЕРМЕТИЧНОМ БЛОКЕ ЭЛЕКТРОННОГО СРЕДСТВА 46
Н.А. Гиркин
ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОГО ОБЪЕМА АВТОМАТИЗАЦИИ ПРИ РАЗРАБОТКЕ АСУ ТП 48
Е.С. Хамова
СИСТЕМА АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ НАСОСОМ ОТКАЧКИ ПОДЗЕМНОЙ ЕМКОСТИ 51
А.О. Ирхин, Н.А. Новгородова
АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЛЯ УЧЕТА И КОНТРОЛЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТУРЫ В ЛОКАЛЬНОЙ СЕТИ 53
В.А. Ягницын, Р.В. Мещеряков
ОПРЕДЕЛЕНИЕ ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ С ПОМОЩЬЮ СИНТЕЗА РЕЧЕВОГО СООБЩЕНИЯ 55
К.В. Картавцев
КОЛЛЕКТИВНОЕ ПОВЕДЕНИЕ АВТОНОМНЫХ РОБОТОВ 57
И.С. Хлыст
К ВОПРОСУ УПРАВЛЕНИЯ РЕЖИМАМИ ТЕРМИЧЕСКОЙ ОБРАБОТКИ ТРАНСПОРТНОГО МЕТАЛЛА 60
К.В. Климентьев
СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ОТДЕЛЬНЫМ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ ИЛИ ОБОРУДОВАНИЕМ ДЛЯ УГОЛЬНЫХ ШАХТ 62
Е.Ю. Копьев
ПРОГРАММНАЯ ЧАСТЬ КОНТРОЛЛЕРА ДЛЯ ЖКХ 64
Ю.А. Коптелина, Н.А. Новгородова
АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПО УЧЕТУ НАГРУЗКИ ПРЕПОДАВАТЕЛЕЙ И ЗАТРАТ НА КОМАНДИРОВКИ 65
Л.С. Краев
КОНТРОЛЛЕР ДЛЯ ЖКХ 67
Е.А. Кузнецов
КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ПРОЕКТИРОВАНИЮ ПОРТА ВВОДА-ВЫВОДА 69

Е.А. Кузнецов
РАСЧЕТ НАДЕЖНОСТИ ДЛЯ ВАРИАНТА С «МОНТАЖНЫМ ИЛИ» 71
Я.Г. Лазарев, А.А. Захаров
РОБОТИЗИРОВАННЫЙ КОМПЛЕКС ДЛЯ УПРАВЛЕНИЯ ВНУТРИСЕРДЕЧНЫМ ЭЛЕКТРОДОМ 74
А.Е. Леонов
СОЗДАНИЕ SCADA-СИСТЕМЫ «РЕЗЕРВУАРНЫЙ ПАРК» ПРИ ПОМОЩИ INFINITYSCADA 76
О.С. Лугачева
ПРОЕКТНОЕ РЕШЕНИЕ АСУ ТП ПАРКА НЕФТЕПРОДУКТОВ 78
В.В. Макаров, Р.Ю. Гороховский
АВТОМАТИЗИРОВАННОЕ АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ 81
С.П. Берляков, Д.С. Бронников, Е.О. Воронина, Т.Р. Муксунов
ИССЛЕДОВАТЕЛЬСКИЙ РОБОТ 82
Ю.А. Никонова
ПРИНЦИПЫ ПРОГРАММИРОВАНИЯ НА «1С: ПРЕДПРИЯТИЕ 8» 85
М.А. Молчанов, О.О. Осипова, Д.А. Третьяков
ПРОДУКЦИОННЫЕ ЭКСПЕРТНЫЕ СИСТЕМЫ 86
Д.Ю. Осипов, Д.А. Синков, М.И. Мельников
СИСТЕМА АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ РАСПРЕДЕЛЕННЫМ ЛИФТОВЫМ ХОЗЯЙСТВОМ 88
А.А. Прошутя
GSM/GPS МОДЕМЫ И МОДУЛИ 90
И.В. Салтыкова, Н.А. Новгородова
АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПО УЧЕТУ СТУДЕНТОВ ГПО 92
Д.А. Самойлис
УСТРОЙСТВО СУТОЧНОЙ РЕГИСТРАЦИИ ЭКГ С ПЕРЕДАЧЕЙ ДАННЫХ ЧЕРЕЗ FLASH-КАРТУ 93
А.А. Шилов
ОБЩЕЕ ОПИСАНИЕ ЧЕТЫРЕХРАЗРЯДНОГО БЛОКА ОБРАБОТКИ ДАННЫХ 95
А.А. Шилов
ЭНЕРГОПОТРЕБЛЕНИЕ, НАДЕЖНОСТЬ И ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ЧЕТЫРЕХРАЗРЯДНОГО БЛОКА ОБРАБОТКИ ДАННЫХ 97
Р.Ю. Широколобов
АВТОМАТИЗАЦИЯ РАБОТЫ ДЕКАНАТОВ ТУСУР С ОТЧЕТНЫМИ ДОКУМЕНТАМИ 100
П.А. Соловей, Н.А. Веретенникова
РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ «СИСТЕМНЫЙ АНАЛИЗ» ДЛЯ РАЗВИТИЯ КОРПОРАЦИЙ В УСЛОВИЯХ КОНКУРЕНТНОЙ БОРЬБЫ 101
П.Н. Сверчков
УПРАВЛЕНИЕ ОБЪЕКТАМИ ПО КАНАЛУ BLUETOOTH 104

Е.В. Узбеков
ВЫБОР МОДЕЛИ РОБОТА ДЛЯ ЛАБОРАТОРНОГО ПРАКТИКУМА ПО ДИСЦИПЛИНЕ «ГАС И РОБОТОТЕХНИКА» 106
Е.В. Узбеков, Н.А. Новгородова
ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ДИСЦИПЛИНЕ «ГАС И РОБОТОТЕХНИКА» 107
Н.А. Веретенникова, П.А. Соловей, М.В. Червяков
МЕТОД ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ПОИСКОВЫХ СИСТЕМ ИНТЕРНЕТА 108
Т.С. Волгина
ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ОАИСАУ 111
И.А. Юсупов
СИСТЕМА АРХИВИРОВАНИЯ ТЕХНОЛОГИЧЕСКОЙ ИНФОРМАЦИИ КОМПРЕССОРНЫХ СТАНЦИЙ 112
В.С. Забавский, Н.А. Новгородова
АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА УСПЕВАЕМОСТИ СТУДЕНТОВ 115
Д.Н. Замятин
АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ ДОБЫЧИ ВОДЫ 116
П.В. Жувагин
ВЫБОР ПЛК ДЛЯ ПРОЕКТИРУЕМОЙ АСУ ТП 120
П.А. Шадрин
ОПЕРАТИВНОЕ ПЛАНИРОВАНИЕ МЕЛКОСЕРИЙНОГО ПРОИЗВОДСТВА 122

СЕКЦИЯ 14
МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Р.Ф. Акчурин, Е.Н. Анищенко, В.А. Трошин, А.П. Зайцев
ОПРЕДЕЛЕНИЕ КОЛИЧЕСТВЕННЫХ ХАРАКТЕРИСТИК КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ 127
Е.Н. Анищенко, Д.В. Кручинин
РЕШЕНИЕ ПРОБЛЕМ АВТОРСТВА ТЕКСТОВ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА РАСТУЩЕГО НЕЙРОННОГО ГАЗА 130
В.С. Аверченко, А.И. Михайловский
МОДЕЛЬ АТАКИ И ЗАЩИТЫ НА АС 133
А.С. Данченко
СИСТЕМА ВИЗУАЛЬНОГО МОДЕЛИРОВАНИЯ ЗАЩИТЫ ПОМЕЩЕНИЙ 135

Н.С. Давыдов
ОБУЧАЮЩАЯ СИСТЕМА НА ОСНОВЕ ПОНЯТИЙНОЙ СТРУКТУРЫ ... 131
М.А. Девяткин
АУТЕНТИФИКАЦИЯ В ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЕ ОБМЕНА СООБЩЕНИЯМИ ... 139
В.А. Довбыш
ЗАЩИТА ЛОКАЛЬНОЙ СЕТИ ОТ ВНЕШНИХ УГРОЗ ... 141
В.Н. Елисеев
ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО КАНАЛА ПЕРЕДАЧИ ИНФОРМАЦИИ МЕЖДУ WEB-СЛУЖБАМИ. PHP-РЕАЛИЗАЦИЯ ... 142
С.С. Ерохин
МОДЕЛЬ НАРУШИТЕЛЕЙ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ЭЛЕКТРОННОЙ КОММЕРЦИИ ... 144
С.С. Ерохин
ОЦЕНКА ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ЭЛЕКТРОННОЙ КОММЕРЦИИ ... 147
С.С. Ерохин
ИДЕНТИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ЭЛЕКТРОННОЙ КОММЕРЦИИ ... 148
С.К. Росошек, О.О. Евсютин
ШИФР CA1 ... 151
И.В. Фролов
ПРОГРАММА «СТРАЖ» ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS ... 153
С.В. Голубев, А.С. Романов, Р.В. Мещеряков
ЭНТРОПИЙНЫЙ ПОДХОД К ИНДЕНТИФИКАЦИИ АВТОРА И ЯЗЫКА КОРОТКОГО ЭЛЕКТРОННОГО СООБЩЕНИЯ ... 156
В.С. Хлебников, Д.В. Черных
ВЫДЕЛЕНИЕ КЛЮЧЕВЫХ СЛОВ ПРИМЕНИТЕЛЬНО К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ... 159
М.А. Хурсевич
КЛАССИФИКАЦИЯ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ ДЛЯ ОПРЕДЕЛЕНИЯ СТРАТЕГИИ ЗАЩИТЫ ИНФОРМАЦИИ ... 160
Д.А. Иванов, И.Г. Боровской
МЕТОД ЗАЩИТЫ ОТ КОПИРОВАНИЯ РАСПРЕДЕЛЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ... 163
Р.К. Измайлов, А.П. Зайцев
АТТЕСТАЦИЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ... 165
Э.Р. Хайретдинов, Р.А. Хусаенов
КОМПЛЕКС ПРАКТИЧЕСКИХ РАБОТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ... 168
М.М. Хандорин
ПРОБЛЕМЫ ПОСТРОЕНИЯ ДЕЦЕНТРАЛИЗОВАННОЙ СЕТИ ПЕРЕДАЧИ СООБЩЕНИЙ ... 170

В.В. Компанец
АВТОМАТИЧЕСКАЯ СЕГМЕНТАЦИЯ РЕЧЕВОГО СИГНАЛА НА ВОКАЛИЗОВАННЫЕ ЗВУКИ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ 172
К.О. Изотов, А.В. Меркульев, В.Г. Кондратьева
ПРОЕКТИРОВАНИЕ, РАЗРАБОТКА И ВНЕДРЕНИЕ WEB-РЕСУРСА, ПОСВЯЩЕННОГО КАФЕДРЕ КИБЭВС 174
Ю.И. Конькова
РАСПОЗНАВАНИЕ ЗВУКОВ К', С', Т' ПРИ ПОМОЩИ НЕЙРОННОЙ СЕТИ MATLAB 176
А.В. Космачев
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИИ 179
А.В. Ковалев
РАСПОЗНАВАНИЕ ПЕЧАТНЫХ СИМВОЛОВ МЕТОДОМ СКЕЛЕТИЗАЦИИ ИЗОБРАЖЕНИЯ 182
Б.М. Козлов
МОДУЛЬ ИДЕНТИФИКАЦИИ И КРИПТОГРАФИИ БИЛЛИНГОВОЙ СИСТЕМЫ 184
И.А. Кукало, Е.Ю. Агеев
КОМПЛЕКСНАЯ СИСТЕМА КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ДЛЯ СРЕДНЕГО И МАЛОГО БИЗНЕСА 185
И.А. Кукало
ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ И ТАБЛИЦЫ ЗАМЕН АЛГОРИТМА ГОСТ 28147–89 188
В.В. Летахов
ЦИФРОВАЯ ПОДПИСЬ НА МАТРИЧНОМ КОЛЬЦЕ 190
И.В. Маренков
ЗАЩИЩЕННЫЙ ДОКУМЕНТООБОРОТ В UNIX-СИСТЕМАХ 192
Е.П. Матченко, Ю.М. Филимонов
МОДЕЛИРОВАНИЕ ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ 195
Ю.С. Михайлова, И.Г. Боровской
МЕТОД ПОЛУЧЕНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ ХУКОВ 198
Н.С. Михайлов
ДЕЦЕНТРАЛИЗОВАННАЯ СИСТЕМА ОБМЕНА СООБЩЕНИЯМИ В СЕТИ ИНТЕРНЕТ 200
А.Л. Навойников
ТИПОВОЙ КОМПЛЕКТ ДОКУМЕНТОВ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ 201
Н.Ю. Омланд
ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ 203
П.Б. Первушин
СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОБЪЕКТ 206
И.А. Петроченко
ОЦЕНКА КАЧЕСТВА СИСТЕМЫ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ПРЕДПРИЯТИЯ 209

М.А. Приходько
АВТОМАТИЗИРОВАННАЯ СИСТЕМА ЗАЩИТЫ САЙТА, РАЗРАБОТАННОГО НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ PHP С ИСПОЛЬЗОВАНИЕМ СЕРВЕРА БАЗ ДАННЫХ MYSQL, ОТ АТАК ТИПА SQL-ИНЪЕКЦИЯ, PHP-ИНЪЕКЦИЯ И МЕЖСАЙТОВЫЙ СКРИПТИНГ 212

М.А. Приходько
КОМПЬЮТЕРНЫЙ ВИРУС КАК БАЗИС РАЗВИТИЯ СРЕДСТВ ЗАЩИТЫ БУДУЩЕГО 215

А.А. Пуха
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОТДЕЛЕ КАДРОВ ОРГАНИЗАЦИИ 217

А.С. Романов
МЕТОД АДДИТИВНОГО СГЛАЖИВАНИЯ В РЕШЕНИИ ЗАДАЧИ ИДЕНТИФИКАЦИИ АВТОРА ТЕКСТА 219

А.С. Романов
КЛАССИФИКАТОР НА ОСНОВЕ МАШИНЫ ОПОРНЫХ ВЕКТОРОВ 222

Е.Ф. Щипунов
ПРОБЛЕМАТИКА РАСПОЗНАВАНИЯ ГЛАСНЫХ И СОГЛАСНЫХ ЗВУКОВ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ 225

А.Р. Селютин, Ж.Е. Каппасов, С.А. Михнов, Л.В. Загребин, Р.В. Литвинов
ОДНОМЕРНЫЕ СВЕТЛЫЕ СОЛИТОНЫ В НАНОКОЛЛОИДНЫХ СИСТЕМАХ 228

К.А. Швейдюк
ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ АКУСТИЧЕСКОЙ (РЕЧЕВОЙ) ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 230

Е.А. Смаль, А.В. Лысова, Ю.М. Филимонов
ЭЛЕКТРОННЫЕ КЛЮЧИ eToken и ruToken 233

П.П. Свешников
ТЕСТОВЫЙ СЕРВЕР ДЛЯ ВЗЛОМА 236

С.Д. Тиунов
БЕЗОПАСНЫЕ USB FLASH DRIVE 238

С.Д. Тиунов
РАСПОЗНАВАНИЕ СМЫЧНЫХ СОГЛАСНЫХ 239

В.А. Цевменков
ОБМЕН СООБЩЕНИЯМИ В ДЕЦЕНТРАЛИЗОВАННОЙ ЗАЩИЩАЕМОЙ СИСТЕМЕ 242

А.Н. Уразаева
ОБЗОР СПОСОБОВ ЗАЩИТЫ БАЗ ДАННЫХ АРХИТЕКТУРЫ КЛИЕНТ–СЕРВЕР 244

Д.Н. Вечерина
ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ ОБМЕНА СООБЩЕНИЯМИ 247

Е.С. Волокитина
МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ 249
А.С. Яценко
РЕГИСТРАЦИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ СЕТИ 251
Д.А. Зайцев, В.А. Нопин, А.П. Зайцев
ПОРТАТИВНЫЙ КОМПЛЕКТ ДЛЯ ОБНАРУЖЕНИЯ СРЕДСТВ СЪЕМА ИНФОРМАЦИИ И ВЫЯВЛЕНИЯ КАНАЛОВ ЕЕ УТЕЧКИ «ПКУ-6М» 253
В.Д. Зыков
МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЛЕЧЕБНО-ПРОФИЛАКТИЧЕСКИХ УЧРЕЖДЕНИЙ ТОМСКОЙ ОБЛАСТИ 255
В.Д. Зыков
КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ СЕРВИСОВ ДОВЕРЕННОЙ ТРЕТЬЕЙ СТОРОНЫ 257
С.В. Дереглазова
ТЕХНОЛОГИЯ ОТБОРА ПРЕТЕНДЕНТОВ ДЛЯ РАБОТЫ И УЧЕБЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 259
О.С. Дулькейт
ИДЕНТИФИКАЦИЯ ЯЗЫКА ЗАШУМЛЕННОГО ТЕКСТА 261
Д.В. Кириллов
МЕХАНИЗМ СОБЫТИЙНО-ОБУСЛОВЛЕННОГО ДЕЛЕГИРОВАНИЯ И ОТЗЫВА ПОЛНОМОЧИЙ 267
Д.О. Косолапов
ПРОТОКОЛ КЛЮЧЕВОГО СОГЛАШЕНИЯ НА ОСНОВЕ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ С ВОЗМОЖНОСТЬЮ ВЫЯВЛЕНИЯ ЗЛОУМЫШЛЕННИКА 277
А.В. Лисин
КОНТРОЛЬ НЕ ПОКРЫТЫХ ВИДЕОНАБЛЮДЕНИЕМ УЧАСТКОВ С ПОМОЩЬЮ ДОПОЛНИТЕЛЬНЫХ ИСТОЧНИКОВ ОСВЕЩЕНИЯ 284
А.В. Черепанов
МЕТОД ОЦЕНКИ СХОДСТВА ЛИЦ НА ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ 289
М.Ю. Дьяконов
ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ АНАЛИЗА ПРОЦЕССОВ 303
А.В. Мокеев
РАЗРАБОТКА МЕТОДА СИНТЕЗА ГЛАВНЫХ КОМПОНЕНТ ДЛЯ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ 309
Д.М. Мурин
РЕАЛИЗАЦИЯ МОДЕЛИ РАСПРОСТРАНЕНИЯ ПРАВ ДОСТУПА TAKE-GRANT КОНЕЧНЫМИ АВТОМАТАМИ 316

В.В. Перевощиков, А.А. Гриценко
ОБ ЭФФЕКТИВНОЙ РЕАЛИЗАЦИИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ 319
А.А. Пономерев
ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ..327
А.А. Пономарев
РАЗРАБОТКА МЕТОДИК АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....335
М.Э. Раисов, Р.В. Мещеряков
ПОЛИГРАФ НА ОСНОВЕ РЕЧЕВОГО ВВОДА.....344
А.Н. Ручай
РАЗРАБОТКА ТЕКСТОЗАВИСИМОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ ДИКТОРА ПО ГОЛОСУ 347
А.Ф. Саляхов, А.И. Фрид, Д.И. Кардаш
УПРАВЛЕНИЕ ОПЕРАЦИОННЫМИ РИСКАМИ БАНКОВСКОГО ПЛАТЕЖНОГО ПРОЦЕССА.....353
С.С. Коновалова
КОМБИНАТОРНО-ГЕОМЕТРИЧЕСКИЙ МЕТОД ИССЛЕДОВАНИЯ СОВЕРШЕННЫХ ШИФРОВ И ИХ СОВРЕМЕННЫХ АНАЛОГОВ.....359
А.В. Ветлов
О ЗАДАЧЕ КРИПТОГРАФИЧЕСКОГО СЖАТИЯ ИЗОБРАЖЕНИЙ В ТЕЛЕМЕДИЦИНЕ 366
В.Д. Котов
СИСТЕМА ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ.....371

Научное издание

Научная сессия ТУСУР-2009

Материалы
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
12–15 мая 2009 г., Томск, Россия
В пяти частях

Часть 3

Тематический выпуск
«СИСТЕМНАЯ ИНТЕГРАЦИЯ И БЕЗОПАСНОСТЬ»

Корректор – **В.Г. Лихачева**
Верстка **В.М. Бочкаревой**

Издательство «В-Спектр».
Сдано на верстку 01.04.2009. Подписано к печати 05.05.2009.
Формат $60\times84^{1}/_{16}$. Печать трафаретная.
Печ. л.24,4 Усл. печ. 21
Тираж 150 экз. Заказ 38.

Тираж отпечатан в издательстве «В-Спектр».
ИНН/КПП 7017129340/701701001, ОГРН 1057002637768
634055, г. Томск, пр. Академический, 13-24. Тел. 49-09-91.
E-mail: bmwm@list.ru