Министерство образования и науки Российской Федерации
Федеральное агентство по образованию

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедре КИБЭВС – 35 лет

НАУЧНАЯ СЕССИЯ ТУСУР – 2006

**Материалы докладов
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР – 2006»,
посвященной 75-летию Ф.И. Перегудова,
4 – 7 мая 2006 г.**

В пяти частях

Часть 3

***(Тематический выпуск посвящен 35-летию кафедры
комплексной информационной безопасности
электронно-вычислительных систем ТУСУРа)***

В-Спектр
2006

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

Научная сессия ТУСУР – 2006: Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 4–7 мая 2006 г. – Томск: Издательство «В-Спектр», 2006. Ч. 3. – 202 с.

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, вопросам проектирования и технологии радиоэлектронных средств, аудиовизиальной техники, бытовой радиоэлектронной аппаратуры, а также автоматизированным системам управления и проектирования. Рассматриваются проблемы электроники СВЧ- и акустооптоэлектроники, физической, плазменной, квантовой, промышленной электроники, радиотехники, информационно-измерительных приборов и устройств, распределенных информационных технологий, автоматизации технологических процессов, в частности в системах управления и проектирования, информационной безопасности и защите информации. Также представлены материалы по математическому моделированию в технике, экономике и менеджменте, антикризисному управлению, автоматизации управления в технике и образовании. Широкому кругу читателей будет доступна информация о социальной работе в современном обществе, философии и специальной методологии, экологии, мониторингу окружающей среды и безопасности жизнедеятельности, инновационных, студенческих идеях и проектах.

Конференция проводится при поддержке
ЦС РНТОРЭС им. А.С. Попова
Посвящается 75-летию Ф.И. Перегудова

ISBN 5-91191-003-9

ISBN 5-91191-006-3 (Ч. 3)

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

Всероссийская научно-техническая конференция студентов и молодых ученых "Научная сессия ТУСУР – 2006" 4–7 мая 2006 г.

ПРОГРАММНЫЙ КОМИТЕТ

Кобзев А.В. – председатель, ректор ТУСУР, д.т.н., профессор.

Ильюшенко В.Н. – сопредседатель, проректор по НР ТУСУР, д.т.н., профессор.

Малюк А.А. – декан факультета информационной безопасности Московского инженерно-физического института (МИФИ), к.т.н., г. Москва.

Майстренко В.А. – проректор по информатизации ОмскГТУ, д.т.н., профессор, г. Омск.

Кравченко В.Б. – зам. проректора по информатизации Российского государственного гуманитарного университета, к.т.н., г. Москва.

Кориков А.М. – зав. каф. автоматизированных систем управления (АСУ) ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор.

Московченко А.Д. – зав. каф. философии, д.ф.н., профессор.

Ехлаков Ю.П. – проректор по информатизации ТУСУР, д.т.н., профессор.

Шурыгин Ю.А. – первый проректор ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор.

Уваров А.Ф. – проректор по экономике ТУСУР, к.э.н.

Шарыгин Г.С. – зав. каф. радиотехнических систем (РТС), д.т.н., профессор.

Пустынский И.Н. – зав. каф. телевидения и управления (ТУ), заслуженный деятель науки и техники РФ, д.т.н., профессор.

Шелупанов А.А. – зав. каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС), д.т.н., профессор.

Осипов Ю.М. – зав. Отделением каф. ЮНЕСКО при ТУСУР, академик Международной академии информатизации, д.т.н., д.э.н., профессор.

Грик Н.А. – зав. каф. ИСР, д. ист.н., профессор.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Кобзев А.В. – председатель, ректор ТУСУР, д.т.н., профессор.

Ильюшенко В.Н. – сопредседатель, проректор по НР ТУСУР, д.т.н., профессор.

Шурыгин Ю.А. – первый проректор ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор.

Акулиничев Ю.П. – председатель совета по НИРС радиотехнического факультета (РТФ), д.т.н., профессор каф. радиотехнических систем (РТС).

Еханин С.Г. – председатель совета по НИРС радиоконструкторского факультета (РКФ), д.ф.-м.н., профессор каф. конструирования узлов и деталей РЭС (КУДР).

Коцубинский В.П. – председатель совета по НИРС факультета вычислительных систем (ФВС), зам. зав. каф. компьютерных систем в управлении и проектировании (КСУП), к.т.н., доцент.

Мицель А.А. – председатель совета по НИРС факультета систем управления (ФСУ), д.т.н., профессор каф. автоматизированных систем управления (АСУ).

Орликов Л.Н. – председатель совета по НИРС ФЭТ, д.т.н., профессор каф. ЭП.

Казакевич Л.И. – председатель совета по НИРС гуманитарного факультета (ГФ), к.ист.н., доцент каф. ИСР.

Ярымова И.А. – зам. зав. отделения послевузовского профессионального образования (ОППО) ТУСУР, к.б.н.

ПОРЯДОК РАБОТЫ, ВРЕМЯ И МЕСТО ПРОВЕДЕНИЯ

Работа конференции будет организована в форме пленарных, секционных и стендовых докладов.

Конференция проводится
с 4 по 7 мая 2006 г.
в Томском государственном университете
систем управления и радиоэлектроники

Регистрация участников будет проводиться
перед пленарным заседанием в главном корпусе ТУСУР
(пр. Ленина, 40) в актовом зале **4 мая с 9:00 до 10:00**.

СЕКЦИИ КОНФЕРЕНЦИИ

Секция 1. РАДИОТЕХНИЧЕСКИЕ СИСТЕМЫ И РАСПРОСТРАНЕНИЕ РАДИОВОЛН – *председатель* ***Шарыгин Г.С.,*** *зав. каф. РТС, д.т.н., профессор; зам. председателя* ***Тисленко В.И.,*** *к.т.н., доцент каф. РТС*

Секция 2. ЗАЩИЩЕННЫЕ ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ – *председатель* ***Голиков А.М.,*** *к.т.н., доцент каф. РТС*

Секция 3. АУДИОВИЗУАЛЬНАЯ ТЕХНИКА, БЫТОВАЯ РАДИОЭЛЕКТРОННАЯ АППАРАТУРА И СЕРВИС – *председатель* ***Пустынский И.Н.,*** *зав. каф. ТУ, д.т.н., профессор; зам. председателя* ***Костевич А.Г.,*** *к.т.н., доцент каф. ТУ*

Секция 4. ПРОЕКТИРОВАНИЕ И ТЕХНОЛОГИИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ. ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ РАДИООБОРУДОВАНИЯ – *председатель* ***Масалов Е.В.,*** *д.т.н., профессор каф. КИПР, зам. председателя* ***Михеев Е.Н.,*** *м.н.с.*

Подсекция 4.1. ПРОЕКТИРОВАНИЕ БИОМЕДИЦИНСКОЙ АППАРАТУРЫ – *председатель* ***Еханин С.Г.,*** *д.ф.-м.н., профессор каф. КУДР*

Подсекция 4.2. КОНСТРУИРОВАНИЕ И ПРОИЗВОДСТВО РАДИОЭЛЕКТРОННЫХ СРЕДСТВ – *председатель* ***Михеев Е.Н.,*** *м.н.с.*

Секция 5. ИНТЕГРИРОВАННЫЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ – *председатель* ***Катаев М.Ю.,*** *д.т.н., профессор каф. АСУ*

Секция 6. КВАНТОВАЯ, ОПТИЧЕСКАЯ И НАНОЭЛЕКТРОНИКА – *председатель* ***Шарангович С.Н.,*** *зав. каф. СВЧиКР, к.ф.-м.н., доцент; зам. председателя* ***Буримов Н.И.,*** *к.т.н., доцент каф. ЭП*

Секция 7. ФИЗИЧЕСКАЯ И ПЛАЗМЕННАЯ ЭЛЕКТРОНИКА – *председатель* ***Троян П.Е.,*** *зав. каф. ФЭ, к.т.н., доцент*

Секция 8. РАСПРЕДЕЛЁННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ – *председатель* ***Ехлаков Ю.П.*** *проректор по Информатизации ТУСУР, зав. каф. АОИ, д.т.н., профессор; зам. председателя* ***Сенченко П.В.,*** *к.т.н., доцент каф. АОИ*

Секция 9. АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ – *председатель* ***Шелупанов А.А.,*** *зав. каф. КИБЭВС, д.т.н., профессор; зам. председателя* ***Раводин О.М.,*** *к.т.н., профессор каф. КИБЭВС*

Подсекция 9.1. ПРОЕКТИРОВАНИЕ И ТЕХНОЛОГИЯ ЭВС

Подсекция 9.2. КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Подсекция 9.3 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Секция 10. АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА В СИСТЕМАХ УПРАВЛЕНИЯ И ПРОЕКТИРОВАНИЯ – *председатель* ***Шурыгин Ю.А.,*** *первый проректор ТУСУР, зав. каф. КСУП, д.т.н., профессор; зам. председателя* ***Коцубинский В.П.,*** *зам. зав. каф. КСУП, к.т.н., доцент*

Секция 11. МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – *председатель* ***Ильюшенко В.Н.*** ***,*** *проректор по НР ТУСУР, зав. каф. РЗИ, д.т.н., профессор; зам. председателя* ***Загоскин В.В.,*** *к.ф.-м.н., доцент каф. РЗИ*

Секция 12. ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И УСТРОЙСТВА – *председатель* ***Светлаков А.А.,*** *зав. каф. ИИТ, д.т.н., профессор; зам. председателя* ***Шидловский В.С.,*** *к.т.н., доцент каф. ИИТ*

Секция 13. РАДИОТЕХНИКА – *председатель* ***Титов А.А.,*** *д.т.н., профессор каф. РЗИ; зам. председателя* ***Семенов Э.В.,*** *к.т.н., доцент каф. РЗИ;*

Секция 14. ПРОМЫШЛЕННАЯ ЭЛЕКТРОНИКА – *председатель* ***Семенов В.Д.****, зам. зав. каф. ПрЭ по НР, к.т.н., доцент; зам. председателя* ***Шевелев М.Ю.,*** *к.т.н., доцент каф. ПрЭ*

Секция 15. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ В ТЕХНИКЕ, ЭКОНОМИКЕ И МЕНЕДЖМЕНТЕ – *председатель* ***Мицель А.А.,*** *д.т.н., профессор каф. АСУ; зам. председателя –* ***Зариковская Н.В.,*** *к.ф.-м.н., доцент каф. ФЭ*

Секция 16. ЭКОНОМИКА И УПРАВЛЕНИЕ – *председатель* ***Осипов Ю.М.,*** *зав. Отделением каф. ЮНЕСКО при ТУСУР, д.э.н., д.т.н., профессор; зам. председателя –* ***Василевская Н.Б.,*** *к.э.н., доцент каф. Экономики*

Секция 17. АНТИКРИЗИСНОЕ УПРАВЛЕНИЕ – *председатель* ***Семиглазов А.М.,*** *д.т.н., профессор каф. ТУ; зам. председателя –* ***Бут О.А.,*** *ассистент каф. ТУ*

Секция 18. ЭКОЛОГИЯ И МОНИТОРИНГ ОКРУЖАЮЩЕЙ СРЕДЫ – *председатель* ***Карташов А.Г.,*** *д.б.н., профессор каф. РЭТЭМ*

Секция 19. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ – *председатель* ***Хорев И.Е.,*** *д.т.н., профессор каф. РЭТЭМ; зам. председателя –* ***Полякова С.А.,*** *к.б.н., доцент каф. РЭТЭМ*

Секция 20. АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОЦИАЛЬНОЙ РАБОТЫ В СОВРЕМЕННОМ ОБЩЕСТВЕ – ***Грик Н.А.,*** *зав. каф. ИСР, д.ист.н., профессор; зам. председателя –* ***Казакевич Л.И.,*** *к.ист.н., доцент каф. ИСР*

Секция 21. ФИЛОСОФИЯ И СПЕЦИАЛЬНАЯ МЕТОДОЛОГИЯ – *председатель* ***Московченко А.Д.,*** *зав. каф. Философии, д.ф.н., профессор; зам. председателя –* ***Раитина М.Ю.,*** *к.ф.н., доцент каф. философии*

Секция 22. ИННОВАЦИОННЫЕ ПРОЕКТЫ, СТУДЕНЧЕСКИЕ ИДЕИ И ПРОЕКТЫ – *председатель* ***Уваров А.Ф.,*** *проректор по экономике ТУСУР, к.э.н.; зам. председателя –* ***Чекчеева Н.В.,*** *зам. директора Студенческого Бизнес-Инкубатора (СБИ)*

Секция 23. АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ В ТЕХНИКЕ И ОБРАЗОВАНИИ – *председатель* ***Дмитриев В.М.,*** *зав. каф. ТОЭ, д.т.н., профессор; зам. председателя* ***Андреев М.И.,*** *к.т.н., доцент ВКИЭМ*

Секция 24. ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ ШКОЛЬНИКОВ – *председатель* ***Дмитриев И.В.,*** *директор ОЦ «Школьный университет», к.т.н.; зам. председателя –* ***Шамина О.Б.,*** *начальник учебно-методического отдела ОЦ «Школьный университет», к.т.н., доцент*

Адрес оргкомитета:

Россия, 634050, г. Томск, пр. Ленина 40, ТУСУР,
Научное управление (НУ), к. 205.
Тел.: 8-(3822)-51-47-57
E-mail: nirs@main.tusur.ru

Материалы научных докладов, предоставленные на конференцию, опубликованы в сборнике «НАУЧНАЯ СЕССИЯ ТУСУР – 2006», состоящем из пяти частей.

В 1 часть сборника включены доклады 1 – 7 секций.

Во 2 часть – доклады 8, 10, 11 секций.

В 3 часть – доклады 9 секции.

В 4 часть – доклады 12 – 16 секций.

В 5 часть – доклады 17 – 24 секций.

СЕКЦИЯ 9

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

*Председатель – **Шелупанов А.А.,** зав. каф. КИБЭВС, д.т.н., профессор;*
*зам. председателя **Раводин О.М.,** к.т.н., профессор каф. КИБЭВС*

Кафедре КИБЭВС – 35 лет

Материалы секции № 9 «Научной сессии ТУСУР – 2006» отражают научные интересы профессорско-преподавательского состава, аспирантов и студентов кафедры КИБЭВС всех курсов очного обучения, а также студентов и аспирантов других специальностей, работающих над вопросами автоматизации технологических процессов, информационной безопасностью и защитой информации. В тезисах докладов описываются результаты разработки интеллектуальных систем в области автоматизации, управления и информационной безопасности автоматизированных систем, компьютерной безопасности. Учитывается важный аспект безопасности – комплексность. Секция 9 представлена тремя подсекциями: 9.1 – проектирование и технология ЭВС, 9.2 – комплексное обеспечение информационной безопасности автоматизированных систем, 9.3 – компьютерная безопасность.

ПОДСЕКЦИЯ 9.1

ПРОЕКТИРОВАНИЕ И ТЕХНОЛОГИЯ ЭВС

РЕАЛИЗАЦИЯ КОНТРОЛЬНОГО СЛЕДА БАЗЫ ДАННЫХ

Н.В. Арифанова, студентка 5 курса каф. КИБЭВС
ТУСУР, г. Томск, xxmop@mail.ru

Реализация контрольного следа модификации данных – задача, преимущественно решаемая для сложных иерархических систем с высокими требованиями к контролю над операционной деятельностью пользователей. Примерами таких систем могут быть программы по контролю оперативно – складского учета, управления людскими ресурсами (HRM – human resource managment) и т.д.

Основными характеристиками данных систем являются:

– высокая сложность системы (система содержит n физических и логических уровней, соединенных в виде цепочки, дерева или другой более сложной структуры);

– система насчитывает, как правило, более 1000 логических сущностей (таблиц, представлений, триггеров, процедур и т.д.) и сотни тысяч (миллионы) строк кода;

– в работе системы участвуют десятки, сотни, тысячи человек. В случае операционной деятельности система должна обеспечить высокий транзакционный параллелизм для каждого пользователя;

– действия каждого пользователя должны быть зафиксированы, чтобы предотвратить или сохранить заведомо неправильные, либо вредоносные для системы операции (т.е. система должна быть аудируемой).

При этом аудирование сущностей в БД должно происходить независимо от количества и структуры таблиц, количества пользователей системы и степени ее загруженности. Для решения задачи аудирования была спроектирована и реализована система автоматизации аудита с помощью стандартных программных интерфейсов ядра СУБД.

Основная концепция разработанной системы – дополнительное хранение всех модифицируемых пользователями данных в таблицах-прототипах. Таблица-прототип представляет собой видоизмененную сущность аудируемой таблицы, предназначенную для хранения всех модифицируемых данных за определенный период времени. Для перехвата аудируемого события используется специальный объект СУБД – триггер, размещаемый в пространстве аудируемой таблицы.

Помимо n таблиц-прототипов система содержит общий журнал всех модифицируемых записей, сохраняющий все атрибуты аутентификации пользователей (доменное имя пользователя, имя хоста, участвующего в сессии), а также общие сигнатуры поиска k-той записи в произвольной таблице-прототипе. Этапы проектирования и реализации системы аудита можно разбить на следующие пункты:

1. Реализация прототипов таблиц на основе выделенных сущностей. Данная задача является сложной по ряду следующих причин:

– СУБД как правило не предоставляет простых запросных конструкций для получения списка пользовательских таблиц.

– Стандарт SQL явным образом не поддерживает динамическое формирование объектов (таблиц, представлений, функций, процедур.

2. Реализация перехвата событий модификации для каждой реальной таблицы:

– Реализация перехвата должна быть выполнена наиболее эффективным способом, и не создавать нагрузку на СУБД в целом, так как количество аудированных таблиц может исчисляться сотнями или даже тысячами;

– Реализация процедур перехвата в терминах СУБД-триггеров должна также выполняться динамически для каждой из реальных таблиц сущностей.

3. Использование вложенных курсорных конструкций для формирования динамических скриптов таблиц – прототипов и триггеров аудита.

4. Управление системой аудита должно осуществляться простыми и понятными процедурами. Как правило, главной сложностью при реализации данных процедур является невозможность модификации системы без полной остановки комплекса аудирования или даже основной службы СУБД. В решение этой задачи, также входит и корректные откаты транзакций, а также обработки ошибок при сбоях аудируемой системы или СУБД в целом.

Проектирование и реализация системы была произведена в промышленной СУБД корпорации Microsoft SQL Server 2000 средствами языка Transact – SQL.

Результатом работы является текст скрипта, который реализует процедуры автоматизирующие аудит для конкретной системы, работающей с СУБД. Разработанная система может быть использована архитекторами инфраструктуры и специалистами по безопасности для ведения аудита своих БД без каких – либо технических ограничений. При этом программа может быть легко модифицирована для каких-либо специфических нужд другими специалистами.

ЛИТЕРАТУРА

1. *Артемов Д.В.* Microsoft SQL Server 2000: профессионалы для профессионалов. М.: «Русская редакция», 2005. 512с.
2. *Хендерсон К.* Профессиональное руководство по Transact – SQL. СПб.: Питер, 2005. 558с.

СОТОВАЯ ПАКЕТНАЯ РАДИОСЕТЬ

Р.Р. Богданов, студент 5 курса каф. КИБЭВС,
Р.В. Мещеряков, к.т.н., доцент
ТУСУР, г. Томск, т. +7-961-097-44-09

Аналогично структуре восковой пластины пчелиного улья сотовая сеть состоит (рис. 1) из множества ячеек (сот). В центре каждой из них располагается базовая станция (БС). Каждая БС работает так, что «видит» только шесть своих соседей. Например, БС 5 «видит» и взаимодействует только с шестью БС, имеющими номера 1, 2, 4, 6, 8, 9. Каждую пару взаимодействующих БС связывает два симплексных канала. Поэтому любая БС работает с 12 радиоканалами, каждый из которых отличается используемой частотой. Благодаря тому, что БС «видит» только шесть партнеров, резко сокращается число полос частот, используемых в сети. Так, например, БС 4 и БС 7 не «видят» друг друга.

Поэтому во множествах исходящих из них радиоканалов могут использоваться одни и те же полосы частот, ибо передача сигналов по ним не мешает друг другу. В выделенном диапазоне частот каждая базовая станция может работать с ограниченным числом систем. Поэтому для увеличения числа абонентов сотовой сети в ней все чаще делают небольшие микросоты. В результате появились *микросотовые радиосети*.

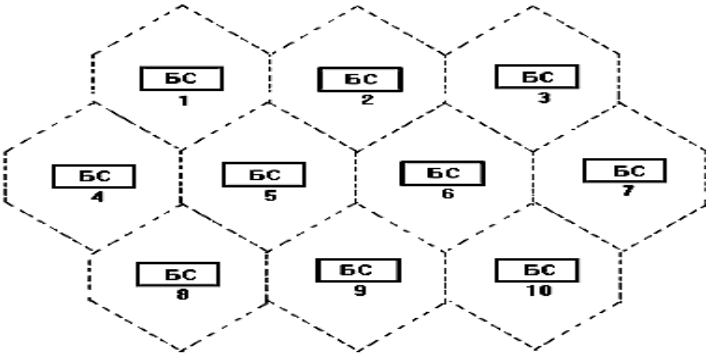


Рис. 1. Топология размещения установок пакетной радиосвязи

Любая абонентская система взаимодействует с той БС, которая находится к ней ближе всего. Для этого в радиосети производится постоянное отслеживание области уверенного приема в зоне местонахождения каждого подвижного объекта и вызов направляется в ту ячейку, в которой он находится. При перемещении объекта (например, автомобиля) сеть меняет номера БС, с которыми взаимодействует этот объект. Система как бы передается от одной БС к другой. Естественно, что место расположения объекта должно быть известно функциональному блоку сети, осуществляющему маршрутизацию блоков данных. Благодаря этому, объект получает блоки не зависимо от того, где он находится в данное время.

Сотовые сети делятся на наземные и спутниковые. Первые характеризуются тем, что их БС располагаются на земле. Во втором случае БС находятся на спутниках связи. Из-за ненадежности спутников коммуникационная сеть создается таким образом, чтобы она нормально работала при потере до 50% спутников. Спутниковые БС связываются друг с другом радиоканалами, а БС, находящиеся на земле, также и оптическими каналами.

Передача в сотовой сети дискретных сигналов обеспечивает надежную организацию большой пропускной способности. Простые в обращении устройства позволяют обрабатывать потоки этих сигналов

более удобными способами, нежели аналоговых сигналов. Поэтому быстрыми темпами создаются так называемые сети Сотовых дискретных пакетных данных CDPD. В стандартах этих сетей используется межсетевой протокол IP сети internet.

Сотовая пакетная радиосеть предназначена для установления связи с абонентскими системами подвижных объектов: самолетов, судов, автомобилей, поездов. В качестве этих систем используются телефонные аппараты, коммуникаторы и небольшие персональные компьютеры. Компонентами сотовой сети являются также локальные радиосети. В сотовой сети функционирует мобильная система передачи данных между транспортными средствами, персональная связь.

Спутник связи устройство, движущееся по орбите вокруг земли и используемое для передачи данных. Прежде всего, спутники связи классифицируются по форме используемой ими орбиты. Геостационарные спутники располагаются на высоте 35786 км над экватором. Благодаря этому, указанные спутники, по сравнению с другими типами, обеспечивают непрерывность передачи данных (они с земли все время видны и не уходят за горизонт). Кроме этого, при работе с геостационарным спутником антенна наземной абонентской системы неподвижна, что значительно упрощает ее конструкцию. Между тем, большая удаленность спутников от земли приводит к значительным запаздываниям в передаче сигнала, что не всегда приемлемо. Кроме этого, из-за взаимных помех, на экваторе не может быть размещено более, чем, примерно, 360 спутников. А число уже размещенных спутников приближается к этому пределу. Использование терминалов VSAT с узкими лучами и многократным повторением частот, расширяет возможности геостационарных спутников. Но, лишь до определенных пределов. Следует также помнить, что геостационарные спутники не видны в приполярных областях земли.

Спутники на высокоорбитальной эллиптической орбите хорошо покрывают полярные области. Между тем, они периодически уходят за горизонт и видны абонентским системам только часть времени их обращения вокруг земли. Поэтому антенны наземных станций должны следить за движением 3–4 спутников и переключаться с одного из них на другой. Сейчас становятся популярными комплексы спутников низкоорбитальных круговых орбитах. Низкоорбитальные спутники запускаются на орбиты до 1000 км с временем вращения вокруг земли, равным 1,5–2 ч. Перемещаясь относительно земли, такие спутники покрывают всю ее поверхность. Низкое расположение спутников позволяет получить на земле сильный сигнал. Примером такой коммуникационной сети на низкоорбитальных спутниках, является спутниковая

сеть Iridium. По своим функциональным возможностям спутники связи подразделяются на два вида. К первому из них относятся спутники-ретрансляторы. Каждый из них принимает сигналы с земли, восстанавливает их форму и на другой частоте вновь передает их на землю. На базе спутника-ретранслятора может быть создана моноканальная сеть. Она имеет два радио канала, соединяемых ретранслятором. Один из каналов собирает данные со всех наземных абонентских систем, а второй радиоканал раздает эти данные тем же системам. Оба канала работают на различных частотах, чтобы не мешать друг другу. На базе спутников-ретрансляторов могут создаваться также сети с маршрутизацией данных. Однако узлы коммутации этих сетей находятся на земной поверхности. В процессе эволюции возникла тенденция размещения на спутнике узла коммутации.

ЛИТЕРАТУРА

1. *EVER94* Everitt D. Traffic Engineering of the Radio Interface for Cellular Mobile Networks. – In: Proceedings of the IEEE, September 1994. C. 81.
2. *Столлингс В.* Беспроводные линии связи и сети. : Пер. с англ. – М. : Издательский дом «Вильямс», 2003. 640с. Парал. Тит. Англ.

РАЗРАБОТКА ЕДИНОЙ ОБОЛОЧКИ И РЕДАКТОРА ДЛЯ АЛГОРИТМОВ ШИФРОВАНИЯ

А.С. Коботаев, студент 3 курса; М.М. Саматов, студент 3 курса; С.И. Боровков, студент 3 курса каф. КИБЭВС
ТУСУР, г. Томск, a111_666@mail.ru

Криптографические методы защиты информации являются объектом серьезных научных исследований и стандартизации на национальных, региональных и международных уровнях.

Целью данной научно-исследовательской работы является создание единой программной оболочки, которая объединяет в себе все уже написанные ранее приложения, реализующие различные алгоритмы шифрования. Так же целью является разработка удобного редактора для добавления новых шифров, для работы с которым не требуются глубокие знания программирования и который будет доступен для использования даже неопытным пользователям. Как расширение функций разрабатываемого программного продукта, рассматривается возможность включить в программу функцию добавления алгоритмов шифрования из специальных файлов, которые должны быть написаны по специальному шаблону. Реализация возможности добавления но-

вых шифров в программу путем подключения новых модулей или других программ представляет собой очень сложную задачу. Принципы написания программного кода в подключаемых модулях должны быть четко определены, и все новые модули должны полностью им соответствовать. Правила подключения должны быть описаны в руководстве пользователя к программе. Эта возможность позволит создавать специальные библиотеки алгоритмов шифрования.

В базовой комплектации (без подключения дополнительных модулей) программа будет содержать следующие алгоритмы шифрования:

– процесс хэширования
– афинный шифр
– афинный рекуррентный шифр
– шифр Хилла
– рекуррентный шифр Хилла
– El Gamal
– RSA
– Rabin
– AES Rijndael
– потоковый шифр Seal
– алгоритм шифрования по ГОСТ 28147-89

Данный проект создается в качестве учебного программного обеспечения для повышения удобства изучения работы различных шифров студентами соответствующих специальностей. Доступ ко всем шифрам будет возможен из одной программы, что очень удобно, особенно, в сочетании с возможностью добавления новых шифров и подключения дополнительных модулей.

Шифры, реализованные в программах, имеющих различный интерфейс, так как они были написаны разными авторами, будут объединены под одним, новым интерфейсом. Это позволит повысить производительность работы и значительно улучшить восприятие информации, так как создание новой, единой оболочки исключает необходимость пользователю осваивать новый интерфейс каждой программы и переход от одного программного продукта к другому.

При добавлении нового шифра требуется полностью изучить все этапы алгоритма его работы, такие как генерация ключей, криптографические алгоритмы зашифрования и расшифрования, и разработать способы его реализации в программе.

В результате работы должна быть написана программа, реализующая различные алгоритмы шифрования и предоставляющая возможность добавления новых шифров и подключения дополнительных

модулей, содержащих библиотеки шифров, с целью более эффективного обучения студентов соответствующих специальностей.

ЛИТЕРАТУРА

1. *Delphi 7.* «Самоучитель. Основы программирования. Решение типовых задач.» Издание 2
2. *Аграновский А.В., Хади Р.А.* «Практическая криптография : Алгоритмы и их программирование»

АНАЛИЗ СТРУКТУРЫ ФАЙЛОВ С ИСПОЛЬЗОВАНИЕМ ЯЗЫКА ПРОГРАММИРОВАНИЯ RUBY

М.Ц. Цыренова, студентка 5 курса каф. КИБЭВС
ТУСУР, г. Томск, ccmurena@sibmail.com

Главной особенностью использования семантического парсера функций является его гибкость использования на этапе проектирования программного обеспечения. Входными данными для такого анализатора являются исходные тексты программ, вне зависимости от языка программирования. Все необходимые данные закладываются, либо в шаблонах, либо профайлах (по существу отличающихся только внутренним форматом). Информацией является заданное синтаксическое правило.

Синтаксическое правило получает на входе номер слова. От этого слова правило пытается построить новую группу определенного типа, соблюдая принцип проективности. На данный момент все правила пытаются объединить входную группу только с группами, находящимися от нее справа; в нашей записи правил входная группа – это первая группа цепочки. Все правила упорядочены, поэтому в данной версии синтаксическая омонимия игнорируется, т.е. строится всегда только один вариант. Классический пример древние стены города анализатор разберет следующим образом: генит_иг(прил_сущ(древние, стены), города). Это происходит из-за того, что правило соединения прилагательного, согласованного с существительным, идет до правила, которое собирает генитивные цепочки[1].

Синтаксическое правило оперирует ограниченным числом объектов. Основными объектами являются:

1. уже построенный набор групп, к которому нужно добавить новую группу;

2. характеристики отдельных слов – омонимов входного отрезка текста.

Таким образом, синтаксические правила находятся выше омонимии, точнее омонимия находится вне этих правил.

Подобные алгоритмы наиболее просто закладываются на языке программирования Ruby.

Главная цель Ruby – эффективность разработки программ. Этот язык хорошо приспособлен для таких проблемных областей, как обработка текста, программирование CGI (есть все, что нужно, включая классы работы с текстом, библиотеку CGI, интерфейс базы данных и даже eRuby, встроенный Ruby, и mod_ruby для Apache) и XML, программирование для сети (есть поддержка сокетов), приложения с графическим интерфейсом (есть интерфейсы Ruby/Tk и Ruby/Gtk), прототипирование и обучение программированию»[2].

ЛИТЕРАТУРА

1 http://www.aot.ru.
2 http://www.chair36.msiu.ru/science/science/articles/2/html/node33.html.

КОМПЬЮТЕРНЫЕ ВИРТУАЛЬНЫЕ ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ

А.Р. Файзулин, 5 курс каф. КИБЭВС
ТУСУР, г. Томск, т.8-923-402-3773, FAnvar@mail.ru

Компьютер обладает большой вычислительной мощью, может хранить большой объем информации и представлять ее в различных формах, в дополнении к этому можно добавить возможность измерять и обработать аналоговые и цифровые сигналы. Для этого существуют как внутренние, так и внешние платы сбора и обработки данных. В качестве таких устройств используют аналогово-цифровые (АЦП) и цифро-аналоговые преобразователи (ЦАП). В последние годы активно развивается направление в области создания плат сбора данных (ПСД) для компьютера.

Виртуальное оснащение аппаратурой можно определить как объединение аппаратных средств и программного решения. Комплекс компьютеризированного прибора может заменить несколько стационарных измерительных приборов. Он имеет гибкую перенастраиваемую структуру, его конфигурация может быть составлена из различного сочетания измерительных блоков, ходящих в состав базового комплекта.

Основной задачей реализации компьютеризированных измерительных приборов является анализ и обработка аналоговых и цифровых сигналов и закономерностей. Исследовательский комплекс может включать в себя блок осциллографа и генератора. Блок осциллографический цифровой, предназначен для исследования однократных и периодических электрических сигналов. За счет регистрации их в цифровой памяти и отображения на экране ЭВМ и цифрового измерения амплитудных и временных параметров, а также математической обработки результатов измерений. Блок генератора сигналов произвольной формы, предназначен для генерации синусоидальных, прямоугольных и треугольных сигналов, сигналов произвольной формы, задаваемых аналитически, графически и программно, а также произвольной комбинации всех вышеперечисленных сигналов, путем формирования их программными средствами в цифровой памяти ЭВМ и преобразования сформированного массива данных в аналоговую форму.

Анализ аппаратной части: Многофункциональный микроконтроллер со встроенными средствами управления, компьютерная часть, устройство сопряжения компьютера и микроконтроллера, программное обеспечение. В микроконтроллер интегрирована функция аналогово-цифрового (АЦП) и цифро-аналогового преобразования (ЦАП). АЦП представляет собой АЦП последовательных приближений, работающий в режиме как единичного, так и непрерывного преобразования. Для запоминания результатов преобразования используется либо режим прерываний при невысокой работе АЦП, либо режим прямого доступа, не влияющего на работу микроконтроллера и позволяющий сохранять результаты преобразования во внешнем оперативном запоминающем устройстве (ОЗУ). Микроконтроллер должен быть оснащен устройством обмена и ввода вывода через параллельный или последовательный интерфейс. Компьютер должен быть обеспечен достаточными ресурсами для работы с панелью приборов и внешним устройством. В программное обеспечение приборов входит прошивка внешнего устройства микроконтроллера, программа – драйвер внешнего устройства, виртуальная панель функциональных блоков прибора. Устанавливается связь: прошивка – драйвер внешнего устройства – панель прибора. Прошивка содержит команды управления и настройки микроконтроллера. Драйвер является посредником и обработчиком команд и данных, как для микроконтроллера (МК), так и для компьютерной панели прибора. Компьютерная панель представляет собой уст-

ройство управления микроконтроллером, в котором устанавливаются параметры функционирования микроконтроллера.

Задачей реализации прибора является выбор панелей с точки зрения функциональности, состава и удобство в пользовании. Создание программных панелей приборов возможно во многих программных средах, но наиболее эффективным решением данной задачи будет среда, профилирующая построение виртуальных приборов различного типа и назначения. Такой средой является программный продукт «LabView» от фирмы «National Instruments». Основным принципом построения системы сбора, обработки и управления на базе программного обеспечения фирмы «National Instruments» является возможность превращения персонального компьютера в измерительный комплекс, с требуемыми метрологическими характеристиками. Конфигурировать измерительные комплексы в системе «LabView» можно как от датчиков и исполнительных механизмов (измерительная часть), так и от обработки данных (вычислительная часть). В первом случае необходимо подсоединить датчики к персональному компьютеру и провести аналогово-цифровое преобразование аналоговых сигналов для дальнейшей обработки данных и построения отчетов. Во втором случае задача решается встроенными программными средствами обработки сигналов, статического анализа, имитации, при необходимости работы внешних устройств.

Задача управления прибором состоит в исполнении микроконтроллером всех функций ввода и вывода, как команд, так и данных, для получения аналоговых и цифровых сигналов. Интерпретатором функций будет драйвер устройства. Входные и выходные параметры прибора это частота, амплитуда, смещение, скважность, время преобразования сигнала.

Данный комплекс можно применять для автоматизации научных исследований, диагностики электрических схем, использование в лабораторных комплексах и для изучения. Он может быть использован для создания автоматизированных измерительных рабочих мест исследователя, настройщика, учащегося.

Данное решение позволяет за счет МК и компьютера реализовать недорогой, функциональный комплекс приборов. Компьютеризированный прибор по сравнению со стационарным прибором имеет большие преимущества: скорость преобразования, автоматизация процесса измерений, решение множества задач в составе набора нескольких блоков приборов, компактность.

ГЕОИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В АНАЛИЗЕ РЫНКА НЕДВИЖИМОСТИ

Т.С. Калинина, студент 4 курса каф. КИБЭВС;
С.С. Прозорова, ассистент каф. КИБЭВС
ТУСУР, г. Томск, e-mail: trinlove@mail2000.ru

Анализ рынка недвижимости является сложным процессом. При оценке объектов недвижимости (квартира, земля, магазин, завод и т.п.) необходимо учитывать множество различных факторов наиболее существенные, из которых напрямую связаны с месторасположением объекта. Некоторые факторные признаки объектов являются атрибутивными, т.е. необходимо введение неких коэффициентов, позволяющих перевести атрибутивные данные в количественные. Существенные факторы и степень влияния каждого из них на уровень цены определяется экспертом по рынку недвижимости.

Наше восприятие устроено так, что большую часть информации человек воспринимает визуально. Для упрощения ее представления часто используются различные графики, диаграммы, но если данные связаны с географическим положением объектов, как в нашем случае, необходим пространственный анализ поверхностей. Для решения проблемы анализа рынка недвижимости, а также визуализации исходных данных и результатов анализа наиболее оптимально использовать современные технологии – географические информационные системы (ГИС).

В достижении поставленной цели – пространственного анализа оценки недвижимости можно выделить три проблемы:

– разработка математического обеспечения (модель, методы, алгоритмы) анализа рынка недвижимости;

– разработка программного обеспечения системы анализа рынка недвижимости, реализующей систему ввода, хранения, обработки информации о состоянии рынка недвижимости;

– визуализация результатов анализа с использованием геоинформационных систем.

На основе сформулированных проблем можно определить задачи, последовательное решение которых поможет достигнуть поставленной цели:

1. Выделить исследуемые объекты и признаки, необходимые для их группирования.
2. Разработать базу данных для эффективного хранения полученной первичной информации.
3. Определить минимальный набор существенных факторных признаков и степень их влияния.

4. Разработать математическое обеспечение инструментальной ГИС, которое включает в себя:

- модель формирования цены объекта недвижимости;
- систему статистического анализа и обработки информации для получения данных, пригодных для отображения с помощью ГИС);
- метод восстановления двумерного геополя по точечным данным;
- метод и алгоритм анализа двумерного геополя с целью выявления пространственных закономерностей.

5. Разработать программный продукт, реализующий поставленные задачи и визуально представляющий геополя на карте исследуемой области.

6. Провести апробацию результатов работы во взаимодействии с агентствами по оценке недвижимости.

Рынок недвижимости имеет не однородную структуру. Он оперирует различного рода объектами: участки земли, предприятия, фирмы, жилой фонд. Выделять объекты целесообразно согласно их функциональному назначению: так как именно от функционального назначения будет зависеть набор признаков самих объектов. Для осуществления дифференцированного подхода к их оценке вводим следующую классификацию объектов недвижимости:

– свободные земельные участки;
– жилые здания и помещения (квартиры, комнаты);
– административные здания и помещения (офисы);
– постройки для промышленности;
– помещения торговли, складские и сферы услуг.

Для картографического отображения уровня цен объектов недвижимости удобнее всего представить каждый сегмент классификации отдельным слоем изолиний и изоконтуров, с возможностью более глубокой детализации (изменением масштаба карты, детализации самого объекта). При этом будут рассматриваться двумерные геополя. Т.е. поверхности, однозначно описываемые функцией от двух пространственных координат x и y. В нашем случае – распределение в пространстве уровня цен объектов недвижимости.

В рамках задач п. 4 одним из наиболее сложных является вопрос восстановления геополей.

Система статистического анализа и обработки первичной информации предназначена для получения точечных данных по цене реализации объекта за 1 кв.м. На основе полученных точечных данных производиться построение математической модели двумерного геополя. Но так как со статистической точки зрения получить абсолютно все данные, необходимые для построения невозможно, необходимо ре-

шить, каким образом будут получены недостающие данные для областей двумерного геополя слабой или нулевой концентрации. При этом стоит учитывать, что дополнительные данные, полученные таким образом, тоже должны учитываться при выявлении пространственных закономерностей. К таким закономерностям относится, например, влияние различных близлежащих объектов на цену реализации друг друга. Также на основе двух и более статистических сводок за разные периоды времени полезным будет выявление временных изменений.

ЛИТЕРАТУРА

1. *Новиков Б.Д.* Рынок и оценка недвижимости в России. М.: «Экзамен», 2000. 512 с.
2. *Кудинов А.В., Марков Н.Г.* Геоинформационные технологии в управлении пространственными инженерными сетями. Томск: Изд-во ТПУ, 2004. 177 с.
3. *Ковин Р.В.* Алгоритмическое и программное обеспечение геоинформационной системы для анализа двумерных геополей. Томск: Изд-во «Томский ЦНТИ», 2004. 19 с.
4. *Гусаров В.М.,* Статистика: учебное пособие для вузов. М.: ЮНИТИ-ДАНА, 2002. 463с.

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ МИКРОКОНТРОЛЛЕРА ПЛАНШЕТНОГО ГРАФОПОСТРОИТЕЛЯ

С.Л. Крыловский, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, Vendigo_ST@mail.ru

Основной задачей является, разработка программы для микроконтроллера (МК) планшетного графопостроителя. Построитель планируется применять в учебном процессе в качестве доступного технического средства изучения основ микропроцессорного управления периферийным оборудованием и в качестве устройства вывода графических документов.

Устройство предназначено управлять:

− двумя шаговыми двигателями перемещения платформы пишущего узла по координатам плоскости X и У;

− соленоидом подачи пишущего пера к носителю графического изображения;

− обменом информацией с ПК – носителем программ ввода/вывода.

С помощью программы необходимо реализовать следующие функции МК:

− ручной режим;

− автоматический режим;
− тестовый режим;
− режим восстановления;
− обмен данными с ПК.

К решению этой задачи необходимо применить системный подход во избежание ошибок при написании программных модулей, и для структуризации программы. Одной из проблем при разработке программы является отсутствие программных отладочных средств для данного контроллера либо большой их стоимостью. Для решения данной проблемы отладка программы производилась на макете, т.к. стоимость отладочного макета значительно меньше стоимости программного отладочного продукта. В качестве инструмента при разработке программных модулей применялась профессиональная среда разработки Keil µVision 3. Данная среда позволяет исходный код программы писать на языках C51(Си 51) и/или A51(Ассемблер 51). Программа будет писаться на языке C51, т.к. он является наиболее функциональным по сравнению с A51. На языке A51 написаны критические участки кода. При написании программы, во–первых, необходимо разбить ее на модули так, чтобы каждый из них выполнял определенную функцию. Во–вторых, определить для каждого модуля его иерархический уровень. Разрабатывать программу необходимо снизу вверх, следуя по иерархическим уровням. Иерархическая структура изображена на рисунке. Применение данного подхода значительно уменьшит размеры, занимаемые файлом прошивки микроконтроллера.

Иерархическая структура

Программа написана на языке высокого уровня C51, а критические участки кода – на A51. В данном случае критическими участками кода являются обработчики внешних прерываний INT0 и INT1. Выбор языка программирования A51 связанно с тем, что в языке C51 обработчики прерываний должны обязательно иметь «begin» или «({)» и «end» или «(})», а обработчики – A51 в конце могут иметь «reti». По событию «end» происходит вызов инструкции процессора «reti», в результате чего происходит выполнение программы с того места, где произошло прерывание. Чтобы реализовать функции мгновенного перехода в ручной режим по нажатию кнопки «Стоп» на пульте построителя и мгновенного перехода в режим восстановления по нажатию кнопки «Восстановление» необходимо после прерывания вернуться в мониторный модуль. Поэтому необходимо сначала очистить стек и вместо «reti» выполнить инструкцию «ljmp»,

т.е. по выходу из обработчика прерывания перейти на выполнение мониторного модуля. Использование прерываний значительно упростит реализацию данных функций. Программа для МК состоит из 7 основных модулей , 2х обработчиков прерываний и мониторного модуля.

Эти модули следующие:

− MAIN – мониторный модуль (ММ). Ее основная цель – синхронизация работы всех основных и вспомогательных программных модулей.

− GENERATOR – генератор команд (ГК). Данный программный модуль генерирует команды в зависимости от режима его работы. В режиме №1 – генерируются команды от пульта ПГ, в режиме №2 – от UART. КОП считывается из ПК по интерфейсу RS-232.

− INTERPRETER – интерпретатор команд (ИК). Данный модуль интерпретирует команду, сгенерированную ГК, и вызывает соответствующий обработчик команды.

− COUNTER – счетчик координат (СК). Данный программный модуль осуществляет счет текущей координаты и запрещает выход за пределы поля рисования. При достижении края области рисования зажигается светодиод «Предел « на пульте ПГ и прекращается движение каретки.

− DRIVER_UART – драйвер последовательного порта МК. Данный программный модуль позволяет обмениваться словом с ПК по протоколу RS-232.

− DRIVER_INDICATORS – драйвер индикаторов. Данный программный модуль осуществляет работу со светодиодами пульта ПГ.

− DRIVER_ DEVICE – драйвер внешних устройств (ВУ). Данный программный модуль осуществляет работу со внешними устройствами.

− DRIVER_ENGINES – драйвер шаговых приводов. Данный программный модуль в зависимости от направления движения генерирует управляющие сигналы, которые необходимы для работы двигателей. Осуществляется один шаг в определенном направлении. Его основная цель – управлять шаговыми приводами.

Данный системный подход позволил написать программу для МК, которая выполняет все перечисленные выше функции.

ЛИТЕРАТУРА

1. *Бродин В.Б., Калинин А.В.* Системы на микроконтроллерах и БИС программируемой логики. М.: Издательство ЭКОМ, 2002. 400с.
2. www.atmel.com/literature/
3. www.keil.com/support/

РАЗРАБОТКА СХЕМЫ ЭЛЕКТРИЧЕСКОЙ ПРИНЦИПИАЛЬНОЙ ДЛЯ МОДУЛЯ УПРАВЛЕНИЯ ПЛАНШЕТНОГО ГРАФОПОСТРОИТЕЛЯ

С.Л. Крыловский, студент 5 курса каф. КИБЭВС
ТУСУР, г.Томск, Vendigo_ST@mail.ru

Задача состоит в разработке схемы электрической принципиальной модуля управления (МУ) планшетного графопостроителя.

Устройство предназначено управлять:

− двумя шаговыми двигателями перемещения платформы пишущего узла по координатам плоскости X и У;

− соленоидом подачи пишущего пера к носителю графического изображения;

− обменом информацией с ПК – носителем программ ввода/вывода.

Требования к функциональному составу МК:

− исполнить на микропроцессорной элементной базе;

− предусмотреть в составе силовые элементы управления электромеханическими узлами;

− предусмотреть оперативную память для загрузки кадров выводимой информации;

− предусмотреть средства подключения к ПК в режиме отладки программы микроконтроллера (МК).

При решении поставленной задачи необходимо провести ряд действий:

− провести анализ технических средств (объектов управления: шаговых приводов (ШП), внешней ОЗУ, соленоида, кнопок, датчиков и т.д.);

− построить функциональную схему;

− выбрать элементную базу;

− разработать схему электрическую принципиальную;

− провести анализ полученного результата.

На первом этапе проектирования необходимо провести анализ технических средств и изучить методы управления ими. В качестве объектов управления имеются: 2 шаговых привода постоянного тока, 1 соленоид, 6 датчиков, 14 кнопок, 11 светодиодов.

Управление шаговыми приводами осуществляется последовательной подачей управляющего напряжения на его обмотки. МК вырабатывает управляющие сигналы, которые далее поступают на полевые транзисторы – силовые элементы управления ШП.

Опрос датчиков и кнопок осуществляется по средством последовательного считывания с регистров (RG1−RG3) информации о их со-

стоянии. Эти регистры подключены через двунаправленный шинный формирователь «F». Переключение направления работы формирователя осуществляется элементом 3И-НЕ входы, которого подключены к соответствующим выходам демультиплексора (DMX). Демультиплексором осуществляется выбор регистра. При работе МК с датчиками и кнопками формирователь работает в обратном направлении, а при работе с соленоидом и светодиодами – в прямом. При работе с внешним ОЗУ необходимо использовать мультиплексированную шину адрес/данные. Что бы реализовать данную функцию необходимо использовать регистр адреса (RGA), который при передачи адреса от МК к ОЗУ открывается. Это осуществляется подачей на вход «C» регистр адреса высокого уровня с управляющего сигнала «ALE». Данный сигнал вырабатывается МК для сопровождения адреса. При передачи или приеме данных в ОЗУ регистр адреса находится в режиме хранения.

Так же в МУ реализован режим отладки программы микроконтроллера. При прошивке контроллера программатор PonyProg 2000 выставляет на линии RST высокий уровень. В этот момент сигналы от LPT порта не проходят на транзисторные ключи, а идут прямо на SPI выводы МК. При работе построителя сигналы от МК не поступают на выводы LPT порта, а поступают только на управляющие транзисторные ключи. Для связи ПК с построителем используется трансивер/преобразователь. Он согласует логические уровни и входные сопротивления COM порта с выводами RxD и TxD МК.

В результате проделанной работы была разработана схема электрическая принципиальная МУ.

ЛИТЕРАТУРА

1. *Бродин В.Б., Калинин А.В.* Системы на микроконтроллерах и БИС программируемой логики. М.: Издательство ЭКОМ, 2002. 400с.
2. *Сташин В.В., Урусов А.В., Мологонцева О.Ф.* Проектирование цифровых устройств на однокристальных микроконтроллерах. М.: Энергоатомиздат, 1990. 224с.

РАСПОЗНАНИЕ РЕЧИ С УЧЕТОМ ОСОБЕННОСТЕЙ РЕЧЕОБРАЗОВАНИЯ

А.Н. Квасов, аспирант кафедры КИБЭВС
ТУСУР, г. Томск, itgroup@inbox.ru

Задача распознавания речи решается уже довольно продолжительное время [1], но системы, обладающие средствами речевого ввода информации, остаются далекими от совершенства. Во многом это свя-

зано со сложностью самих процессов речеобразования и речевосприятия. Проблема оказалась сложной и обладающей свойством разветвляться в другие области знаний: статистическую радиотехнику, лингвистику, психоакустику, анатомию и многие другие[1]. Существенно снизить вероятность ошибки распознания речи и идентификации позволяет информация о поле диктора, для чего необходима разработка методик автоматической идентификации пола диктора по речевому сигналу (AGI – Automatic Gender Identification) [2, 3, 4]. Основным подходом для решения задачи AGI является выявление информативных параметров и набор статистики [2, 3, 4] с целью эвристического поиска механизма функционирования акустической системы. Обычно эти подходы реализуются с помощью кепстральных коэффициентов или коэффициент косинусного преобразования Фурье и моделей Гаусса. Недостатком данного подхода является слабая связь с параметрами анатомии человека. Предлагаемый подход заключается в построении модели речеобразовательной системы человека, что позволит определить роль параметров элементов системы речеобразования на структуру речевого сигнала. В частности установить отличия между мужской и женской речью. Для решения этой задачи необходимо проанализировать строение и принцип действия речеобразовательной системы, а также различия речевых аппаратов мужчин и женщин.

Речевой аппарат состоит из двух тесно связанных между собой частей: центрального (или регулирующего) речевого аппарата и периферического (или исполнительного) [5, 6]. Центральный речевой аппарат находится в головном мозге. Он состоит из коры головного мозга (преимущественно левого полушария), подкорковых узлов, проводящих путей, ядер ствола (прежде всего продолговатого мозга) и нервов, идущих к дыхательным, голосовым и артикуляторным мышцам [5]. Периферический речевой аппарат состоит из трех отделов: 1) дыхательного; 2) голосового; 3) артикуляционного (или звукопроизводящего) [5]. Органы речи периферического аппарата также делятся на активные – подвижные органы, и пассивные – неподвижные органы [5, 6]. Основными частями исполнительного периферического аппарата являются: дыхательная система, гортань, ротовая и носовая полость.

Речь, как и другие проявления высшей нервной деятельности, развивается на основе рефлексов. Речевые рефлексы связаны с деятельностью различных участков мозга. Лобные извилины (нижние) являются двигательной областью и участвуют в образовании собственной устной речи (центр Брока). Височные извилины (верхние) являются речеслуховой областью, куда поступают звуковые раздражения (центр Вернике). Благодаря этому осуществляется процесс восприятия чужой

речи. Для понимания речи имеет значение теменная доля коры мозга. Изначально основная структура высказывания формируется в зоне Вернике, затем она по дугообразному пучку передается в зону Брока, где включает детальную и координированную программу вокализации [7]. Эта программа приходит в смежные лицевые области моторной коры, которая активирует соответствующие мышцы рта, губ, языка и т.д.

Рассмотрим основные отличия параметров элементов системы речеобразования мужчин и женщин (таблица).

Основные отличия речевых аппаратов мужчин и женщин

Название параметра	Знач. муж.	Знач. жен.
Жизненная емкость легких	3,5-7,0 л	2,5 – 6,0 л
Диаметр трахеи	13-27 мм	10-23 мм
Длина трахеи	9 – 13 см	8 – 12 см
Длинна голосовых складок	20-24 мм	18-20 мм
Ширина голосовых складок	3-3.5 мм	2.5 – 3 мм
Длина гортани	44 мм	36 мм
Поперечный диаметр гортани	43 мм	41 мм
Переднезадний диаметр гортани	36 мм	26 мм
Длина речеобразующего тракта	16.5 – 18 см	13.5 -16 см

Самыми существенными отличиями мужского речеобразующего тракта от женского являются – длина речеобразующего тракта, размеры гортани, параметры голосовых складок.

Не удалось найти какие – либо достоверные сведения о различиях в области управления и координации речи у мужчин и женщин.

В ходе работы было проанализировано строение, и принцип действия речеобразовательной системы, а также были проанализированы различия мужской и женской речевых систем. Наиболее вероятной причиной отличия женского голоса от мужского являются различия в строении речевых аппаратов, в частности длина речеобразующего тракта, размеры гортани, параметры голосовых складок. Эти отличия могут быть учтены при построении математической модели для определения их степени влияния на речевой сигнал, с целью формулирования критериев анализа речи при определении пола диктора.

ЛИТЕРАТУРА

1. *Коцубинский В.П.* Математические модели образования звучной речи. Дисс. на соискание ученой степени кандидата технических наук. Томск 2004. 151 с.
2. *Vergin R., Farhat A., O'Shaughnessy D.* Robust gender-dependent acoustic-phonetic modeling in continuous speech recognition based on a new automatic male/female classification. INRS-Telecommunications 16 Place du Commerce, Ile-des-Sceurs, H3E1H6, Quebec, Canada.

3. *Sigmund M., Dostal T.* Automatic Gender Distinction by Voice. – (Czech Republic) ACTA Press publishes numerous proceeding volumes for international conferences in the general areas of engineering and computer science.
4. *Slomka S., Sridharan S.* Автоматическая идентификация пола диктора в неблагоприятных условиях. ICASSP 97.
5. *Филичева Т.Б.* Основы логопедии: Учеб. пособие для студентов пед. ин-тов по спец. «Педагогика и психология (дошк.)» / Филичева Т. Б., Чевелева Н.А.., Чиркина Г.В. М.: Просвещение, 1989. 223 с.
6. Домашняя медицинская энциклопедия. Гл. ред. Покровский В.И. В одном томе. М.: «Медицина», 1993. 496 с.
7. *Балацкая Л.Н., Бондаренко В.П., Корнилов А.Ю., Коцубинский В.П., Терешков А.М.* Биологическая обратная связь при обучении устной речи. РАО 2005.

АНАЛИЗ РЕЧЕВОГО ПОТОКА В ЗАДАЧАХ ИДЕНТИФИКАЦИИ ДИКТОРА

А.Н. Квасов, аспирант кафедры КИБЭВС
ТУСУР, г. Томск, itgroup@inbox.ru

В связи с ростом производительности вычислительной техники начали активно развиваться методики идентификации диктора по голосу и распознавания речи, которые находят все большее применение в повседневной жизни. Но задачи идентификации личности и распознания речи по сегодняшний день остаются актуальными и полностью не решенными [1, 2, 3]. Одним из способов повышения эффективности подобных систем является учет информации о поле диктора [1, 2, 3]. В связи с чем, представляет интерес анализ речевого потока с целью оценки возможности идентификации пола диктора. Это требует определение элементов речевого потока на основе которых можно проводить идентификацию, параметры, которые могут нести информацию о дикторе.

С физической точки зрения устная речь состоит из последовательности звуков речи гласных и согласных, произносимых, как правило, слитно, с паузами только после отдельных слов или групп звуков. Слитность произношения звуков речи, вследствие непрерывности артикуляционных движений органов речи, вызывает взаимное влияние смежных звуков друг на друга. Артикуляционные органы имеют неодинаковые размеры у разных людей, и каждому человеку свойственна своя манера произнесения звуков речи, поэтому для каждого человека звуки речи имеют индивидуальный характер. Но при всем их многообразии они являются физическими реализациями небольшого

числа фонем (наименьшая звуковая единица данного языка, существующая в речи в целом ряде конкретных звуков). В русской речи их насчитывается 41. Звуки также можно подразделить на вокализованные и невокализованные.

Формирование невокализованных звуков связано с наличием какой-либо шумообразующей преграды (артикуляторов) для выходящей из легких струи воздуха, например язык, зубы, губы и т.д. образуя завихрения, создающие шумы с широкополосным сплошным спектром.

Процесс формирования вокализованных звуков намного сложнее, они характеризуются наличием голоса (фонацией), их артикуляция обусловлена вибрацией голосовых связок и свободным проходом выдыхаемого воздуха через ротовую полость. Импульсы потока воздуха, создаваемые голосовыми связками при произнесении звонких звуков речи, могут считаться периодическими. Находящиеся в гортани голосовые складки, или связки, выступают в качестве модулятора создаваемого легкими воздушного потока.

Акустически мелодические характеристики речи соотносятся с изменяющейся во времени частотой самой низкой составляющей в спектре звука – частотой основного тона. Частота основного тона является величиной, обратной периоду колебания, и характеризует все периодические и квазипериодические звуки. Частота основного тона – базовая частота колебаний голосовых связок она лежит обычно в пределах от 70 до 450 Гц. В речевых звуках первый период колебания соответствует полному циклу работы голосовых связок. Изменение частоты основного тона во времени имеет сложную структуру (рис. 1). Соседние периоды основного тона, как правило, отличаются по величине друг от друга, и эти различия передают разную информацию. Участок сигнала, отмеченный работой голосовых связок, называется вокализованным. Импульсы основного при их периодическом повторении образуют дискретный спектр с большим числом обертонов или гармоник. Речевой тракт представляет собой сложный акустический фильтр с рядом резонансных полостей, создаваемых артикуляционными органами, в результате чего выходной сигнал, т. е. произносимая речь, имеет спектр с огибающей сложной волнообразной формы. Максимумы концентрации энергии в спектре звука называются формантами, а резкие провалы – антиформантами. В речевом тракте у каждого звука речи свои резонансы и антирезонансы, поэтому, огибающая спектра этого звука имеет индивидуальную форму. Для большинства гласных звуков речи характерно свое расположение формант, антиформант и соотношение их уровней, для согласных важен также ход изменения формантных частей во времени [4].

У звонких звуков речи, особенно гласных, высокий уровень интенсивности, у глухих – самый низкий. Поэтому при произнесении речи громкость ее непрерывно изменяется, особенно резко при произнесении взрывных звуков. Диапазон уровней речи находится в пределах 35–45 дб. Длительность гласных звуков в среднем около 0,15 сек, согласных – около 0,08 сек, звука «п» – около 0,03 сек [4].

В теоретической фонетике существует понятие коартикуляция, означающее взаимовлияние соседних звуков. С точки зрения артикуляции человек не может после произнесения одного звука мгновенно перестроить речевой аппарат, чтобы произнести следующий звук – возникает фаза перестройки речевого аппарата или переходный участок. Упрощенно можно сказать, что речь состоит из стационарных участков звуков и переходов между ними. Эти переходные участки бывают, невелики по длительности, но зато очень информативны. Индивидуальный характер артикуляторных конфигураций определяется не только индивидуальными особенностями анатомического строения речеобразующего тракта, но и индивидуальными характеристиками коартикуляции, т. е. влиянием соседних звуков на данный. Тем самым можно говорить не только об индивидуально-анатомических типах, но и об индивидуальных типах динамики развития артикуляторных конфигураций в процессе речеобразования [5].

В ходе работы были проанализированы элементы и параметры речевого потока. При решении задач определения параметров анатомии, в частности пола диктора из слитной речи интерес представляют не только вокализованные звуки на стационарном участке, но и переходные участки которые могут содержать информацию о поле диктора и особенностях строения речевого аппарата, а также об индивидуальном типе функционально–динамических комплексов навыков артикуляции.

ЛИТЕРАТУРА

1. *Vergin R., Farhat A.*, *O'Shaughnessy D.* Robust gender-dependent acoustic-phonetic modeling in continuous speech recognition based on a new automatic male/female classification. INRS-Telecommunications 16 Place du Commerce, Iles-des-Sceurs, H3E1H6, Quebec, Canada.
2. *Sigmund M., Dostal T.* Automatic Gender Distinction by Voice. (Czech Republic) ACTA Press publishes numerous proceeding volumes for international conferences in the general areas of engineering and computer science.
3. *Slomka S., Sridharan S.* Автоматическая идентификация пола диктора в неблагоприятных условиях. ICASSP 97.
4. *Сапожков М. А.*, Речевой сигнал в кибернетике и связи. М.: Радио и связь, 1963. 357 с.
5. *Галунов В.И.*, Исследование вариативности речевого поведения человека. Автореф. дис., на соискание ученой степени доктора биологических наук.

АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ И АРХИТЕКТУРЫ УМК SDK1.1

О.В. Лядин, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 8-903-914-6661, ladinoleg@mail.ru

Внедрению УМК SDK1.1 в учебный процесс препятствует низкое качество сопроводительной документации, что не позволяет однозначно интерпретировать технический материал. Поэтому необходимым является исследование путем натурных экспериментов, сбора дополнительной информации по объектам состава стенда с тем, чтобы восполнить названный пробел.

Для ускоренного освоения приемов работы с элементной базой однокристальных ЭВМ и стенда в частности, необходима доработка технических материалов производственных организаций в форму ориентированную на обеспечение учебного процесса.

В сопроводительной документации на учебный стенд УМК SDK1.1 имеется ряд неточностей, основное из которых – несоответствие истинных компонент заявленному составу. Путем исследования было определено, что предъявленный стенд построен на базе однокристальной микро-ЭВМ ADuC842 и содержит в своем составе следующие устройства:

– микроЭВМ ADuC842 с архитектурой MCS-51.

– flash-память 128Кб, которая подключена к внешнему разъему ADuC842 и используется как память данных.

– оптически развязанный приемопередатчик инструментального канала RS232C.

– E2PROM-память (2 Кбайт), подключенная к ADuC842 через интерфейс I2C;

– интегральные часы со встроенным ОЗУ PCF8583 (Philips), подключены так же через I2C;

– модуль символьного ЖКИ 2*16;

– матричная клавиатура 4*4;

– звуковой излучатель;

– 8 управляемых светодиодов.

После тщательного анализа состава стенда, была проведена проверка работоспособности всех его компонентов. С использованием Assembler были написаны тестовые программы, наглядно показывающие работу отдельных устройств стенда. Все эти программы могут быть использованы в виде модулей для создания более крупных проектов.

Работа с ЖКИ, клавиатурой, светодиодами и звуковым излучателем ведется через регистры ПЛИС MAX3064 (фирмы Altera).

Как уже было сказано, часы и E2PROM-память (2 Кбайт) подключены к ADuC842 через интерфейс I2C. Стандартная диаграмма передачи данных представлена на рисунке.

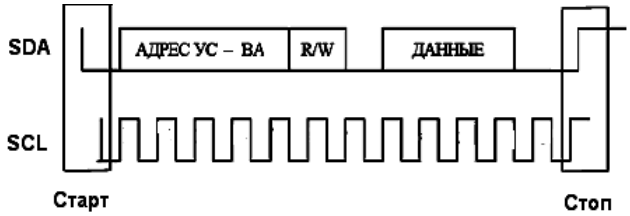


Диаграмма передачи данных по I2C

Разработчики SDK1.1 рекомендуют вести работу со стендом в инструментальной среде mVision фирмы Keil. Однако автоматическое создание приложений на начальном этапе усложняет процесс обучение основам микропроцессорной техники. Поэтому был предложен следующий алгоритм работы с УМК SDK1.1:

1. Созание программы на Assembler.

С помощью ассемблера версии 2.5 поддерживающего систему команд ядра Intel MCS-51 в текстовом редакторе составляется листинг программы. Это позволяет сделать программы более наглядными, чем при использовании mVision.

2. Компиляция программы, в результате чего создается HEX образ программы. Компиляция осуществляется с помощью TASM – набора таблично управляемых кросс ассемблеров.

3. Загрузка HEX образа программы в память микроЭВМ и передача ей управления.

Последний этап реализуется за счет прилагаемых к стенду программ, одна из которых (HEX202) находится в памяти микроЭВМ, а другая (T2) находится на ПК. После создания HEX образа необходимо запустить программу T2, с помощью которой по RS232 данные передаются в микроЭВМ. Программа HEX202, распознает принимаемые данные и записывает их по назначенному адресу во внутреннюю память ADuC842, которая имеет объем 62 Кбайт.

Стенд SDK-1.1 имеет дискретный 20-тиразрядный параллельный порт, позволяющий организовать взаимодействие с различными цифровыми устройствами.

Из всего выше сказанного можно сделать вывод о том, что основными областями использования комплекса являются:

- обучение основам вычислительной и микропроцессорной техники, систем управления;
- автоматизация простых технологических процессов и лабораторных исследований;
- макетирование микропроцессорных систем, отладка программного обеспечения для систем на базе широко распространенного ядра Intel MCS-51;

• построение устройств управления приборами разнообразного применения.

Доработанная документация в сочетании с комплексом примеров программ для УМК SDK1.1 позволила создать серию лабораторных работ для студентов по курсу микропроцессорной техники. Для этого все указания к лабораторным работам выполнены в виде единой обучающей программы.

ЛИТЕРАТУРА

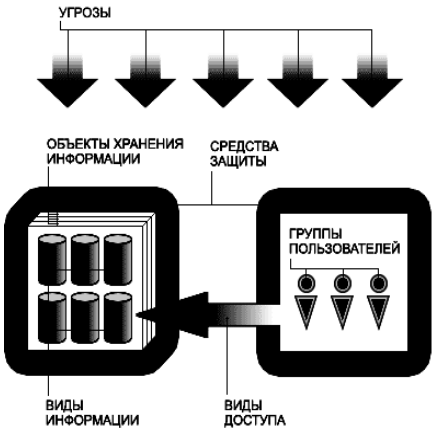
1. *Интернет* (http://lmt.cs.ifmo.ru)
2. *ООО «ЛМТ»* 2001 г. Учебный стенд SDK 1.1 Руководство пользователя.
3. *Бродин В.Б., Калинин А.В.* «Системы на микроконтроллерах и БИС программируемой логики»

МЕТОДЫ ОЦЕНКИ РИСКОВ

П.С. Лысюк, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, т. 8-909-546-91-89, e-mail pallmell@ms.tusur.ru

Обеспечение информационной безопасности – одна из главных задач современного предприятия. Угрозу могут представлять не только технические сбои, но и несогласованность данных в различных учетных системах, которая встречается едва ли не у каждой второй компании, а также неограниченный доступ сотрудников к информации



Информационные риски – это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий. Иными словами, IT-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи, что схематично изображено на рисунке.

Процесс оценивания рисков

Процесс оценивания рисков содержит несколько этапов*:*

– Идентификация ресурса и оценивание его количественных показателей (определение потенциального негативного воздействия на бизнес).

– Оценивание угроз.

– Оценивание уязвимостей.

– Оценивание существующих и предполагаемых средств обеспечения информационной безопасности.

– Оценивание рисков.

На основе оценивания рисков выбираются средства, обеспечивающие режим ИБ. Ресурсы, значимые для бизнеса и имеющие определенную степень уязвимости, подвергаются риску, если по отношению к ним существует какая-либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для них.

Сегодня существует ряд подходов к измерению рисков. Давайте рассмотрим наиболее распространенные подходы, а именно оценку рисков по двум и по трем факторам.

*Оценка рисков по двум факторам***.** В простейшем случае используется оценка двух факторов: вероятность происшествия и тяжесть возможных последствий. Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий. Общая идея может быть выражена формулой:

$$\text{РИСК} = P_{\text{происшествия}} \times \text{ЦЕНА ПОТЕРИ}$$

Если переменные являются количественными величинами, то риск – это оценка математического ожидания потерь.

Если переменные являются качественными величинами, то метрическая операция умножения не определена. Таким образом, в явном виде эта формула использоваться не должна. Рассмотрим вариант использования качественных величин (наиболее часто встречающаяся ситуация). Вначале должны быть определены шкалы. Определяется субъективная шкала вероятностей событий, например: *A* – Событие практически никогда не происходит; *B* – событие случается редко; *C* – вероятность события за рассматриваемый промежуток времени – около 0,5; *D* – скорее всего, событие произойдет; *E* – событие почти обязательно произойдет

Кроме того, определяется субъективная шкала серьезности происшествий, например:

N (Negligible) – воздействием можно пренебречь; Mi (Minor) – незначительное происшествие: последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию – незначительно. Mo (Moderate) – происшествие с умеренными результатами: ликвидация последствий не связана с крупными затратами; воздействие на информационную технологию невелико и

не затрагивает критически важные задачи. S (Serious) – происшествие с серьезными последствиями: ликвидация последствий связана со значительными затратами; воздействие на информационные технологии ощутимо, воздействует на выполнение критически важных задач. C (Critical) – происшествие приводит к невозможности решения критически важных задач.

Для оценки рисков определяется шкала из трех значений:

– Низкий риск,

– средний риск,

– высокий риск.

*Оценка рисков по трем факторам***.** В зарубежных методиках, рассчитанных на более высокие требования, чем базовый уровень, используется модель оценки риска с тремя факторами: угроза, уязвимость, цена потери. Угрозу и уязвимость определим следующим образом.

Угроза – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

Уязвимость – слабость в системе защиты, которая делает возможным реализацию угрозы.

Вероятность происшествия, которая в данном подходе может быть объективной либо субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей:

$$P_{\text{происшествия}} = P_{\text{угрозы}} \times P_{\text{уязвимости}}$$

Соответственно, риск определяется следующим образом:

$$\text{РИСК} = P_{\text{угрозы}} \times P_{\text{уязвимости}} \times \text{ЦЕНА ПОТЕРИ}$$

Данное выражение можно рассматривать как математическую формулу, если используются количественные шкалы, либо как формулировку общей идеи, если хотя бы одна из шкал – качественная. В последнем случае используются различного рода табличные методы для определения риска в зависимости от трех факторов.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании. При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами (например, при определении стоимостных характеристик), так и качественными (например, учитывающими штатные или чрезвычайно опасные нештатные воздействия

внешней среды). Таким образом, анализ и управление информационными рисками позволяет обеспечить экономически оправданную безопасность компании.

ЛИТЕРАТУРАЪ

1. *Основы* Информационной Безопасности. Р.В Мещеряков, А.А Шелупанов. ТУСУР, 2002.
2. *Балашов П.А., Кислое Р.И., Безгузиков В.П.* Оценка рисков информационной безопасности на основе нечеткой логики // Безопасность компьютерных систем. Конфидент. 2003. № 5.
3. *Современные* технологии анализа рисков в информационных системах (PCWEEK N37'2001), Сергей Симонов. http://daily.sec.ru
4. *Материалы* компании «Джет Инфосистемс». http://daily.sec.ru
5. *Материалы* компании «Digital Security». http://daily.sec.ru
6. *Александрович Г.Я., Нестеров С.Н., Петренко С.А*. Автоматизация оценки информационных рисков компании// Там же. №2. С. 78-81.
7. http://www1.rql.kiev.ua/library/11/main.htm

УПРАВЛЕНИЕ ПРОЦЕССОМ РЕЧЕВОЙ РЕАБИЛИТАЦИИ НА ОСНОВЕ БИОЛОГИЧЕСКОЙ ОБРАТНОЙ СВЯЗИ

А.Б. Миронов, студент 3 курса; С.А. Пахандрин, студент 3 курса; Д.С. Иванов, студент 3 курса

В. П. Бондаренко, д.т.н., профессор каф. КИБЭВС

ТУСУР, г. Томск, amir@sibmail.com

XX в. отметился широким развитием компьютерных технологий. В настоящее время различная компьютерная техника широко используется во всех сферах общества. Не стала исключением и медицина. Внедрение высокотехнологичных устройств в медицинскую практику позволило проводить такие операции, о которых мы раньше не могли даже представить. Но даже при современном развитии медицины проблема онкологических заболеваний все еще остается нерешенной. Наиболее часто используются хирургические методы. Однако даже после успешной операции остается вопрос о реабилитации пациентов для нормальной жизни.

В процессе сотрудничества кафедры и сотрудников НИИ онкологии разработана методика создания пищеводного голоса у пациентов, перенесших операцию по удалению гортани (ларинготомию). Методика основана на использовании принципа биологической обратной связи (БОС). БОС метод позволяет человеку управлять своим состоянием,

используя внешнюю обратную связь. В этом случае человек получает возможность в буквальном смысле видеть и слышать свои физиологические параметры: активность мозга, состояние мышц, температура, давление и изменять их. Практическое же применение данной методики ограничено в связи с отсутствием подходящих инструментов для визуализации этих параметров и обеспечения обратной связи. Создание новейших аппаратных устройств и их внедрение связано с большими трудностями. Необходимо специальное оборудование и комплектующие, стоимость которых может превышать возможности обычной государственной больницы. Поэтому использования в качестве аппаратной платформы обычного персонального компьютера может быть более предпочтительным. Тогда возникает вопрос о разработке специализированного программного обеспечения.

В нашей работе поставлена задача, разработать программную систему для персонального компьютера, способную реализовать описанную методику. Планируется создать программный комплекс, в возможности которого входит не только организация БОС с пациентом, но и анализ результатов тренировок по созданию пищеводного голоса и представления их в удобном графическом виде лечащим врачам. Процесс реабилитации состоит из множества фаз. На каждой производятся некоторые действия, имеющие цель – получение некоторого результата. Процесс реабилитации заканчивается на достижении глобальной цели – освоением пациентом пищеводного голоса. При автоматизации такого длительного процесса следует начать с электронного документооборота по учету результатов реабилитации. Эта задача очень важна, так как исследования в области речевой реабилитации сдерживаются, прежде всего, отсутствием упорядоченной базы данных по разнообразным параметрам реабилитационных мероприятий. Выработка новых методик и оценок невозможна без накопления статистики, на основании которой можно вырабатывать оптимальные траектории тренировок, давать оценки эффективности реабилитационных мероприятий. Поэтому обязательным пунктом в системе автоматизированного управления процессом реабилитации, является создание базы данных пациентов.

Вторая важная деталь проекта – это метод анализа речевого сигнала. В настоящее время традиционным способом анализа является преобразование Фурье. Другие алгоритмы, которые рассматривались для разработки – метод вейвлет-анализа, анализ при помощи гребенки полосовых нерекурсивных цифровых фильтров и при помощи гребенки полосовых рекурсивных цифровых фильтров. Наиболее подходящим по временным затратам, требованиям к производительности и

точности был выбран метод анализа с помощью гребенки полосовых рекурсивных цифровых фильтров.

Третья часть проекта – это реализация БОС. От того, насколько успешно система взаимодействует с пациентом, будет зависеть успешность применения методики в целом. При создании пищеводного голоса самой важной особенностью системы является то, что функция, которая требует тренировки, не существует после операции. Поэтому задача логопеда состоит в том, чтобы дать пациенту начальные навыки в использовании пищевода в качестве голосового аппарата. Далее тренировка этих навыков будет проходить с помощью разрабатываемой программной среды. В процессе тренировки данные обрабатываются, сравниваются с эталоном и предыдущими результатами. При появлении улучшений система фиксирует это и сигнализирует пациенту, подкрепляя его действия. Таким образом осуществляется положительная обратная связь с пациентом. Кроме положительной обратной связи вводится отрицательная обратная связь. Отрицательная обратная связь вычитает прошлый достигнутый результат из текущего, уменьшая сигнал подкрепления. Это необходимо для стимулирования дальнейшей тренировки.

В заключение хочется отметить, что немаловажной частью системы является интерфейс взаимодействия программы и пользователя. Необходимо учитывать не только возможную неподготовленность больного к работе с персональным компьютером, но и послеоперационное моральное состояние пациентов. Для этого интерфейс программы должен быть наиболее понятен и дружественен.

ЛИТЕРАТУРА

1. *Корнилов А.Ю.* Управление процессом речевой реабилитации на основе биологической обратной связи, диссертация, 2005. 128 с.

СИСТЕМА ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ГОЛОСУ

Д.А. Неустроев, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 8-913-849-21-88, e-mail nda@ms.tusur.ru

Биометрия – это методы автоматической идентификации человека и подтверждения личности человека, основанные на физиологических или поведенческих характеристиках. Биометрия – уникальная, измеримая характеристика человека для автоматической идентификации или верификации. Термин «автоматически» означает, что биометрические технологии должны распознавать или верифицировать человека

быстро и автоматически, в режиме реального времени. Идентификация с помощью биометрических технологий предполагает сравнение ранее внесенного биометрического образца с вновь поступившими биометрическими данными.

Идентификация и аутентификация

В биометрии делается различие между терминами идентификация и аутентификация. Если говорить об идентификации, то система пытается найти, кому принадлежит данный образец, сравнивая образец с базой данных для того, чтобы найти совпадение (также этот процесс называют сравнение «одного ко многим»).

Аутентификация – это сравнение, при котором биометрическая система пытается верифицировать личность человека. В этом случае, новый биометрический образец сравнивается с ранее сохраненным образцом. Сравнивая эти два образца, система подтверждает, что этот человек действительно тот, за кого он себя выдает. В процессе идентификации система сравнивает один образец со многими, тогда как процесс аутентификации сравнивает один с одним.

В последнее время системы идентификации голоса вызывают все больший интерес во всем мире. Это объясняется, во-первых, естественностью, привычностью речевого канала общения, а, во-вторых, тем, что производительность ЭВМ позволяет решать задачи этого класса.

Идентификация по голосу использует акустические особенности речи, которые различны и в какой-то мере уникальны. Эти акустические образцы отражают как анатомию (например, размер и форму горла и рта), а также приобретенные привычки (громкость голоса, манера разговора). Преобразование этих образцов в голосовые модели (также называемые отпечатками голоса) наделило данный способ идентификации названием «поведенческая биометрия». Биометрическая технология разбивает каждое произнесенное слово на несколько сегментов. Этот голосовой отпечаток хранится как некий математический код. Для успешной идентификации человека просят ответить на три вопроса, ответы на которые легко запомнить. Например: фамилия, имя, отчество; дата рождения. Некоторые современные системы создают модель голоса и могут сопоставлять ее с любой фразой, произнесенной человеком.

В настоящий момент самый распространенный метод аутентификации пользователя является пароль. Идентификация личности по голосу хорошо вписывается в существующую технологию доступа с помощью пароля, как дополнительное средство защиты, так и самостоятельное.

В последнее время для анализа речевого сигнала наиболее часто используется метод линейного предсказания. Линейное предсказание является одним из наиболее эффективных методов анализа речевого сигнала. Этот метод становится доминирующим при оценке основных параметров речевого сигнала, таких, как, например, период основного тона, форманты, спектр, функция площади речевого сигнала. Важность такого метода обусловлено высокой точностью получаемых оценок и относительной простотой вычисления. Основной принцип метода линейного предсказания состоит в том, что текущий отсчет речевого сигнала можно аппроксимировать линейной комбинацией предшествующих отсчетов. Преимущество в том, что он способствует быстрому и точному выполнению необходимых расчетов. Для характеристики индивидуальности голоса применяются коэффициенты линейного предсказания. Коэффициенты предсказания – это весовые коэффициенты, используемые в линейной комбинации.

В основу кодирования с линейным предсказанием (КЛП) положена идея в том, что любое значение речевого сигнала может быть представлено как линейная комбинация p предыдущих отсчетов. Основание для такого предположения дает та избыточность, которая неминуемо присутствует в речевом сигнале.

Существует много методов определения коэффициентов предсказания. Один из многих основан на минимизации среднеквадратичной ошибки предсказания на некотором коротком отрезке речи.

Метод КЛП может быть использован для представления различных свойств речевого сигнала, в том числе и для автоматического распознавания дикторов. Так, например сравнение спектра, полученного с помощью, так называемого, кепстрального анализа речевого отрезка, со спектром, определенным с помощью коэффициентов предсказания, показал их большое сходство. При этом для точного представления спектра достаточным оказалось определение $p = 12$ коэффициентов. Было показано, что для $p = 12$ ошибка предсказания минимальна.

Алгоритмы поиска пиковых значений для оценки формантных частот убедили, что корни полинома предсказателя хорошо соответствуют формантным частотам.

Коэффициенты линейного предсказания могут быть преобразованы в ряд других представлений речевого сигнала, например, в кепстральное представление, заключающее в измерении компонентов логарифмического спектра. С помощью коэффициентов предсказания можно рассчитать ряд представление таких как импульсная характеристика, автокорреляционная функция, функция площадей поперечного сечения в неоднородной акустической трубе без потерь и кепстр. Все

параметры дают примерно одинаковую вероятность ошибки, однако точность кепстрального метода несколько выше, чем всех других.

В данный период реализована программа, содержащая в себе, необходимые процедуры и методы для обработки сигнала, то есть быстрое преобразование Фурье и нормализация голоса.

Для полной работы данной программы необходимо усреднять речевые отрезки по результатам записи нескольких произношений. Результаты записи можно хранить в полном объеме или сжимать эффективными алгоритмами, которые позволяют сохранять индивидуальные параметры голоса без искажения (метод линейного предсказания).

Некоторые системы не удаляют из ключевой фразы слабовыраженные речевые участки (паузы, шумы). Данная работа будет удалять слабовыраженные речевые участки путем ее деления на отрезки, соответствующие фонемам базового языка, из которых затем выделяется совокупность требуемых параметров.

Основным достоинством описанной работы является простота построения. Широкие возможности их реализации на основе стандартных процедур цифровой обработки сигнала (ЦОС) и невысокие требования к вычислительным ресурсам.

ЛИТЕРАТУРА

1. *Рамишвили Г.С.* Автоматическое опознавание говорящего по голосу. М.: Радио и связь, 1981. 224 с.
2. *Рабинер Л.Р. Гоулд Б.* Теория и применение цифровой обработки сигналов: Пер. с англ. М.: Мир, 1978. 848 с.
3. *Маркел Дж., Грей А.Х.* Линейное предсказание речи / Пер. с англ. М.: Связь, 1980.
4. *Марпл.-мл. С.Л.* Цифровой спектральный анализ и его приложения: Пер. с англ. М.: Мир, 1990. 584 с.

.

СИСТЕМА УПРАВЛЕНИЯ ВЕРСИЯМИ

Д.Д. Нигматуллин, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, rob_in_zone@sibmail.com

В случае работы с SVN связь с репозиторием строится способом копирование-изменение-слияние. Т.е. оба пользователя при редактировании одного и того же файла могут вести работу одновременно. При этом пользователь Салли сделала свои правки первой, и опубликовала их на сервере. После того как пользователь Гарри внес в копию свои изменения, он делает попытку публикации правки в репозиторий, и если его исправления файла не перекрывают исправления, сделан-

ные Салли, то SVN автоматически производит слияние обеих правок. В результате в репозитории хранятся изменения обоих пользователей.

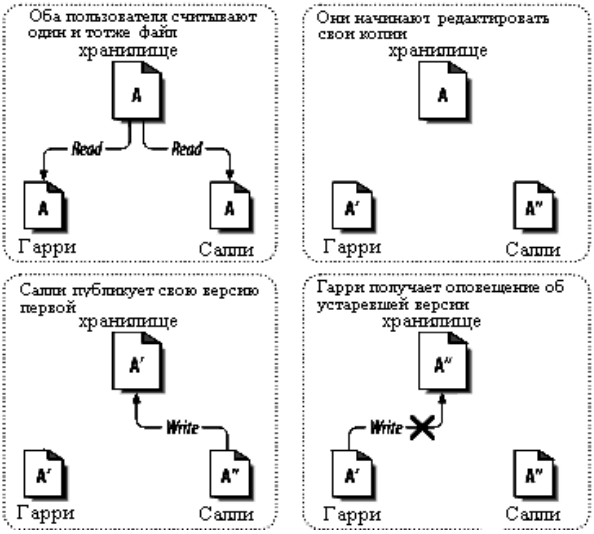


Рис. 1

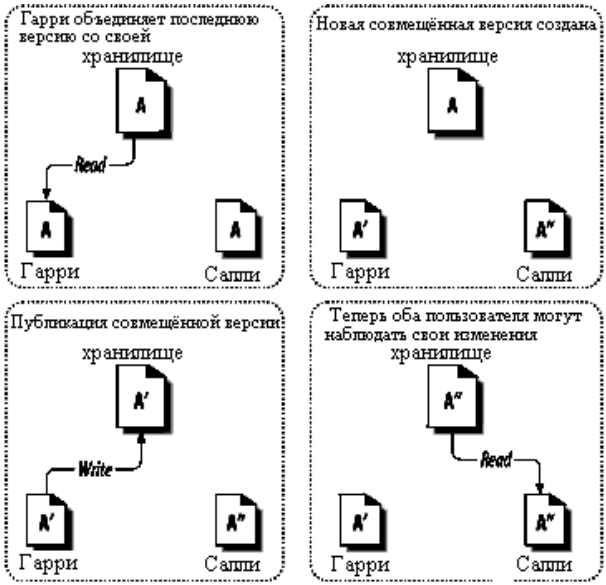


Рис. 2

Если же редактирования Гарри, перекрываются с исправлениями, сделанными Салли, то SVN сообщает о том, что версия файла Гарри устарела. После чего он делает обновление файла и смотрит на те изменения, которые внесла Салли. Затем самостоятельно производит слияние обеих корректировок и публикует окончательную версию в репозиторий [1] (рис. 1).

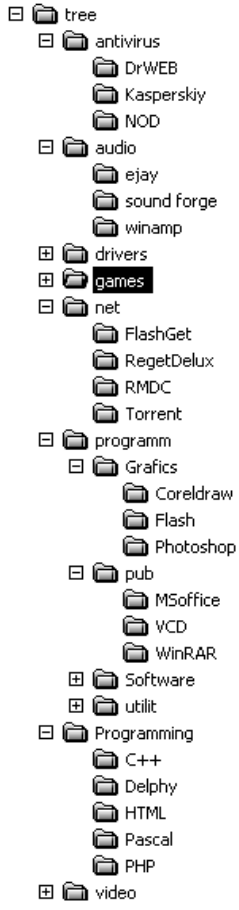


Рис. 3

В репозитории (хранилище файлов) создается дерево программ. Определение структуры берется исходя из интуитивно понятному любому пользователю набору программного обеспечения. На рис. 2. представлен некоторый возможный состав репозитария. Как пример: в каталоге «audio» представлены продукты, предназначенные для воспроизведения аудиофайлов.

Основой всей системы является файл-конфигуратор *.swc (SVN Windows Configurator). Данный файл является простым текстовым файлом, но содержит всю информацию, необходимую для обновления программы до ее последнего выпуска.

В создании дерева и файлов-конфигураторов может принимать как администратор дерева SVN, так и обычный пользователь, имеющий права на изменение данных на сервере (рис. 3).

Начальные шаги для клиента: создание списка установленного программного обеспечения. Возможно применение бесплатной версии программы EVEREST, которая имеет функцию экспорта в текстовый файл в автоматическом режиме информацию о текущем состоянии установленного программного обеспечения. Данная информация сохраняется в базу данных, которая в дальнейшем будет использоваться для процесса обновления [2].

После этого клиент соединяется с сервером SVN, и копирует на свою машину дерево программ. Клиентская программа указывает на те программные продукты, которые имеют возможность для обновления.

Процесса обновления состоит из следующих шагов:

1. Считывание версии установленного ПО и поиск файла *.swc более новой версии.

2. Считывание информации из *.swc и выполнение процесса обновления по алгоритму, записанному в этом файле.

3. Обновление базы установленных программ.

ЛИТЕРАТУРА

1. *Бен Коллинз, Сассман Брайан У. Фитцпатрик.* svn(Управление версиями в Subversion)
2. http://www.lavalys.com/

ПОДХОД К ПРОЕКТИРОВАНИЮ КОНСТРУКЦИИ ПЛАНШЕТНОГО ГРАФОПОСТРОИТЕЛЯ

В.В. Онищук, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, wowchic@mail2000.ru

Планшетный графопостроитель – устройство предназначено для применения в учебном процессе для демонстрации и вывода графических изображений во взаимодействии с персональным ЭВМ.

Как и к любому техническому устройству к графопостроителю предъявляются определенные требования к конструкции. Среди требований целесообразно выделить только наиболее актуальные:

– обеспечение быстрой замены неисправных узлов и деталей, удобный доступ ко всем частям, приборам ЭС;

– максимальное использование унифицированных блоков и узлов;

– минимально возможные затраты времени, труда и материалов, средств на разработку, изготовление и эксплуатацию электронного средства.

Для выполнения быстрой замены и удобного доступа ко всем частям устройства, требуется предварительный анализ работ, которые будут проводится над прибором.

Удобный доступ ко всем частям устройства, обеспечивается грамотным расположением разъемов и соединительных проводов внутри корпуса, а также достаточной длинной проводов между частями устройства.

В основе проектирования необходимо взять за основу структуру геометрических и кинематических связей графопостроителя и используя метод моноконструкций, который предполагает минимизацию числа связей между функциональными узлами на основе несущего каркаса. Исходя из метода, необходимо обозначить все свободные объемы графопостроителя и оптимально разместить все проектируемые узлы. Также следует рассматривать минимизацию числа связей с

четом удобного доступа ко всем узлам, что обеспечивает не только эффективность конструкции, но и ее ремонтопригодность.

В результате проектирования необходимо получить конструкцию хорошую не только как конструктив, но хорошую с точки зрения качества для потребителя. Как конструкция графопостроитель обладает всеми необходимыми средствами для демонстрации в учебном процессе, а также для наглядного представления работы микроконтроллера с памятью, с внешними устройствами, обмена информацией и многое другое. Поэтому для потребителя, а это студенты, качество прибора будет определятся, несколько иными параметрами. А это прежде всего наглядность и простота исполнения всех модулей, прозрачность работы всех устройств и функциональных блоков. Поэтому при разработке конструкции следует опираться на качество.

Критериями оценки качества являются:

– функциональные возможности изделия;
– рабочие характеристики (быстродействие, мощность и т.п.);
– работоспособность;
– долговечность (работа без поломок);
– обслуживаемость (время до ремонта);
– эстетика (цвет, мода, удобства, форма и пр.).

Исходя из этих критериев, и следует разрабатывать конструкцию устройства.

ЛИТЕРАТУРА

1. *Бродин В.Б., Калинин А.В.* Системы на микроконтроллерах и БИС программируемой логики. М.: Издательство ЭКОМ, 2002. 400с.
2. *Сташин В.В., Урусов А.В., Мологонцева О.Ф.* Проектирование цифровых устройств на однокристальных микроконтроллерах. М.: Энергоатомиздат, 1990. 224с.

АНАЛИЗ И ВЫБОР ПРОГРАМНОГО ОБЕСПЕЧЕНИЯ ВЕРХНЕГО УРОВНЯ ПЛАНШЕТНОГО ГРАФОПОСТРОИТЕЛЯ

В.В. Онищук, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, wowchic@mail2000.ru

Для связи с персональным ЭВМ, планшетный графопостроитель использует распространенный интерфейс RS-232. При выводе информации из персонального ЭВМ сразу возникает вопрос, каким образом переносить информацию с экрана на бумагу. Так как графопостроитель выводит информацию последовательно, т.е. перемещая каретку пишущего узла по рабочему пространству. То есть область применения графопостроителя лежит в выводе графических материалов, таких

как графики, схемы и другое. Соответственно для выполнения возложенных на устройство функции, необходимо создавать определенный протокол обмена между графопостроителем и персональным ЭВМ, в который будет закладываться механизм отработки данных в графопостроителе.

Для точного вывода графических материалов на твердые носители, исходное изображение, необходимо обработать и привести к печатному виду. Решатся данная задача может либо на нижнем уровне – уровне микроконтроллера, либо на верхнем – на уровне персонального ЭВМ. Но поскольку подобная программа должна выполнять сложные функции: интерполирование и преобразование координат, то целесообразней не обременять микроконтроллер такими задачами и отвести ему задачу управления всеми объектами.

Вследствие этого для решения задач обработки информации можно выделит гораздо большие ресурсы и создать программу, которая позволит любое изображение, будь-то график или схема, интерактивно с пользователем и в соответствии с его желаниями получить конечный продукт в короткое время и без особых усилий.

Протокол передачи от ПЭВМ к графопостроителю, будет простым, так как для управления кареткой графопостроителя необходимо всего несколько команд: влево, вправо, вниз, вверх, поднять, опустить перо и несколько управляющих сигналов, конец, начало данных, перейти в начало координат, взять карандаш и др. Однако исходное изображение может быть очень расплывчатым и не точным, но благодаря возможностям программы, рисунок будет обработать, а после корректировки пользователем изображение будет декодироваться и передаваться в графопостроитель. Который будет решать свою задачу: быстрой прорисовке полученных данных.

ЛИТЕРАТУРА

1. Архангельский А.Я. Программирование в Delphi 7. М.: «Бином-Пресс», 2005 1152 с.

КОМПЬЮТЕРНАЯ СУДЕБНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА. СУЩЕСТВУЮЩИЕ АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ЕЕ ПРОВЕДЕНИЯ

М.В. Петруй, студент 5 курса,
И.В. Давыдов, аспирант каф. КИБЭВС
ТУСУР, г. Томск, т. 8-913-806-69-27, e-mail gomozila@sibmail.com

Компьютерная судебно-техническая экспертиза

Расследование и раскрытие неправомерного доступа к компьютерной информации, когда средства компьютерной техники использу-

ются для подготовки, совершения или сокрытия рассматриваемого правонарушения, невозможно без привлечения специальных познаний в области современных информационных технологий.

Основной формой использования специальных познаний является компьютерно-техническая экспертиза.

Видовую классификацию компьютерно-технических экспертиз целесообразно организовать на основе обеспечивающего предназначения компьютерных средств (аппаратных (технических), программных, информационных) и использовать ее в виде, соответствующем процессам разработки и эксплуатации любых компьютерных систем. Поэтому можно выделить: аппаратно-техническую и программно-техническую экспертизу (данных). Кроме того, достаточно оправданным представляется выделение еще одного вида компьютерно-технической экспертизы – компьютерно-сетевой экспертизы для исследования фактов и обстоятельств, связанных с использованием сетевых и телекоммуникационных технологий.

Поскольку в системе судебно-экспертных учреждений нет специальных экспертных подразделений по производству таких экспертиз, они могут быть поручены специалистам соответствующей квалификации из внеэкспертных заведений.

Экспертное (Forensic) исследование компьютерных систем обычно выполняется обученными специалистами с использованием специализированного оборудования и программного обеспечения. Популярность операционных систем Windows как на рабочих станциях, так и на серверах, является главным фактором необходимости таких исследований. В результате, диапазон инструментов, которые можно использовать для анализа платформ Windows, непрерывно растет. Однако, истинное экспертное исследование компьютера (то, в котором может потребоваться собрать доказательства для суда) ограничивается не только рамками технологий, но и рамками законодательства, а иногда и находится под всевидящим оком прессы.

Успех в компьютерной экспертизе зависит не только от возможности сбора доказательств с компьютерной системы, но также от возможности придерживаться правильной методологии в процессе сбора доказательств и их обработки так, чтобы эти доказательства могли быть использованы в суде.

Многие исследования дискредитируются людьми, использующими саму подозреваемую систему для поиска улик. Хорошим примером этого является исследователь, использующий встроенные Windows инструменты на исследуемой машине для поиска и открытия файлов. Эти действия могут уничтожить данные, имеющие доказательное значение, одновременно делая так, что вскрытые улики не смогут быть использованы в суде.

Первый шаг в экспертном исследовании жесткого диска компьютера почти всегда состоит в снятии «побитовой» копии, или образа (image), содержащего каждый бит информации, независимо от того, является ли тот частью файловой системы.

После того, как образ создан, как нам узнать, что все сделано корректно? Как мы можем удостовериться, что копия в точности соответствует оригиналу? Ответ содержится в использовании алгоритма MD5. Эта процедура дает число, называемое «дайджест сообщения», значение которого определяется расположением данных на диске.

После того, как образ создан, можно начинать поиск улик. Некоторые коммерческие инструменты для работы с образами, кроме возможностей по созданию копий дисков, также предоставляют возможности для анализа образов

Использование шифрования обеспечивает другой тип затруднений для компьютерных экспертов. В данном случае, восстановление данных – только половина пути, задача дешифровки представляет потенциально более высокое препятствие. Шифрование, встроенное в приложение или обеспеченное отдельным программным продуктом, бывает различных видов и силы.

Сейчас перед юристами и экспертами по информационной безопасности стоят многие проблемы, затрудняющие производство таких экспертных исследований и использование их результатов в гражданском и уголовном процессе.

В целом при назначении технико-криминалистической экспертизы компьютерных систем следователям приходится решать следующие наиболее существенные проблемы:

– Отсутствие в штате экспертных подразделений правоохранительных органов и Министерства юстиции достаточно квалифицированных специалистов в области компьютерной информации.

– Недостаточная подготовка в области компьютерной техники, не позволяющая правильно сформулировать вопросы для эксперта (особенно по общеуголовным составам). Постановка перед экспертами вопросов, выходящих за рамки их компетенции.

– Трудности в интерпретации результатов экспертизы.

В учреждениях, обеспеченных финансированием, эксперты могут использовать специализированное программное обеспечение. В ряде стран Западной Европы и США разработаны программы, предназначенные специально для производства экспертизы компьютерной техники.

Существующие автоматизированные системы проведения экспертиз

Судебно-экспертный комплекс EnCase. Один из мировых лидеров в области разработки программного обеспечения и программных средств, организации профессионального обучения специалистов для

сферы судебно-экспертного исследования компьютерных систем является компания Guidance Software.

Разработанная компанией технология EnCase представляет собой комплекс инструментальных методов и средств обеспечения всех стадий экспертного исследования компьютерных систем – от предварительного просмотра компьютерной информации до составления заключения эксперта как источника доказательств.

Инструментальные экспертные средства Vogon International. В настоящее время частое применение в зарубежной следственной практике находят инструментальные средства Vogon International. Использование данного комплекса, как свидетельствуют специалисты правоохранительной сферы, имеет особую эффективность при раскрытии и расследовании таких преступлений, как мошенничество, Internet/e-mail – злоупотребления, убийство, терроризм и пр. Наибольшее распространение средства Vogon International получили в Великобритании и ряде стран Европы, Северной Америки и Дальнего Востока.

Особенностью технологии Vogon International является обеспечение проведения судебно-экспертного исследования на высоком технологическом уровне посредством использования аппаратных компьютерных средств, и мощных инструментов программного обеспечения.

Экспертная система ILOOK Investigator. Данная система (разработка Elliot Spencer & the Criminal Investigation Division of the United States Internal Revenue Service, U.S. Treasury Department) служит задачам обеспечения производства судебной экспертизы в сфере современных информационных технологий. Программный комплекс ILOOK является экспертным инструментом, предназначенным для всестороннего исследования и анализа представленной на экспертизу компьютерной системы. ILOOK функционирует в среде на следующих 32-битных системах: WinNT или Win2K.

ILOOK используется как для экспертизы целой компьютерной системы посредством создания побитной копии (образа) носителя информации, так и исследования отдельных файлов различных типов.

AccessData Forensic Toolkit. Наблюдаемый рост числа компьютерных преступлений требует от судебных экспертов и специалистов в области компьютерной безопасности применения новейших технологий для противодействия киберпреступности. Forensic Toolkit – новейший инструмент для судебных экспертов, занимающихся производством компьютерно-технических экспертиз. В данный продукт фирма разработчик (AccessData) вложила свой опыт за период более 30 лет в области восстановления паролей и дешифрования файлов.

ЛИТЕРАТУРА

1. *Усов А.И.* «Основы методического обеспечения судебно-экспертного исследования компьютерных средств и систем» – М.: Право и закон, 2002
2. http://skte.narod.ru/ – сайт, посвященный компьютерно-технической экспертизе.
3. http://www.vogon-international.com/ – сайт компании «Vogon International»
4. http://www.ilook-forensics.org/ – сайт продукта ILOOK investigator
5. http://www.guidancesoftware.com/ – сайт компании «Guidance Software»
6. http://www.encase.com/products/ee_index.asp – сайт компании «EnCase»
7. http://www.accessdata.com/products – сайт компании «AccessData»

ДОБАВЛЕНИЕ ПРОИЗВОЛЬНЫХ ТИПОВ АВТОРИЗАЦИИ В ПРИЛОЖЕНИЯХ WINDOWS

Р.А. Белик, А.В. Забелин, М.В. Савчук, М.А. Шабаловский,
студенты 4 курса каф. КИБЭВС
ТУСУР, гр.522, г. Томск, mehos1@yandex.ru

В настоящее время существует большое количество различных механизмов авторизации. Среди них можно выделить классическую парольную защиту, идентификация пользователей по смарт-картам, по биометрическим характеристикам, электронным ключам и т.д. Однако при проектировании программного обеспечения разработчик руководствуется только своими собственными представлениями о том, как обеспечивать защиту от несанкционированного доступа.

Можно выделить как минимум три слабых стороны такого подхода:

- Механизмы авторизации не стандартизированы, что не позволяет говорить об их гарантированной высокой надежности.
- Программный код, реализующий указанные механизмы не отделен от основного кода программы, что увеличивает размер исполняемого файла и препятствует их независимому обновлению.
- Такой подход не обеспечивает необходимой гибкости. Для добавления дополнительных механизмов в программное обеспечение (например, возможности запуска данной программы только в определенный интервал времени) необходимо связываться с его разработчиками.

Таким образом, разработчик вынужден уделять значительное количество времени добавлению функционала, не связанного с непосредственной предметной областью, для работы с которой предназначается разрабатываемый продукт.

В некоторой степени данные проблемы решаются средствами операционной системы. Однако в основном действия сводятся либо к запрещению, либо к разрешению запуска программы для конкретного пользователя или групп пользователей.

Для операционной системы Linux разработан механизм, названный PAM (Pluggable Authentication Modules). Он позволяет использовать различные модули авторизации от независимых разработчиков, причем их состав и качество определяется администратором системы. В пользу такого подхода можно привести то, что многие ведущие разработчики программного обеспечения используют PAM.

Однако для операционной системе Windows до сих пор не существует подобного механизма. Таким образом, целью данной работы является разработка системной библиотеки, позволяющей с легкостью внедрять модули авторизации в различные приложения на этапе их разработки. В операционной системе Windows последних версий имеется развитый механизм назначения прав, согласно т.н. спискам доступа, но это не обеспечивает требуемого уровня гибкости и защищенности для приложений.

Можно выделить некоторые критерии, которым должна удовлетворять разрабатываемая система:

- Библиотека должна представлять собой автономный объект системы, следовательно, необходимо использовать механизм динамически связываемых библиотек (DLL).
- Должен существовать удобный и универсальный механизм подключения новых модулей. Проектированию интерфейса взаимодействия библиотеки со сторонними модулями необходимо уделить наибольшее внимание.
- Необходимо обеспечить удобный способ использования библиотеки разработчиками программного обеспечения. Для этого следует написать соответствующие заголовочные файлы на нескольких популярных языках программирования.

Следует обеспечить разработчиков программного обеспечения и соответствующих модулей исчерпывающей документацией.

Для демонстрации и расширения возможностей библиотеки планируется написание нескольких модулей:

- Модуль авторизации при помощи HASP ключей.
- Авторизация на основе SQL сервера.
- Авторизация при помощи сменных носителей: гибких, flash, компакт– дисков,

Кроме того, планируется разработать продукт, заменяющий стандартное окно авторизации в Windows. Это позволит расширить возможности управления доступом пользователей.

Таким образом, разрабатываемая библиотека позволит значительно повысить надежность программного обеспечения, наделить его гибкими возможностями, позволяющими снизить вероятность несанкционированного доступа.

ЛИТЕРАТУРА

1. *Ивлев С.Ю.,* Как работает PAM. http://www.opennet.ru/base/net/pam_linux.txt.html
2. *Linux Pam Group*. http://cygwin.dp.ua/pub/linux/libs/pam/index.html
3. *Страуструп Б.* Дизайн и эволюция C++. П: Питер, 2006. 534 с.
4. *Басс Л.*, *Клементс П.*, *Кацман Р.* Архитектура программного обеспечения на практике. П: Питер, 2003. 448 с.

LDAP СЛУЖБА КАТАЛОГА НА БАЗЕ ОС FREEBSD 6.0

А.В. Симаков, студент гр. 521-1 каф. КИБЭВС
ТУСУР, г. Томск, т. 8-960-975-19-82, e-mail andrake@mail.ru

CCITT (Consultative Committee for International Telegraphy and Telephony) разработал серию рекомендаций для создания так называемого сервиса Директории или Каталога. Каталог является сервером или распределенным набором серверов, которые поддерживают распределенную базу данных, содержащую информации о различных субъектах, таких как пользователи, устройства и т.п. Эта распределенная база данных называется Информационной Базой Каталога (Directory Information Base – DIB). Информация включает имя субъекта, а также различные атрибуты, характеризующие этот субъект. Данные рекомендации носят название стандарта X.500. Первоначально LDAP начал развиваться как программный продукт переднего плана (front end) для Каталога X.500.

LDAP предоставляет большинство возможностей X.500 при существенно меньшей стоимости реализации. Например, удалены избыточные и редко используемые операции. LDAP, в отличие от X.500, использует стек TCP, а не OSI.

Следует заметить, что базовые операции протокола могут быть отображены на подмножество сервисов Каталога X.500. Однако не существует отображения один-к-одному между операциями протокола LDAP и операциями протокола DAP (Directory Access Protocol) стандарта X.500.

Первая реализация LDAP написана в Мичиганском университете. Большинство ранних реализаций LDAP основано на ней.

Что такое LDAP?

LDAP (Lightweight Directory Access Protocol) – это протокол, который используется для доступа к информации, хранящейся на распределенных в сети серверах.

Эта информация представляет собой данные, хранящиеся в атрибутах. При этом предполагается, что такие данные чаще читаются, чем модифицируются. LDAP основан на клиент-серверной модели взаимодействия.

Общая модель данного протокола состоит в том, что клиент выполняет операции протокола на серверах. Клиент передает запрос, описывающий операцию, которая должна быть выполнена сервером. Сервер выполняет необходимые операции в Каталоге. После завершения операции (операций) сервер возвращает клиенту ответ, содержащий результаты или ошибки.

Заметим, что хотя требуется, чтобы серверы возвращали ответы всякий раз, когда такие ответы определены в протоколе, не существует требования синхронного поведения клиентов или серверов. Запросы и ответы для нескольких операций могут пересылаться между клиентом и сервером в любом порядке, однако клиенты должны получить ответ на каждый свой запрос.

Информация на сервере LDAP представляет собой совокупность записей, которые содержат набор атрибутов и сгруппированы в древовидную иерархическую структуру.

Запись идентифицируется глобально уникальным именем (Distinguished Name – DN) – подобно имени домена в структуре DNS.

Каталог является специализированной базой данных, которая может использоваться в повседневной жизни – телефонная книга, программа передач и т.п. Предполагается, что данные Каталога достаточно статичны. Классическим примером подобной специализированной базы данных является сервис DNS.

Преимущества LDAP

Основные причины роста популярности LDAP связаны с тем, что:

LDAP имеет стандартную схему хранения информации в отличие от реляционных баз данных, когда в каждом случае определяется своя схема хранения в терминах таблиц и столбцов. Поэтому в LDAP нет специфичного для каждого Каталога и для каждого приложения управления – нет так называемой «проблемы N+1 Каталога». Для всех серверов LDAP используется единая схема хранения, единый способ именования хранимых объектов и единый протокол доступа.

LDAP позволяет быстро отыскивать необходимые данные, поскольку ориентирован в большей степени на чтение и поиск информации, чем на модификацию.

LDAP не обязательно должен быть ограничен конкретным сервером, есть возможность организовывать распределенные системы из нескольких серверов. В LDAP предусмотрена возможность создавать ссылки между различными серверами LDAP, что обеспечивает возможность поиска сразу на нескольких серверах LDAP.

Как протокол LDAP, так и структура Каталога LDAP организованы в соответствии со стандартами, в результате чего можно единообразно использовать реализации LDAP различных производителей.

Еще одно важное назначение LDAP – хранение всей информации, относящейся к PKI, а именно сертификатов, CRL и т.п.

При сравнении такого способа хранения информации с базами данных LDAP превосходит второй способ по большинству пунктов.

Принципы развертывания серверов LDAP

– При развертывании серверов LDAP необходимо выполнить следующие задачи:

– решить, что должно храниться в Каталоге. Необходимо четко понимать, какие приложения будут работать с данными.

– определить структуру данных в Каталоге и установить их взаимосвязи.

– разработать схему Каталога с учетом требований приложений.

– определить пространство имен.

– определить топологию размещения серверов.

– определить требуемые репликации, гарантируя, что данные будут доступны везде, где они необходимы.

– определить оптимальный уровень безопасности с учетом конкретных требований безопасности.

Для того чтобы использовать механизм аутентификации GSSAPI что соответствует пятой версии Керберос, требуется набор библиотек SASL(Simple Authentication and Security Layer), который бы позволял передавать имя пользователя получившего билет из области(Realm) Керберос службе каталога, которая в свою очередь при помощи директивы файла конфигурации преобразовывала имя в уникальное имя дерева LDAP, осуществляла его поиск в дереве и в случае если такое имя существует, производила аутентификацию пользователя.

Для защиты сеанса связи, в частности целостности и конфиденциальности применяется протокол TLS 1.0 поддерживаемый набором библиотек OpenSSL.

В результате данной работы были получены практические навыки по настройке сервера LDAP с поддержкой аутентификации и защитой транспортного уровня. Получено представление о принципах работы популярных пакетов обеспечения информационной безопасности и о протоколе Lightweight Directory Access Protocol.

ЛИТЕРАТУРА

1. www.intuit.ru
2. www.citforum.ru
3. www.opennet.ru
4. www.openload.org

АНАЛИЗ ПОКАЗАТЕЛЕЙ СРЕДСТВ ВВОДА-ВЫВОДА НЕПРЕРЫВНЫХ СИГНАЛОВ УМК SDK 1.1/S

Р.С. Титов, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск

Учебный микропроцессорный комплекс SDK 1.1 предназначен для освоения студентами архитектуры и методов проектирования систем на базе микропроцессоров, однокристальных микроЭВМ, а также встраиваемых контроллеров и систем сбора данных.

В состав аппаратной части данного комплекса входят такие блоки, как: микроконтроллер ADuC842, внешняя E^2PROM память, клавиатура, жидкокристаллический индикатор, часы реального времени, набор сигнальных светодиодов, а также внешняя SRAM память. Интерфейс между CPU и внутренней периферией обеспечивается применением регистров специального назначения (sfr), которые включают в себя регистры управления и конфигурирования, регистры данных. Регистры располагаются во внутренней памяти данных по адресам 80h-FFh и доступны прямым методом адресации.

Объектом предлагаемого сообщения является анализ технических показателей устройств непрерывного ввода-вывода стенда SDK 1.1/S.

Основой УМК SDK 1.1/S является микроконтроллер ADuC842 фирмы Analog Device, в состав которого включены восьмиканальный 12-битный АЦП и два 12-битных ЦАПа. Кроме того, в состав микроконтроллера входит температурный сенсор, определяющий температуру микроконтроллера.

Работа АЦП полностью контролируется тремя регистрами специального назначения, формат которых представлен на рис. 1.

Регистр ADCCON1 управляет преобразованием, временем переключения, режимами работы АЦП и токопотреблением устройства. Регистр ADCCON2 допускает побитовую адресацию и управляет выбором номера одного из восьми каналов, либо преобразованием от температурного сенсора, а также режимами преобразования. Регистр ADCCON3 устанавливает индикацию занятости АЦП для прикладных

программ. После установки описанных регистров, АЦП сконфигурирован для преобразования данных с записью результата в два восьмиразрядных sfr-регистра старшего (ADCDATAH) и младшего (ADCDATAL) байта результата, формат которых приведен на рис. 2.

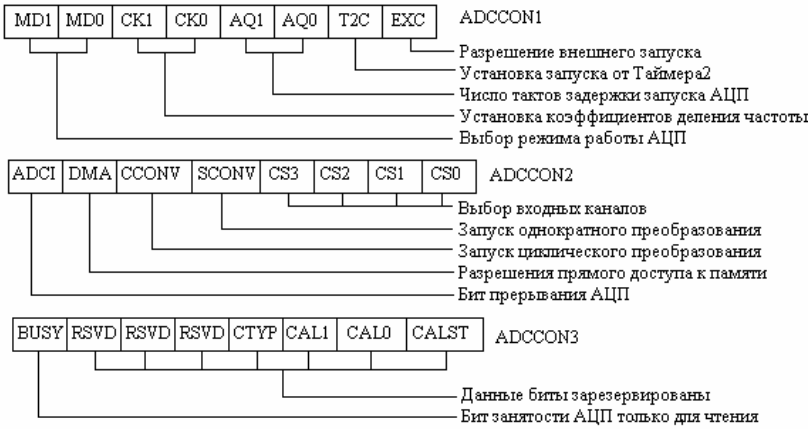


Рис. 1. Формат регистров установки АЦП

Как видно из рис. 2, четыре бита фиксируют код канала результата, а остальные 12 разрядов соответствуют результату преобразования: 4 и 8 бит слова состояния в старшем и младшем регистрах соответственно.

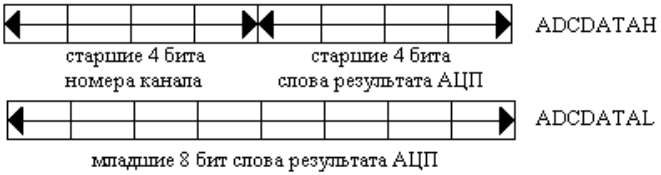


Рис. 2. Формат регистров результата

Работа обоих цифро-аналоговых преобразователей обеспечивается настройкой регистра специального назначения DACCON, формат которого представлен на рис. 3. Входными данными ЦАПа являются 4 старших и 8 младших байта, которые хранятся в регистрах DAC0H/DAC1H и DAC0L/DAC1L соответственно.

Для подключения входов/выходов контактов устройств непрерывного ввода/вывода преобразователей на стенде применен 20-контактный разъем J1, выведенный на лицевую панель стенд. Четные контакты выведены на корпус, нечетные представляют собой набор входов/выходов преобразователей.

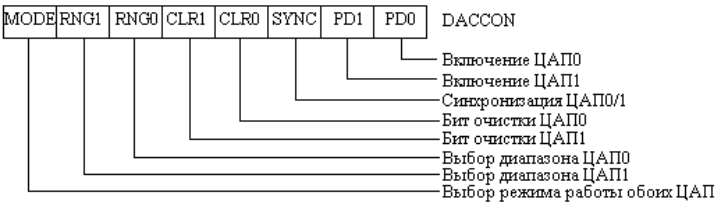


Рис. 3. Формат регистра DACCON

Работоспособность стенда проверяется переключателем SW1, который находится на панели стенда и предназначенный для аппаратного соединения соответствующих каналов преобразователей.

Для программирования стенда может использоваться ассемблер или С с трансляторами для ядра 8051 в HEX-формат.

Доставка образа в постоянную память стенда осуществляется с персонального компьютера через интерфейс RS232. Резидентный загрузчик HEX202 располагается во Flash – памяти контроллера начиная с адреса 0100h. Он обеспечивает начальную инициализацию системы, загрузку программ в HEX – формате в память SDK и передачу им управления. Начальная инициализация заключается в установке всех sfr-регистров их значениями по умолчанию. Терминалом для взаимодействия загрузчика HEX202 с персональным компьютером является программная инструментальная система T167B (DOS) и T2 (Windows).

Этапы программирования стенда на примере подключения устройств непрерывного ввода вывода.

1. Написание программы. Ниже представлен фрагмент программы на языке Assembler:

```
mov ADCCON1,#0ACh; ADCCON1: деление частоты на 4, 4 такта задержки при дежурном режиме без цикла преобразования
mov ADCCON2,#1000B; канал температурного сенсора
mov DACCON,#03DH; ЦАП0 в 12-битный режим с синхронизацией
setb SCONV; инициализация однократного АЦП преобразования
jnb ADCI,$; если бит установлен, то произошло преобразование; размещение результата АЦП в регистры ЦАПа
mov DAC0H,ADCDATAH; старшие байты
mov DAC0L,ADCDATAL; младшие байты
```

2. Трансляция и загрузка:

2.1. Транслятор «tasm.exe» для создания образа программы.

2.2. Инструментальная среда T2 (Windows)

2.3. Добавление стартового адреса в командной строке среды T2, по которому произойдет передача управления загруженной программе:

```
# 0x0000 0x0 addhexstart C:/primer.hex
```

2.4. Настройка COM-порта 1 на передачу со скоростью 9600 бит/с:
9600 openchannel com1
2.5. Загрузка образа программы: # loadhex C:/primer.hex
2.6. Выход из среды: # bye

После перезагрузки стенда управление перейдет к загруженной программе.

ЛИТЕРАТУРА

1. ООО «ЛМТ» 2001 г. Учебный стенд SDK Руководство пользователя.
2. http://lmt.cs.ifmo.ru.

ОСОБЕННОСТИ РАЗРАБОТКИ ОБУЧАЮЩИХ КУРСОВ ПО АССЕМБЛЕРУ ДЛЯ СТУДЕНТОВ СПЕЦИАЛЬНОСТЕЙ, СВЯЗАННЫХ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

С.Д. Тиунов, студент 1 курса; Г.В. Петрова, каф. КИБЭВС
ТУСУР, г. Томск, т.414-476, t5d@mail.ru

Предлагаемый курс ассемблера предназначен для студентов первого курса специальностей, связанных с информационной безопасностью. Обучение студентов непосредственно специальности целесообразно предварять изучением языка низкого уровня программирования. Этому есть несколько причин:

– Как правило, информационная безопасность основана на затруднении взлома системы. Это достигается за счет использования недокументированных функций системы, либо за счет использования оригинальной структуры программы. С помощью языков высокого уровня (ЯВУ) второй вариант практически нереализуем, а первый довольно ограничен сам по себе.

– Если изучать дисциплину с наиболее низкого уровня, то дальнейшее обучение становится проще. Другими словами ассемблер должен стать фундаментальным знанием студентов-программистов.

– Студент может быть заинтересован и в других областях программирования, например, в кодировании информации. После курса должно прийти понимание того, что для реализации таких задач как сжатие данных, например, проще всего пользоваться ассемблером.

Язык ассемблера неисчерпаем в любых более или менее разумных рамках, в том числе и в рамках этого курса. Будут изучены только основные возможности ассемблера:

– регистры;
– арифметика и логика;
– стек, процедуры (функции);

– память: прямая и косвенная адресация;

С учетом этого курс содержит достаточно полный набор основных, наиболее важных понятий программирования. Более того, любая программа курса не более 40 строк кода. На СИ, например, подобные программы, несложно разместить в 15 строках. Это сделано преднамеренно: незачем усложнять задачу, так как уже теоретический материал сложен для начинающих, как правило, знакомых с каким-либо ЯВУ. На решение простой задачи (с полным пониманием проделанного) студенту потребуется не менее получаса.

Курс рассчитан на 8 лабораторных работ. Главы распределены так, что теории становится все меньше, а требуемого кода все больше. Тем не менее, под эту концепцию не подходят последние главы, где пишутся довольно серьезные программы, которые сопровождаются не менее серьезной теорией и заданием. На выполнение этих заданий может потребоваться уже не полчаса, а до двух лабораторных работ. Это сделано еще и потому, что заключительные главы играют особую роль – они должны окончательно закрепить полученные знания. Другими словами – последние главы написаны по тому принципу, что гораздо быстрее прочитать и понять материал еще раз, чем искать его в других главах или вспоминать.

Для наиболее быстрого понимания сути лабораторных работ будут использоваться многочисленные примеры использования тех или иных операторов. Весьма вероятно, что для понятности примеры следует сделать полезными (например, поиск/сортировка), что делает их сложнее заданий лабораторной.

Несмотря на относительную сложность последних работ (глава 7 – параметры и оптимизация размера, глава 8 – разбор командной строки), для самостоятельного обучения не хватает некоторого материала. Например, интерфейс BIOS, DOS, приемы низкоуровневого программирования: примеры использования стека и динамического изменения тела программы и другие интересные темы, не затрагиваемые ни курсом, ни любым из последующих курсов ЯВУ. Учебный курс будет содержать эти главы в качестве дополнительных. По мере накопления знаний обучающегося, ему будут предлагаться те главы, которые он в состоянии (на данный момент) освоить, и соответственно, которые подходят по тематике к данной обязательной главе.

О среде выполнения. Большинство лабораторных работ обучающемуся придется выполнять с помощью программных средств тестирования и отладки программ. В этом бесспорный плюс изучения ассемблера: программа, такая непонятная на бумаге, выполняется в динамике, что позволяет понять работу тех или иных операций. Начиная с логической середины курса, студента знакомят с более быстрыми средствами разработки (компилятор + компоновщик), что, однако, не

уменьшает значение отладчика в его работе. Так последние главы содержат обширную теорию, и только овладев отладчиком, можно оперативно выполнять наиболее сложные задания курса. Предполагается также знакомство с такими инструментами как hex-редактор и дизассемблер.

В качестве формата исполняемых файлов используются наиболее простые com-файлы. Модель памяти, соответственно, tiny, что с одной стороны хорошо (наиболее оптимизирован, не нужно следить за сегментами), с другой – не очень, так как учащийся не узнает о других моделях памяти. Но, как уже говорилось, низкоуровневое программирование необъятно в рамках данного курса, впрочем, данный вопрос достаточно интересен для внесения его в дополнительную главу.

Предполагается, что обучение будет сопровождаться (и закрепляться) тестовыми заданиями, предлагаемыми к каждой лабораторной работе. По мере накопления теоретического материала будет увеличиваться и количество вопросов. Предполагается создать среду для тестовых заданий, которая и будет управлять процессом тестового контроля, то есть давать список случайных вопросов по данной теме (а также случайно – по ранее пройденным) и оценивать результат, записывая в log-файл. Скорее всего, вопросы лучше всего предлагать именно по материалам лабораторных работ, ведь только так можно достичь цели – оставить у студента стройное понятие об организации функциональных блоков компьютера.

ЛИТЕРАТУРА

1. *Абель П.* Язык ассемблера для IBM PC и программирования / Пер. с английского Ю.В. Сальникова. М.: Высш. шк., 1992. 447 с.
2. *Зубков С.В.* Ассемблер DOS, Windows и Unix. М.: ДМК, 1999. 640 с.

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К МОДИФИКАЦИИ БАЗОВЫХ СХЕМ МОДУЛЯ СОПРЯЖЕНИЯ В РЕЖИМЕ ЗАПРОСА ОТ ОБЪЕКТА

С.Л. Крыловский, студент 3 курса;
М.Г. Власова, студент 3 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 8-903-951-1825,8-913-851-3569

В работе рассмотрен подход к модификации базовых схем модуля сопряжения в режиме запроса от объекта.

Задача в общем виде формулируется так: Представить схему сопряжения канала процессора с электроавтоматикой объекта автоматизации для заданной ситуации (вариант 25). За основу мы приняли схемы, представленные в учебном пособии [1, рис. 7.1 и 7.2] и [2, рис.

1.34 и 1.35], исключив элементы, не относящиеся к управлению заданной ситуацией («Поиск тары»). Иначе, произвести модификацию базовой схемы. Подсистема управления объектом по индивидуальным запросам обслуживания с индивидуальными адресами флагов F1-F6. Управление ситуацией «Поиск тары». Ресурсы процессора выделены для управления заданной ситуацией [2, базовая схема 1, п.п. 1.5.2; математическая модель управления – п.п. 2.3].

Подходы к решению. Модификация базовых электрических функциональных схем физического (аппаратного) слоя подсистемы в соответствии с определенным заданием варианта описана на уровне математических моделей в п. 2.3 и 2.4 [2]. Модификация касается подключения к базовой схеме узлов формирования запросов, сбора запросов и чтения флагов F5 и F6 состояния объекта.

Функциональные схемы этих узлов представлены в п. 3.1 [2] для проектируемого варианта 25 задания и для других вариантов.

Концептуальная модель модификации схем модуля представлена на рис. 1. Базовая схема 1 связана с каналом в соответствии с протоколом программного обмена. Из базовой схемы 1 исключены все элементы структуры, не относящиеся к функциям, указанным в варианте задания (вариант 25). Базовая схема подключена к объекту линиями FL3 и FL4, а по линии F3 – к формирователю запроса ZP1, передаваемого через канал процессору для анализа и организации обслуживания.

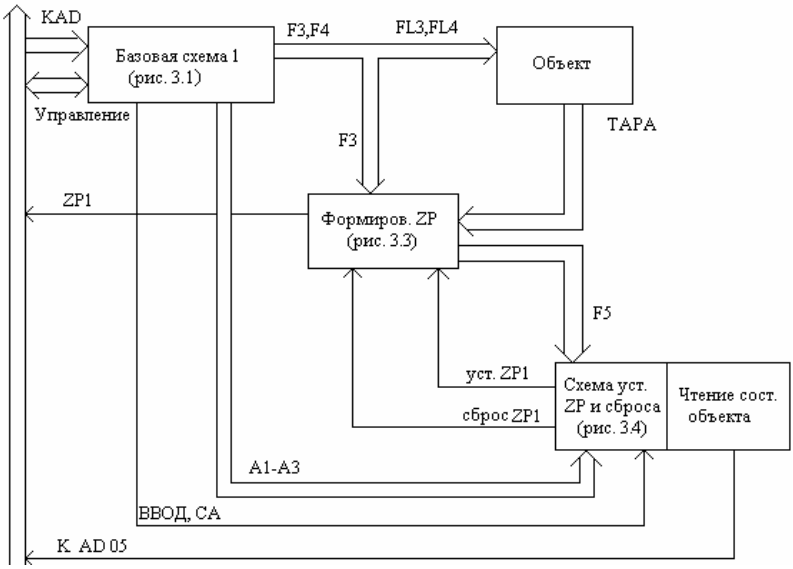


Рис. 1. Концептуальный подход к модификации модуля сопряжения. Проектируемая структурная схема модуля сопряжения

Кроме того, базовая схема 1 передает формирователям синхронизирующих сигналов УСТановки и СБРоса запроса ZP1 системный управляющий сигнал ВВОД и признак СА селекции адреса модуля сопряжения. Для идентификации флагов F1-F6 с индивидуальными адресами к упомянутым формирователям от базовой схемы 1 по трехразрядной шине поступает адресное поле А(3-1). Узел чтения состояния объекта использует флаг F5, поле А(3-1) и сигналы ВВОД и СА.

Выводы. Проблема модификации базовых схем с помощью подключения узлов формирования запросов, сброса запросов и чтения флагов F5 и F6 усложняет задание курсовой работы студентов. В результате был разработан концептуальный подход к модификации модуля сопряжения, с помощью которого можно доступно и понятно модифицировать базовую схему модуля сопряжения для проектируемого варианта 25 и для других вариантов задания.

ЛИТЕРАТУРА

1. *Прищепа Л.С.* Компьютерные средства в системах автоматизации и управления. Книга 3: Учебное пособие. Локальная вычислительная система автоматизации. Программное оснащение. Сопряжение с объектом. Томск: Изд-во Том. ун-та, 1997. 115 с.
2. *Прищепа Л.С.* Компьютерные средства в системах автоматизации и управления. Системотехника, вычислительные комплексы и сети ЭВС: Учебное методическое пособие к курсовому проектированию. Томск: ТМЦДО, 2003. 144 с.

ГРАФИЧЕСКИЙ ПАРОЛЬ

Р.А. Яковлев, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 261000, jrom@ultranet.tomsk.ru

Идентификацию и аутентификацию можно по праву считать основой программно-технической средств безопасности поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. *Идентификация* и *аутентификация* – это первая линия обороны, «проходная» информационного пространства организации.

Современные средства *идентификации*/*аутентификации* должны поддерживать концепцию *единого входа в сеть*. *Единый вход в сеть* – это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная *идентификация*/*аутентификация* становится слишком обременительной. К сожалению, пока

нельзя сказать, что *единый вход в сеть* стал нормой, доминирующие решения пока не сформировались.

Основной проблемой в парольной аутентификации является то, что обычные рядовые пользователи, некоторые по не знанию, некоторые по каким-то другим причинам, например для легкого запоминания, вводят очень простые пароли (свои имена, имена детей, телефоны, простые последовательности букви цифр – «qwerty», «12345» и т.д.), которые не составляет большого труда подобрать по словарю или после небольшого знакомства с этим человеком можно выяснить имя ребенка и т.п.

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

Другой подход к надежной *аутентификации* состоит в *генерации нового пароля* через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу *аутентификации* должен быть известен алгоритм *генерации паролей* и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

Биометрия представляет собой совокупность автоматизированных методов *идентификации* и/или *аутентификации* людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи. Но главная опасность состоит в том, что любая «пробоина» для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей систем.

Проблему безопасности компьютерных сетей надуманной не назовешь. Практика показывает: чем масштабнее сеть и чем более ценная информация доверяется подключенным к ней компьютерам, тем больше находится желающих нарушить ее нормальное функционирование ради материальной выгоды или просто из праздного любопытст-

ва. Идет постоянная виртуальная война, в ходе которой организованности системных администраторов противостоит изобретательность компьютерных взломщиков. Основным защитным рубежом против злонамеренных атак в компьютерной сети является система парольной защиты, которая имеется во всех современных программных продуктах. В соответствии с установившейся практикой, перед началом сеанса работы с операционной системой пользователь обязан зарегистрироваться, сообщив ей свое имя и пароль. Имя требуется для идентификации пользователя, а пароль служит подтверждением правильности произведенной идентификации.

Для более простой и легкой в запоминании аутентификации пользователей предлагается использовать графику. Формальный приоритет на авторизованный доступ посредством графической картинки принадлежит некоему Грегу Блондеру (Greg Blonder) и защищен американским патентом №5559961 от 1996 г. Однако знатоки фантастики могут вспомнить, что еще в 1981 г. основоположник киберпанка Уильям Гибсон в рассказе «Джонни-Мнемоник» описал пароль в виде зрительного образа, открывающего доступ к зашифрованному архиву. Впрочем, ни Гибсона, ни Шахерезаду (с ее сказкой о пещере, закрытой акустическим кодом) не стоит считать первопроходцами – такие пароли, наверняка, использовались с незапамятных времен. В простом случае идентификация происходит по щелчкам мышью на заранее обговоренных местах пейзажей с большим количеством деталей. В более сложном случае паролем является набор пиктограмм, которые показываются пользователю в комбинации с другими пиктограммами. Чтобы не опасаться троянских программ и разного рода «подглядывания из-за плеча». Трудно поверить, но она делает бесполезным любое подсматривание за процессом авторизации, кроме самого первого ввода, когда пароль создается. Представьте, что вам показывают набор из множества небольших, но запоминающихся иконок. Из них надо выбрать несколько штук (скажем, пять), которые вы не забудете и не спутаете с другими. Когда выбор сделан, пароль считается созданным. При последующей авторизации вам снова показывают большое поле, заполненное множеством значков, среди которых вы находите не менее трех ранее выбранных. Дальше нужно мысленно образовать из трех иконок треугольник и кликнуть где угодно внутри него! Для надежности эта процедура повторяется несколько раз – вам показывают несколько наборов значков, и вы несколько раз кликаете внутри треугольников, существующих только у вас в голове. Ключевые иконки при этом никак не выделяются, поэтому, даже записав «ввод» пароля на видео, взломщику придется сделать полноценный криптоанализ введенных комбинаций. По словам автора алгоритма Леонардо Собрадо (Leonardo Sobrado), пользователь не столько вводит пароль, сколько доказывает

системе его знание. Подобрать такой пароль, даже фиксируя щелчки мышью, будет не просто.

Самым большим преимуществом у графического пароля является – легкость его запоминания, так как здесь уже работает совершенно другой вид памяти – зрительная память. Против картинок хакеру придется подбирать колоссальное количество комбинаций, которые могли бы подойти под соответствующий изображению цифровой код, хранящийся в операционной системе.

ЛИТЕРАТУРА

1. *Галатенко В.А.* Основы информационной безопасности. Интернет Университет Информационных Технологий, INTUIT.ru
2. *Девянин П.Н., Проскурин В.Г., Черемушкин А.В.*Введение в криптографию / Под ред. В. В. Ященко.
3. *Методы* и средства защиты информации. Авторские права: Беляев А.В. 2000.
4. *Зегжда Д.П., Ивашко А.М.* Основы безопасности информационных систем. М.: Горячая линия-Телеком. 2000.
5. http://www.osp.ru
6. http://citforum.ru
7. http://www.p-stone.ru

ЗАЩИЩЕННЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

А.А. Гнатына, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, т. +7-923-402-43-59 , e-mail: gnatyna@gmail.com

Недостаток квалификации персонала и особенности национального менталитета неумолимо накладывают отпечаток на общую эффективность организации рабочего процесса. Компьютеры в большей своей массе продолжают использоваться как усовершенствованные печатные машинки, и авторитетные специалисты не раз отмечали, что внедрение вычислительных средств без серьезной проработки информационной структуры предприятия лишь усиливает неразбериху.

С задачей поиска нужных документов так или иначе связаны 30% перемещений сотрудников по офису, в общей сложности этот процесс отнимает у них около одного месяца в год, причем 15% бумажных документов безвозвратно теряются. На согласование документов уходит 60–70% рабочего времени. В свете вышеуказанного, 20–30% поставленных задач вообще не решаются. Все эти проблемы призвана решить грамотная организация безбумажных технологий управления.

Несмотря на сравнительно высокую стоимость систем электронного документооборота, многие производители приводят впечатляю-

щие данные, подтвержденные экономическими расчетами и многочисленными примерами реальных внедрений. Они свидетельствуют о том, что затраты на внедрение системы окупаются за срок от шести месяцев до полутора лет, в зависимости от масштабов предприятия и степени его охвата автоматизацией. Но, если в крупных предприятиях момент истины назрел уже давно, то сейчас в организации электронного документооборота больше всего заинтересованы представители малого и среднего бизнеса, а они, надо отдать им должное, всегда лучше считают деньги.

Базовой единицей информации в теории управления документами является непосредственно документ. Понятие электронного документа включает в себя не просто файл (набор символов, слов, таблиц, диаграмм, изображений и мультимедийных данных), а целую совокупность таких файлов разных типов – составных частей документа, правила их обработки, связи с другими электронными документами, информацию о маршруте движения документа и многое другое. Обязательным является наличие у документа регистрационной карточки – набора реквизитов документа (вид документа, регистрационный номер, краткое содержание и другие атрибуты, в общем случае регламентируемые ГОСТами, но они могут отличаться в конкретных случаях). В таком виде документ становится базой построения системы электронного документооборота – системы, организующей полный жизненный цикл документа, начиная от регистрации и заканчивая списанием в архив.

Обязательные задачи, решение которых должна обеспечивать любая система электронного документооборота, – это непосредственная работа с регистрационной карточкой, контроль исполнения, ввод и вывод документов, их поиск и организация защищенной работы в сетевом режиме.

В настоящее время, в эпоху стремительного развития средств коммуникаций, в частности Интернет, целесообразно использовать существующие сети передачи информации в сферах деятельности, которые требуют тщательной защиты от несанкционированного доступа. Одним из примеров такой сферы деятельности может быть деятельность налоговой инспекции, или пенсионного фонда РФ.

Налоговая отчетность должна предоставляться гарантированно конфиденциально, но искушение использовать для этого разветвленную инфраструктуру сетей слишком велико. Именно поэтому требуется создание площадки, которая будет гарантировать конфиденциальность пересылаемой информации, ее достоверность, и которая будет использовать в качестве линий передачи Интернет.

Следует отметить, что система, отвечающая этим требованиям, может использоваться во многих сферах деятельности, начиная от документооборота, заканчивая перепиской между друзьями.

Для реализации данной системы, мы выдвинули несколько требований к ней. В частности к ее структуре.

Она должна включать в себя следующие компоненты:

• Клиентская часть

• Серверная часть

• Монитор

Это минимальный набор компонент, который требуется для реализации. Он может быть расширен для повышения функциональности.

Каждый компонент системы отвечает за строго определенный круг задач. Рассмотрим их.

Клиентская часть

Эта часть, которая установлена на стороне клиента. Она должна осуществлять прием/передачу информации из/в сеть, шифрование/дешифрование данных, подпись данных, проверку подписей. В практической реализации клиентская часть представляет из себя программный продукт, реализующие перечисленные выше функции.

Серверная часть

Серверная часть должна обеспечивать транспорт системы. Она работает только как временное хранилище передаваемой информации.

Для гарантирования достоверности информации, подтверждения факта ее передачи, серверная часть должна вести подробные логи приема/передачи сообщений.

Монитор

На монитор системы возлагается вычислительная нагрузка. Так как система работает с подписанными с помощью ЭЦП сообщениями, должен соблюдаться регламент обмена такими сообщениями. Монитор выступает как арбитр.

Его функции – это забрать пришедшее на сервер сообщение от отправителя, проверить с помощью открытого ключа отправителя его ЭЦП, чтобы подтвердить достоверность информации, поставить временной штамп на сообщение, чтобы зафиксировать время его отправки отправителем, занести все проделанные операции с их результатом в лог и перенаправить переподписанное сообщение получателю.

Таким образом, монитор должен хранить открытые ключи всех пользователей системы.

Общий алгоритм работы системы

Пользователь системы формирует сообщение для получателя (другого пользователя системы). Далее клиентская часть его шифрует,

подписывает электронной подписью пользователя-отправителя и отправляет на сервер. Сервер получает зашифрованное и подписанное сообщение, заносит в журнал необходимые данные (отправителя, получателя, время, размер сообщения, контрольную сумму и т.д.) и передает его монитору. Монитор забирает сообщение, проверяет электронную подпись отправителя, заносит результаты в журнал, переподписывает сообщение своей электронной подписью с временным штампом и передает его серверу с пометкой, что оно должно идти получателю. Так же монитор отправляет уведомление отправителю, что его письмо учтено арбитром и отправлено получателю. Получатель (клиентская часть) забирает сообщение, проверяет подпись монитора, временной штамп монитора, проверяет подпись отправителя, расшифровывает сообщение и читает его.

Таким образом, выполняется регламент обмена подписанными сообщениями, ведется 2 журнала обмена, по которым можно восстановить картину обмена, пользователи уверены в достоверности информации, спорные вопросы решает арбитр посредством журнала.

ЛИТЕРАТУРА

1. *ГОСТ* Р 51624-2000 Защита информации. Автоматизированнные системы в защищенном исполнении. Общие требования.
2. *ГОСТ* Р 50922-96. Защита информации. Основные термины и определения.
3. *ГОСТ* Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования.
4. http://demo.kontur-extern.ru/first.aspx СКБ «Контур»
5. http://www.fdc.ru/portal/page?_pageid=34,182153&_dad=portal&_schema=PORTAL «Форс – центр разработки»
6. http://www.infin.udm.ru/aboutsystem.htm «ИНЖИНФОРМПРОЕКТ»
7. http://www.evfrat.ru/info/press8.htm «ЕВФРАТ Документооборот»
8. http://www.e-notary.ru/analitics/princ/ «E-Notary Центр Поддержки Электронных Сервисов»

ПРИНЦИПЫ РАБОТЫ ИНФОРМАЦИОННЫХ ПОИСКОВЫХ СИТЕМ

П.А. Коцюба, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, т. 8-913-800-01-99 , e-mail pashik@ms.tusur.ru

Менее десяти лет назад появился Internet – уникальное явление в человеческой жизни. В его необъятных просторах есть, наверное, вся или почти вся информация. Однако найти ее там далеко не просто.

До возникновения Internet люди тратили колоссальное количество времени, чтобы «откопать» требуемые сведения из газет, журналов, справочников. Благодаря новым информационным технологиям ситуация значительно упростилась. Сегодня можно оперативно находить ответы на многие практические вопросы и проводить аналитические исследования, не выходя из офиса.

В настоящее время в США и странах Западной Европы сбор информации из Internet представляет самостоятельный и очень прибыльный бизнес. Этим занимаются специализированные исследовательские центры.

Поиск информации. Модель поиска.

В информационно-поисковых системах реализуются различные модели поиска, определяющие то, какими средствами задается запрос к системе, и то, какие результаты пользователь получает в ответ.

В Интернет-поисковых машинах наиболее популярна плоская «векторная» модель. Запрос в ней состоит из нескольких слов через пробел. Из этих слов составляется правило отбора документов. Когда количество ресурсов в сети было еще невелико, некоторые машины могли работать по заданным словам с логическим оператором ИЛИ, что, безусловно, вело к значительному расширению понятия релевантности результатов. На сегодня большинство машин работает по принципу наличия в документе всех слов запроса. Причем некоторые накладывают еще более строгие ограничения, требуя по умолчанию, чтобы все слова стояли рядом, например, в одном предложении. Но все равно, на такие запросы выпадает, как правило, огромное количество документов, поэтому вся содержательная алгоритмическая нагрузка ложится на функцию ранжирования. 99% пользователей никогда не просматривают больше двух страниц результатов поиска, поэтому чрезвычайно важно, какие документы ИПС поставит на первые позиции. В большинстве алгоритмов ранжирования в том или ином виде используется «векторный» подход, учитывающий частотность терминов запроса в документе. Однако лучшие поисковые системы комбинируют векторный подход с другими принципами ранжирования, основанными не только на содержании документа, но и на мета-информации о нем (популярность сайта и пр.).

В основе любой современной полнотекстовой ИПС лежит так называемый «инверсный индекс». В упрощенном понимании, индекс ИПС – это информация о вхождениях слов в документы, упорядоченная по словам. Несмотря на то, что принципы построения индексов во всех ИПС похожи, от структуры индекса зависит большое количество качественных характеристик поисковой машины.

Поисковый алгоритм.

Запрос для ИПС с логической моделью поиска представляет собой иерархическое дерево с элементарными операндами в листах (термины запроса, а также – результат сканирования словарей индекса) и операциями в узлах дерева (логические – И, ИЛИ, И НЕ, а также контекстные – расстояние, следование). Многие Интернет-поисковые машины, работающие с векторной моделью поиска, оптимизированы под плоские запросы из 3–4 слов, и достигают высоких скоростей за счет сокращения накладных расходов в подобных простых случаях.

Роботы поисковой системы.

Роботы поисковой системы, иногда их называют «пауки» или «кроулеры» (crawler) – это программные модули, занимающиеся поиском web-страниц.

Поисковые роботы стоит воспринимать, как программы автоматизированного получения данных, путешествующие по сети в поисках информации и ссылок на информацию.

Когда, зайдя на страницу «Submit a URL», вы регистрируете очередную web-страницу в поисковике – в очередь для просмотра сайтов роботом добавляется новый URL. Даже если вы не регистрируете страницу, множество роботов найдет ваш сайт, поскольку существуют ссылки из других сайтов, ссылающиеся на ваш. Вот одна из причин, почему важно строить ссылочную популярность и размещать ссылки на других тематических ресурсах.

Прийдя на ваш сайт, роботы сначала проверяют, есть ли файл robots.txt. Этот файл сообщает роботам, какие разделы вашего сайта не подлежат индексации. Обычно это могут быть директории, содержащие файлы, которыми робот не интересуется или ему не следовало бы знать.

Роботы хранят и собирают ссылки с каждой страницы, которую они посещают, а позже проходят по этим ссылкам на другие страницы. Вся всемирная сеть построена из ссылок. Начальная идея создания Интернет сети была в том, что бы была возможность перемещаться по ссылкам от одного места к другому. Вот так перемещаются и роботы.

На сколько робот будет корректен в отношении индексирования страниц в реальном режиме времени зависит от инженеров поисковых машин, которые изобрели методы, используемые для оценки информации, получаемой роботами поисковика. Будучи внедрена в базу данных поисковой машины, информация доступна пользователям, которые осуществляют поиск. Когда пользователь поисковой машины вводит поисковый запрос, производится ряд быстрых вычислений для уверенности в том, что выдается действительно правильный набор сайтов для наиболее релевантного ответа.

Вы можете просмотреть, какие страницы вашего сайта уже посетил поисковый робот, руководствуясь лог-файлами сервера, или результатами статистической обработки лог-файла. Идентифицируя роботов, вы увидите, когда они посетили ваш сайт, какие страницы и как часто.

ЛИТЕРАТУРА

1. Конкурентная разведка в Интернет / В.В. Дудихин, О.В. Дудихина. 2-е изд., испр. и доп. М.: ООО «Издательство АСТ»: Издательство «НТ Пресс», 2004. 229 с.
2. http://www.intuit.ru.
3. www.webmasterpro.com.ua.
4. http://www.integrum.com Информационная система «Артефакт».

ПОДСЕКЦИЯ 9.2

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ЭФФЕКТИВНОСТЬ ЗАЩИТЫ С ПОМОЩЬЮ ЗАПУТЫВАЮЩИХ ПРЕОБРАЗОВАНИЙ

Д.Н. Буинцев, инженер каф. КИБЭВС;
О.О. Шевцова аспирант каф. КИБЭВС
ТУСУР, г. Томск, т.51-36-00, studprof@tusur.ru

При защите программных средств (ПС) с помощью запутывающих преобразований основными характеристиками являются:

– эффективность защиты (эффективность запутывающих преобразований);

– размер требуемых ресурсов вычислительной системы (ВС), который выражается увеличением объема текста ПС и времени выполнения ПС. Размер таких ресурсов может быть определен с помощью экспериментов с ПС или их моделями.

Эффективность защиты возможно определить с помощью методики, предложенной С.П. Расторгуевым.

Запутывание будет считаться эффективным тогда, когда время, потраченное на анализ кода программы, соизмеримо и больше, чем время, потраченное на написание нового кода.

Вероятность того, что защита не будет снята с защищенной программы ни одним из средств на момент времени *t*, будет определяться по формуле:

$$p_1(t) = 1 - L_1 r_1(t), \quad (1)$$

где $r_1(t)$ – вероятность наличия у пользователя средства на момент времени *t* из множества средств снятия защиты; L_1 – вероятность, что пользователь опробует имеющиеся у него средства для автоматического снятия защиты с защищаемой программы.

Для получения численной экспертной оценки надежности защитного механизма используется качественное понятие «Уровень Понимания Программного Продукта» (УППП).

Это понятие отражает знание и понимание экспертом назначения команд и операндов программы. Единица его измерения – число машинных команд, операндов. Уровень понимания программного продукта максимален, когда эксперт в состоянии «откомментировать» назначение каждой команды и каждого операнда.

Вероятность того, что эксперт за время *t* не сможет разобраться с защитным механизмом, можно представить как формулу:

$$p_2(t) = 1 - L_2 \frac{U(t)}{N}, \quad (2)$$

где L_2 – вероятность того, что пользователь опробует имеющиеся у него средства для исследования программной системы защиты; $U(t)$ – УППП на момент времени *t*; N – объем защищенной программы в машинных командах.

Значение $U(t)$ – рассчитывается по формуле:

$$U(t)dt = kdU, \quad (3)$$

Понимание экспертом каждой анализируемой команды или операнда во многом определяется тем, как он смог освоить уже исследованную часть модуля (т.е. если эксперт продолжает исследовать программу в течении времени dt, то его уровень понимания изменится на *dU*):

При этом *U*(*t*) имеет смысл только тогда, когда его значение меньше или равно *N*, т.е.

$$0 \le U(t) \le N.$$

Коэффициент k в формуле – это коэффициент сложности анализа, определяющим фактором которого цикломатического число Маккейба. Оно определяет число линейно независимых контуров в графе, тем самым отражает сложность понимания назначения команд в их зависимости друг с другом.

$$k = e - v + 2\mu, \qquad (4)$$

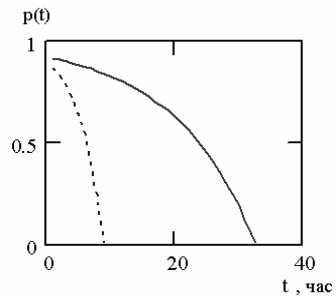
где e – число дуг ориентированного графа, v – число вершин, μ – число компонент связанности графа.

В качестве исходных программ для тестирования были выбраны программы, реализующие различные виды сортировки последовательности элементов по методам «пузырька», «выборки», «вставки» и «Шелла».

Результаты расчета вероятности того, что программа не будет взломана в данный момент времени приведены на рисунке на примере программ сортировки методом «Шелла».

Объем в инструкциях для исходной программы сортировки методом «Шелла» – значения параметра $N = 16000$, коэффициент сложности анализа $k = 4$. Для запутанной программы, значение $N = 20740$, коэффициент сложности анализа $k = 13$.

Из приведенного графического отображения и сравнения количественных характеристик для исходной и запутанной программ видно, что на анализ исходного текста программы будет затрачено меньше времени, чем запутанного кода. Это следует из того, что для любого момента времени величина $p(t)$ для запутанной программы больше, чем вероятность $p(t)$ для исходной.



Расчет вероятностей для программ сортировки методом «Шелла»: сплошная линия – для запутанной программы, пунктирная линия – для исходного текста программ

Обобщая полученные результаты численных расчетов получено, что среднее значение вероятности того, что защита запутанного текста не будет снята, составляет 0,87. Для анализа исходного текста программного средства будет затрачено времени в 8 раз меньше, чем на анализ запутанного текста.

ЛИТЕРАТУРА

1. *Расторгуев С.П.* Программные методы защиты информации в компьютерах и сетях. М.:»Яхтсмен», 1993. 188 с.
2. *Расторгуев С.П., Дмитриевский Н.Н.* Искусство защиты и «раздевания» программ. М.: Совмаркет, 1991. 94 с.
3. Ч*ернов А.В.* Анализ запутывающих преобразований программ: http://mksoft.km.ru/my/pda/channels/geturl.php?url=http://citforum.ru//security/articles/analysis/

ПРОБЛЕМА ХАРАКТЕРИСТИКИ ЛИЧНОСТИ КИБЕРПРЕСТУПНИКА В ОТЕЧЕСТВЕННОЙ И ЗАРУБЕЖНОЙ КРИМИНАЛИСТИКЕ

И.В. Давыдов, аспирант; К.Н. Филькин, аспирант
ТУСУР, каф. КИБЭВС, г. Томск, davidoffi@mail.ru; astron@ngs.ru

С увеличением производительности компьютерной техники возрастает изощренность компьютерной преступности, а с бурным развитием глобальной информационной сети Интернет мир столкнулся с таким явлением как «киберпреступность». Вопросы криминалистической характеристики субъектов преступной деятельности в сфере использования компьютерных технологий, субъективно-личностные свойства ее участников еще недостаточно изучены, а постоянно нарастающая динамика совершения киберпреступлений требует принятия неотложных действий.

В настоящее время компьютерная преступность в отличие от другого рода преступлений характеризуется высокой латентностью, и именно поэтому получить достоверные данные относительно лиц, которые совершают преступления в сфере использования компьютерных технологий, просто невозможно.

Проблема характеристики личности «компьютерного преступника» требует как его изучения на уровне сущностной оценки обобщенных фактических данных, так и анализа статистических данных, характеризующих объект исследования, уголовно-правовой характеристики личности преступника.

Выявление существенных данных о личности преступника является одним из ключевых моментов не только в расследовании преступления, но и в организации мер противодействия и профилактики киберпреступлений.

Согласно статье В.А. Голубева «Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий», **субъект преступления** – это минимальная совокупность признаков, характеризующих лицо, совершившее преступление, которая необходима для привлечения его к уголовной ответственности.

Можно предложить и другое определение субъектам киберпреступления – это подготовленные в профессиональном плане индивиды, действующие в самостоятельном или групповом формате на основе политических, криминальных, хулиганских побуждений, профессионального интереса или исследовательских целей.

Личностные качества киберпреступника и внешняя среда в своем взаимодействии последовательно определяют мотивацию принятия

решения для преступной деятельности в сфере компьютерных технологий.

Количество личностных качеств киберпреступника можно выделять сколь угодно много и все они будут в той или иной степени характеризовать его сущность. Естественно и то, что у всех этих личностных качеств есть своя определенная значимость для киберпреступления. Выделение важных качеств позволит построить модель киберпреступника, а в дальнейшем и адекватную модель противодействия.

Предложенное В.Б. Веховым разделение киберпреступников на три обособленные группы (лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности; лица, страдающие новым видом психических заболеваний – информационными болезнями или компьютерными фобиями; и профессиональные компьютерные преступники с ярко выраженными корыстными целями) позволяет выделить следующие немаловажные личностные качества киберпреступника, такие как: профессионализм в области компьютерной техники, знание уголовного законодательства в области в области обеспечения информационной безопасности и смежных областях (мошенничество, кража, изготовление подделок и т.д.), принадлежность к организованным преступным группам, а также социальное положение в обществе и киберпространстве.

Анализ из этих качеств каждого в отдельности и в сумме позволит определить некий тип киберпреступника и оптимизировать оперативно-розыскные, следственные действия, а также иные действия необходимые в процессе расследования киберпреступления.

Немаловажно, чтобы правоохранительные органы постигли природу кибепреступлений и противоборствовали со злоумышленниками их же оружием – Интернетом. Сегодня в России и во всем мире принимаются меры по обеспечению конституционных прав граждан, касающихся защиты информации и гарантирования информационной безопасности, созданию благоприятных условий для предотвращения и борьбы с киберпреступлениями. Однако киберпреступность не признает границ и традиционные приемы обнаружения и борьбы с киберпреступлениями недостаточно эффективны. В этом контексте актуальным является дальнейшее исследование криминологических проблем киберпреступлений, научный поиск эффективных путей повышения уровня информационной безопасности посредством совершенствования организационно-правовой защиты информации в компьютерных системах, решения проблем предупреждения и расследования компьютерных преступлений, подготовки специалистов-правозащитников в этой сфере.

Знание личностных свойств субъектов преступной деятельности в сфере использования компьютерных технологий позволит оперативным работникам, следователям своевременно выявлять, раскрывать и расследовать такие преступления, определять тактику проведения допроса, криминалистических операций.

ЛИТЕРАТУРА

1. *Голубев В.А.* Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий. http://www.crime-research.org/library/Golubev0104.html.
2. *Вехов В.Б.* Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: Учеб.-метод. пособие. Изд. 2-е, доп. и испр. М.: ЦИ и НМОКП МВД России, 2000. 64 с.
3. *Криминалистическая* методика расследования отдельных видов преступлений: Учебное пособие в 2-х частях. Ч. 2: / Под ред. А.П. Резвана, М.В. Субботиной. М.: ИМЦ ГУК МВД России, 2002. 232 с
4. *Криминалистика:* Учебник. Изд. 2-е, доп. и перер. / Под редакцией д.ю.н, профессора Закатова А.А., док. юрид. наук, профессора Смагоринского Б.П. М.: ИМЦ ГУК МВД России, 2003. 432 с.
5. *Головин А.Ю.* Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации. http://www.crime-research.org/library/Golovin.htm.
6. *Криминалистика:* Учебник для среднего профессионального образования / Редкол.: Закатов А.А., Смагоринский Б.П. (отв. редакторы), Тарасов В.П., Копылов И.А., Резван А.П. Волгоград: ВА МВД России, 2000. 472 с.
7. *Егорышев А.С.* Криминалистический анализ лиц, осуществляющих неправомерный доступ к компьютерной информации. / Южно-уральские криминалистические чтения. Сборник научных статей: Выпуск 10 / Под редакцией И.А. Макаренко. Уфа: РИО БашГУ, 2002. С. 76 – 81.

МЕТОД ОЦЕНКИ РИСКОВ, ОСНОВАННЫЙ НА ПОСТРОЕНИИ МОДЕЛИ УГРОЗ И УЯЗВИМОСТЕЙ

С.С. Ерохин, студент 4 курса ФВС

ТУСУР, г. Томск, ess_84@inbox.ru

Вопросы обеспечения информационной безопасности исследуются в разных странах довольно давно. В настоящее время сложилась общая точка зрения на концептуальные основы информационной безопасности. Четко стандартизовать аспекты безопасности впервые были удачно предприняты в Британском стандарте BS7799 «Практические правила управления информационной безопасностью», в 1995 г.. Позже этот стандарт переиздан в 2002 г. – ISO1779902. Одним из

основных критериев в стандарте ISO1779902 является критерий оценки рисков. Само понятие «оценка рисков» появилось сравнительно не давно и вызывает большой интерес у специалистов в области информационной безопасности.

Оценки рисков должны применяться на предприятиях с различным родом деятельности и с различным уровнем доходов. Оценка рисков позволяет получить результаты, характеризующие безопасность, как автоматизированных систем, так и бизнес процессов, что в настоящее время является актуальной темой у руководителей предприятий. А так же сформировать адекватные требования к системе защиты, что существенно уменьшает затраты предприятия на обеспечение информационной безопасности.

В настоящее время существует три программных продукта, которые позволяют провести оценку рисков по различным методикам. Первый и самый старый – метод CRAMM (ССЕФ Risk Analysis and Management Method), который был разработан в 1985 году агентством по компьютерам и телекоммуникациям Великобритании.

Исследование информационной безопасности данным методом проходит в три этапа:

– анализируется все, что касается идентификации и определения ценностей ресурсов;

– анализируется все, что относится к идентификации оценки уровней угроз для групп ресурсов и уязвимостей;

– поиск адекватных контрмер.

CRAMM имеет обширную базу, содержащую описание около 1000 примеров реализации подсистем защиты различных компьютерных систем. Данные описания можно использовать в качестве шаблонов.

Недостатками данного продукта является высокая стоимость; добавлять данные в базу знаний не представляется возможным; создавать свои шаблоны так же нельзя; данный продукт существует только на английском языке.

Следующее программное обеспечение – RiskWatch. Данный программный продукт является мощным средством анализа рисков, в который включены средства, предназначенные для анализа физических методов защиты; информационных рисков; соответствия системы стандартам ISO 17799 и HIPAA (Healthcare Insurance Portability and Accountability Act).

RiskWatch осуществляет анализ рисков в четыре этапа:

– определение предмета исследования (тип организации, состав исследуемой системы, базовые требования к безопасности);

– определение конкретных характеристик системы (ресурсы, потери, частота возникновения угроз, степень уязвимости);

– производится количественная оценка рисков;

– генерация отчетов.

Рассматриваемый программный продукт позволяет оценить не только риски, которые существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных средств и механизмов защиты. Это обусловлено тем, что на этапе количественной оценки рисков вычисляется эффективность внедрения средств защиты, описываемая с помощью показателя ROI (Return on Investment), который показывает отдачу от сделанных инвестиций за определенный период времени.

К недостаткам данного программного обеспечения можно отнести очень высокую стоимость; используемые методы не учитывают комплексный подход к информационной безопасности; осуществляется анализ только на программно-техническом уровне защиты; существует только на английском языке.

Последняя из рассматриваемых систем – ГРИФ. Данный программный продукт является системой анализа и управления рисками информационной безопасности предприятия. Система ГРИФ позволяет анализировать уровень защищенности ценных ресурсов предприятия; оценивать возможный ущерб от реализации угроз информационной безопасности; выбор оптимальных контрмер по соотношению цена\качество.

Анализ рисков с использованием рассматриваемой системы можно проводить двумя методами: построение модели информационных потоков и построение модели угроз и уязвимостей системы.

При использовании метода построения модели информационных потоков анализ происходит в четыре шага:

– описываем все существующие объекты информационной системы (группы, ресурсы);

– определяем связи между группами и ресурсами;

– отвечаем на вопросы, связанные с политикой безопасности;

– генерация полной модели информационной системы с точки зрения информационной безопасности.

При использовании метода построения модели угроз и уязвимостей анализ происходит в три шага:

– описываем все существующие объекты информационной системы (группы, ресурсы);

– определяем связи между группами и ресурсами;

– генерация отчета с указанием значения риска для каждого ресурса в системе.

Все рассмотренные программные продукты обладают одним недостатком – высокой стоимостью для одного рабочего места. В связи с

этим была поставлена задача: «разработать и построить модель анализа рисков для автоматизированной системы с минимальными затратами». Для достижения этой цели был проведен анализ существующих моделей автоматизированных систем с целью обнаружения базовой модели. Обнаружение базовой модели предоставляет возможность преобразовать большую систему в ряд базовых, что существенно может упростить оценку рисков для экспертов.

Для базовой автоматизированной системы была построена модель угроз и уязвимостей. На вход данной модели поступают ресурсы, критичность ресурса, угрозы, уязвимость, вероятность реализации угрозы. На выходе данной модели получаем суммарный риск реализации всех угроз для ресурсов; риск реализации угрозы для автоматизированной системы; эффективность контрмер.

ЛИТЕРАТУРА

1. *Симонов С.В.* Анализ рисков, управление рисками. Jet Info.
2. *Петренко С.А., Симонов С.В.* Анализ и управление информационными рисками. АйТи, 2003.
3. *Куканова Н.А.* Методика оценки риска ГРИФ 2005 из состава Digital Security – BugTraq.

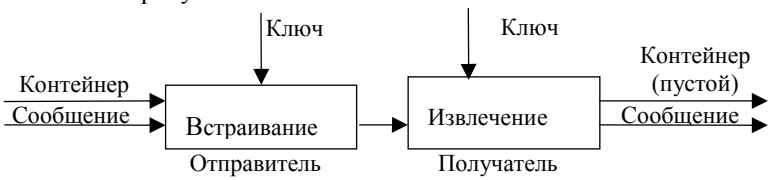
ОБЗОР МЕТОДОВ СТЕГАНОГРАФИЧЕСКОГО СОКРЫТИЯ ИНФОРМАЦИИ В ГРАФИЧЕСКИХ ФАЙЛАХ

С.Н. Филькин, студент 3 курса каф. КИБЭВС

ТУСУР, г. Томск, tiere@ngs

Как известно, цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений. Стеганография имеет другую задачу, и ее цель – скрыть сам факт существования секретного сообщения. При этом, оба способа могут быть объединены и использованы для повышения эффективности защиты информации (например, для передачи криптографических ключей).

Обобщенная модель скрытого канала передачи информации представлена на рисунке.



Обобщенная модель стегосистемы

Контейнером называется любая информация, предназначенная для сокрытия тайных сообщений. Ключ – данные, позволяющие скрыть и обнаружить сообщение.

В качестве контейнера удобно выбирать графические или мультимедийные файлы, которые имеют ряд преимуществ над текстовыми файлами. Прежде всего, оно заключается в простоте реализации и надежности. Гораздо проще изменить на тон цвет точки на рисунке или частоту звука, чем заменять или переставлять слова в текстовом файле. К тому же с помощью чувств такие изменения заметить практически невозможно.

Существуют различные виды графических форматов. Во-первых, они делятся на векторные и растровые форматы. Обобщенно говоря, в векторных форматах хранится информация (команды) по воссозданию изображения, а в растровых форматах хранится информация о каждой точке изображения. Растровые форматы в свою очередь могут использовать сжатие данных, причем оно может быть как без потери качества, так и с его потерей. Ниже приведен обзор методов, позволяющих сокрытие информации в графических файлах.

Методы, использующие особенности формата файла-контейнера.

Обычно графический файл содержит внутри себя определенные части: заголовок, блок данных и т.д. И для того, чтобы указать то место в файле, с которого начинается данные, ставится специальный символ. Все, что находится до него, воспринимается как служебная информация, следовательно, она не будет восприниматься программами-просмотрщиками. Поэтому если туда вставить какую-либо информацию, то это никак не отразится на внешнем виде картинки, и фактически, скажется только на объеме результирующего файла. Эта методика может быть применена ко всем типам файлов, которые имеют блочную структуру: блок данных и блок служебной информации, который не воспринимается просмотрщиками или специализированными программами, работающими с данным типом файлов. Данный метод скрытия данных достаточно легко выявляется программами-анализаторами.

Метод замены младших битов (LSB метод – Least Signification Bits)

Метод, основанный на замене нескольких младших битов в байтах данных. Применяется для графических файлов, использующих для формирования цвета пикселя значения некоторых составляющих (например, основных цветов – красного, зеленого и синего). LSB метод возможен благодаря тому, что человеческие органы чувств неспособны различать незначительные искажения. Однако, следует учесть, что фактически неизвестно, что будет стоять в младшем значащем разряде

цифрового представления данного цвета. Данный метод не увеличивает размеров файла-контейнера и позволяет сохранять достаточно большой объем информации, порядка 40% от объема файла. Выявления факта скрытия информации достаточно сложно как программами анализаторами, так и человеком. Следует уточнить, что применение LSB-метода ограничено растровыми форматами, использующими сжатие без потери качества (например RLE- или LZW-сжатие).

Метод замены цветовой палитры

Данный метод предназначен для сокрытия текстовой информации в графических файлах, использующих цветовые палитры. В качестве контейнера, в данном случае, следует выбирать файлы, содержащие некоторый цвет в избытке. Например, это могут быть схемы, рисунки или отсканированный текст черного цвета на белом фоне. Такое сочетание цветов вообще является оптимальным для использования данного метода, поэтому описание будет приводиться на этом примере (хотя, по аналогии, можно использовать любые цвета). При применении данного метода к двухцветным контейнерам объем скрываемой информации равен количеству точек, т.е. площади картинки. Это один из самых емких методов сокрытия информации в графических файлах, который позволяет оставлять картинку без изменения качества и объема. Однако данный метод достаточно легко выявляется средствами программного стеганоанализа.

Метод сортировки палитры

В данном методе, как и в предыдущем, в качестве контейнера используются файлы с индексированными цветами, содержащие монохромное (обычно градации серого). Суть метода заключается в предварительной подготовке файла – контейнера. Палитра файла упорядочивается таким образом, чтобы цвета с соседними номерами минимально отличались друг от друга и равномерно изменялись от черного цвета для 0-го номера до белого цвета для 255-го номера. После этого скрываемое сообщение привносится в младшие биты точек изображения, то есть искажаются номера цветов, а не сами цвета, но благодаря предварительно отсортированной палитре цвет точки заменяется на похожий. Следует отметить, что данный метод также достаточно легко выявляется средствами программного анализа.

Скрытие информации в JPEG файлах

Несколько особняком среди растровых графических форматов стоит формат JPEG. Главной особенностью файлов JPEG является то, что изображение в них сжимается с потерями, для чего используется метод дискретного косинусоидального преобразования DCT, перево-

дящий преобразование растровых данных в информацию об интенсивности изменений. Затем квантование округляет результаты DCT, приводя их в меньший диапазон величин. Это шаг, на котором JPEG получает потери; коэффициенты квантования просто определяют, какое количество данных теряется и, следовательно, определяют диапазон сжатия и качество восстановленного изображения. И, наконец, для получения окончательного результата, выходные данные квантования сжимаются с использованием либо кодирования Хаффмана, либо арифметического кодирования. Скрытие информации в файлах JPEG возможно либо путем изменения числа квантования, либо использования таблицы квантования DQT. Однако все эти методы характеризуются малым количеством скрываемого изображения и обычно используются для нанесения различных «водяных знаков».

ЛИТЕРАТУРА

1. *Соколов А.В., Степанюк О.М.* Защита от компьютерного терроризма. Справочное пособие. СПб.: БХВ-Петербург Арлит, 2002. 498 с.
2. *Суть* стеганографии // http://www.fedchuk.ru

ДЕЙСТВИЕ ПРОГРАММНЫХ ЗАКЛАДОК ТИПА «ТРОЯНСКИЙ КОНЬ»

С.Н. Филькин, студент 3 курса каф. КИБЭВС
ТУСУР, г. Томск, tiere@ngs

Закладка типа «троянский конь», как видно по названию, представляет собой программу, которая на первый взгляд абсолютно безвредна, но имеет скрытую функцию, способную нанести вред компьютеру. «Троянский конь» обычного типа часто распространяется по электронной почте с целью скопировать пароль доступа компьютера, а затем пересылает украденные данные анонимному получателю. Троянской программой, также может быть программа с известными пользователю свойствами, в которую были внесены изменения, чтобы помимо известных функций она могла втайне от него выполнять некоторые разрушительные действия.

В общем случае действия троянской программы могут быть любыми – от определения регистрационных номеров программного обеспечения, установленного на компьютере, до составления списка каталогов на его жестком диске. А сама троянская программа может маскироваться под текстовый редактор, под сетевую утилиту или любую программу. «Трояны» написаны для всех операционных систем и представляют значительную угрозу компьютерам, поскольку их дейст-

вия могут носить не только деструктивный характер, но и сбор конфиденциальной информации о системе. Обнаружить такие троянские программы удается, как правило, чисто случайно.

«Трояны» делятся на 3 типа:

1. Key Logger
2. E-mail trojan
3. Back Door

Key Logger

Злоумышленник отсылает кому-нибудь «Троян». «Троян» записывает все нажатые им в оффлайне клавиши и, когда он подсоединяется к Интернету, высылает их на mail злоумышленника. Это самый примитивный вид «Троянов», но очень действенный, когда жертва при соединении с интернетом не ставит галочку на «Запомнить пароль».

E-mail trojan

Принцип тот же. Только программа не записывает нажатые клавиши, а высылает злоумышленнику все пароли, которые найдет у жертвы.

Back Door

Это самый популярный на данное время вид «Троянов». Обычно он состоит из 3 файлов: Client, Server и Editserver. Главная цель настройки «трояна» – это получить IP жертвы, который отсылается на mail, указанный в настройках закладки. После отправки обязательно нужно, чтобы атакуемый его запустил, а он это сделает, если у него не выдается сообщение, что это вирус. Когда атакуемый запустит троян, он автоматически копируется в систему и прописывается в реестре. Таким образом, «троян» будет запускаться при каждом входе в Windows и жертва не сможет его удалить. Когда атакуемый подключается к Интернет, злоумышленник заходит в client, для этого он тоже должен зайти в сеть и набирает IP жертвы. Если IP правильный, то злоумышленник у него в компьютере, а тогда он может сделать практически все, вплоть до удаления содержания Flash-BIOS. Разрушительные последствия этого вполне понятны.

Методы защиты от троянских программ:

1. Запрещение запуска файлов – успешно работает против абсолютного большинства ныне действующих «троянов».

2. Блокирование связи «трояна» с автором. Если известно с каким «трояном» атакуемый имеет дело, то этот «троян» может просто скачать из Интернета и подсоединиться к себе самому по адресу 127.0.0.1. Дальше нужно найти там опцию типа: remove server, kill server или delete server. Если даже зараженный файл и останется, то он не будет больше угрожать, и можно без проблем его удалить.

Несмотря на простоту этого способа, могут возникнуть проблемы. При попытке соединиться с собой, «троян» может спросить пароль на соединение с сервером, а без него никак нельзя. Тогда нужно просто войти в сервер скаченного «трояна». Он скопируется в систему, и, как правило, заменит собой уже имеющийся «троян».

3. Использование программ для удаления «троянов» из реестра Windows(TrojanCleaner, AVTrojan, BackWork и т.д.).

ЛИТЕРАТУРА

1. *Соколов А.В., Степанюк О.М.* Защита от компьютерного терроризма. Справочное пособие. СПб.: БХВ-Петербург Арлит, 2002. – 498 с.
2. *Классификация* вредоносных программ // http://z-oleg.com

ПРОГРАММА ФОРМИРОВАНИЯ ПИСЕМ «AUTOSETUP» ДЛЯ УПРАВЛЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ В СИСТЕМЕ ЭЛЕКТРОННАЯ ОТЧЕТНОСТЬ ПО КАНАЛАМ СВЯЗИ

В.А. Холодков, студент 5 курс каф. КИБЭВС;
Р.В. Мещеряков, к.т.н., доцент каф. КУИБЭВС
ТУСУР, г. Томск, т. 416-000, vah@ctb.rk.tusur.ru

1. Система электронной отчетности по каналам связи

Система формирования и сдачи налоговой и бухгалтерской отчетности в электронном виде по каналам связи (далее система ЭОКС) представляет собой совокупность программно-аппаратных средств, принадлежащих налогоплательщикам, налоговым органам и специализированному оператору системы, а также совокупность документов, регламентирующих взаимоотношения участников системы. Существует программный комплекс «Спринтер», который разработан в рамках этой системы. Он обеспечивает автоматизированное формирование документов бухгалтерской и налоговой отчетности и доставку их в налоговые органы с использованием защищенной электронной почты.

Главной функцией системы ЭОКС является осуществление обмена открытой и конфиденциальной информацией между налогоплательщиками и налоговыми органами, в том числе при передаче подписанных электронной цифровой подписью и зашифрованных электронных документов, содержащих данные бухгалтерской и налоговой отчетности или сведения об исполнении налоговых обязательств перед бюджетом. Для своевременной замены ключевой информации во избегания конфликтных ситуаций связанных с однозначной идентифика-

цией абонентов системы – отправителей электронных документов, разработана программа «Create AutoSetup».

2. Назначение программы «Create AutoSetup»

Программа «Create AutoSetup» написана в визуальной среде программирования Borland Delphi 7, предназначена для формирования письма «AutoSetup», содержащего ключевую и регистрационную информацию абонента которую необходимо заменить на рабочем месте налогоплательщика в программе Dipost. Если абонент присутствует в программе Dipost, то меняется старый открытый ключ на новый, если абонента нет в программе Dipost у налогоплательщика, то абонент добавляется. Программа применяется для замены (добавления) информации об участниках системы ЭОКС: ИФНС, специализированного оператора системы ЭОКС, ПФР.

3. Общие принципы функционирования

Письмо «AutoSetup» – представляет два файла с одинаковым расширением:

1. ectdd.??? – «Конверт» письма «AutoSetup». Содержит следующую информацию:

– дата формирования письма;

– адрес отправителя;

– адрес получателя;

– темы письма;

– название ящика в программе Dipost, с которого будет отправляться данный файл

– информацию о подклеенном файле

2. fctdd.??? – «Тело» (подклеенный файл) письма «AutoSetup». В этом файле содержится ключевая и регистрационная информация абонента которую необходимо заменить (добавить) на рабочем месте налогоплательщика, а именно:

– Наименование абонента

– Адрес электронной почты в системе ЭОКС

– Сертификат открытого ключа абонента в MIME-кодировке

Программа «Create AutoSetup» использует регистрационную информацию из баз данных Microsoft Access 97, которые входят в состав программы Офисный Модуль Провайдера (ОМП) предназначенной для: регистрации абонентов системы ЭОКС; создания необходимых документов для подключения абонентов; формирования настроечных дискет для настройки программы Dipost на рабочем месте налогоплательщика. Программа «Create AutoSetup» обращается к базе OMP_CurrentUsers.mdb либо OMP_NewUsers.mdb в зависимости от информации необходимого абонента для формирования письма. Все

абоненты после регистрации в системе ЭОКС делятся на группы «Получатели» – ИФНС, ПФР и «Отправители» – налогоплательщики.

Программа позволяет формировать письма в двух направлениях для связи абонентов системы ЭОКС. Например, при подключении абонента для отправки пенсионной отчетности в Пенсионный фонд необходимо создать письмо «AutoSetup» для пенсионного фонда с регистрационной и ключевой информацией абонента и соответственно для этого абонента письмо «AutoSetup» с регистрационной и ключевой информацией пенсионного фонда.

В программе реализована функция сортировки абонентов по наименованию или по адресу электронной почты в системе ЭОКС, что увеличить скорость поиска необходимой информации.

Предусмотрена и реализована функция группового создания писем «AutoSetup». Например, при замене ключевой информации у ИФНС, с помощью этой функции можно создать сразу все письма «AutoSetup» для абонентов данной инспекции, используя функцию сортировки по адресу электронной почты.

ЛИТЕРАТУРА

1. *Программный* комплекс «Спринтер» системы электронной отчетности по каналам связи.
2. *Руководство* пользователя программного комплекса «Спринтер».
3. www.taxcom.ru

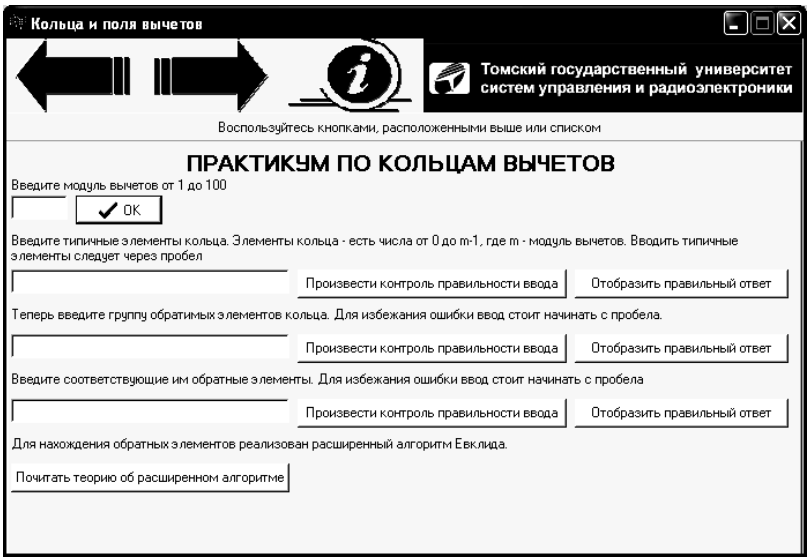
АВТОМАТИЗИРОВАННАЯ ОБУЧАЮЩАЯ СИСТЕМА ПО ДИСЦИПЛИНЕ «СПЕЦИАЛЬНЫЕ ГЛАВЫ ВЫСШЕЙ МАТЕМАТИКИ»

М.В. Ильенко, С.К. Росошек, студенты 2 курса ФВС
ТУСУР, г.Томск, marishail@yandex.ru

В процессе обучения в 3-м семестре по специальности «Комплексное обеспечение информационной безопасности» студентам необходимо изучить дисциплину «Специальные главы высшей математики. Математические основы криптографии». Так как в процессе обучения студентам приходится сталкиваться с различного рода проблемами в понимании и усвоении огромного количества информации, мною была рассмотрена проблема автоматизации обучения данной дисциплине.

Программа обучения данной дисциплине является продолжением курса математической логики и теории алгоритмов и подготавливает студентов к изучению важных в их специальности дисциплин, таких как криптографические методы защиты информации.

Для того чтобы студенты могли изучать специальные главы не только в стенах университета при непосредственном участии преподавателя, но и дома, например при дистанционном обучении, была создана представленная обучающая система.



Вид одной из страниц программы

Обучающая система построена таким образом: сначала студенту предлагается для изучения теоретический материал. После его прочтения студент может перейти к практической части обучения. Это позволит преподавателю рассматриваемого курса легче организовывать работу студентов на практических занятиях. Задания, подобранные преподавателем, реализованы в программе таким образом, что студент, выполняющий задание не может перейти к следующему заданию, а, следовательно, и к следующей части курса, не изучив предыдущую, и не выполнив все предложенные задания. Практическое задание может быть автоматически выбрано компьютером из уже имеющихся, или введено студентом со слов преподавателя.

После изучения каждой главы студентам предлагается пройти контроль знаний, представленный в виде набора практических заданий, ранее рассматриваемых в течение изучения главы. Контроль правильности выполнения таких контрольных работ может произвести только преподаватель, предварительно введя пароль. Данные в поля

ввода при выполнении контрольной работы можно вводить только один раз.

В системе обучения существует также возможность выполнения домашнего задания и записи его в файл, который потом можно загрузить в программу и проверить правильность выполнения предложенного преподавателем задания.

Таким образом, внедрение этой автоматизированной системы для обучения студентов на кафедре КИБЭВС позволит преподавателям уделить больше времени теоретическому рассмотрению курса, вести непосредственный контроль успеваемости каждого студента.

ИДЕНТИФИКАЦИЯ АВТОРА НЕИЗВЕСТНОГО ТЕКСТА

А.С. Коботаев, студент 3 курса; М.М. Саматов, студент 3 курса; С.И. Боровков, студент 3 курса каф. КИБЭВС

ТУСУР, г. Томск, a111_666@mail.ru

Цель работы – реализация и исследование алгоритма идентификации автора неизвестного текста.

С появлением компьютеров и увеличением объемов хранимой в электронном виде текстовой информации открываются новые возможности для исследования литературы и языка. Компьютер, способный автоматически обрабатывать большие объемы информации позволяет широко применить статистические методы в лингвистике и литературоведении. Применить математический аппарат для решения задачи установления авторства впервые предложил, в 1851 г., английский логик Август де Морган. С тех пор было разработано множество методов как статистических, так и опирающихся на разработки в области искусственного интеллекта и, несмотря на произошедшие изменения в методиках и инструментах, суть проблемы остается прежней: по каким-либо статистическим характеристикам текста необходимо установить, кто является его автором.

Задача установления авторства текстов с заданным набором альтернатив формулируется следующим образом: дан некий текст и задано множество авторов, один из которых является автором этого текста. Необходимо определить принадлежность авторства. Подобная формулировка предполагает, что известен некий набор альтернатив, среди которых производится выбор, и этот выбор всегда сходится к одной из этих альтернатив.

Основным предположением, без которого бессмысленно говорить о задаче автоматического определения автора текста, является то, что

любой авторский текст обладает определенным набором свойств, уникальных для данного автора. Эти свойства вносятся неосознанно, независимо от желания писателя, и поэтому они являются индивидуальной характеристикой конкретного автора.

Сложность определения автора заключается в нахождении характеристик, отражающих авторский стиль, а так же правильность их интерпретации. В качестве таких характеристик могут браться различные параметры текста. Одними из возможных являются различные частотные характеристики, такие как, например, частота встречаемости служебных слов, количество абзацев, количество предложений определенной длины, количество слов в предложении и т. д. Состоятельность выбранной характеристики, на сегодняшний день, может быть определена только экспериментально.

После того, как исследователь определился с характеристиками, на основе которых будет строиться вывод об авторстве текста, необходимо определить, каким образом сделать этот вывод. Для принятия решения об авторстве на основе характеристик текста, как правило, используют следующие группы методов:

1. *Статистические методы* основываются на достижениях современной математической статистики и сводятся к определению того, насколько значимо отличаются характеристики текста, авторство которого необходимо определить, от уже известных характеристик для данного автора. Как вариант может проводиться сравнение характеристик текстов, автор которых неизвестен, и ставится задача определить, написаны ли эти тексты одним автором или разными.

2. *Методы искусственного интеллекта* используют такие методики как нейронные сети, которые, обучившись на некоторых входных данных, способны далее самостоятельно принимать решение о принадлежности предъявленного текста перу того или иного автора. Эти методы, обычно, более универсальные и гибкие, а также более простые с математической точки зрения, чем статистические. Кроме того, они обладают способностью к обучению, чего лишены большинство статистических методов. Однако методы искусственного интеллекта обладают двумя большими недостатками. Во-первых, это отсутствие строгого математического обоснования используемых методик. Для искусственных нейронных сетей доказана теорема Колмогорова, но она говорит лишь о возможности представления нейронной сетью любого отображения, но не дает конкретных рекомендаций относительно необучаемых (число нейронов, число слоев, вид активационной функции) параметров сети, которые в большинстве случаев приходится подбирать и подтверждать экспериментальным путем.

В данной работе будут реализованы методы искусственных нейронных сетей. Достоинством искусственных нейронных сетей является достаточно высокая точность классификации.

Идея использования искусственных нейронных сетей в задаче определения авторства текста состоит в том, чтобы подавать на вход сети специально отобранные характеристики текста, а на выходе получать вектор, описывающий принадлежность текста к тому или иному автору. Для этих целей больше всего подходит архитектура «многослойный перцептрон», которая и используется в большинстве случаев.

На задаче классификации текстов по количественным признакам нейронные сети превосходят другие методики по эффективности, но при этом их настройка занимает не мало времени.

Итогом данной работы будет разработанная программа, определяющая автора входного текста, из множества уже известных программе авторов, с применением алгоритмов на искусственных нейронных сетях. Для расширения множества авторов необходимо обучить нейронную сеть, указав тексты добавляемого автора.

ЛИТЕРАТУРА

1. http://soft.neurok.ru/pub/lectures.shtml
2. *От Нестора* до Фонвизина. Новые методы определения авторства. М.: Издат. Группа Прогресс, 1994.

ПРОБЛЕМА ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Н.А. Кокорева, студентка гр. 522-1 ФВС
ТУСУР, г. Томск

В настоящее время вопросам обеспечения безопасности информации уделяется все большее и большее внимание. Это связано с тем, что информация в жизни общества, в эффективном функционировании организации играет важную роль, а в некоторых случаях и определяющую. Так, по оценкам специалистов в области информационной безопасности следует, что если организация допускает утечку 20 и более процентов важной информации, то такая организация в 60 случаях из 100 банкротится. Поэтому экономически развитые страны в настоящее время тратят большие деньги на обеспечение безопасности, в том числе и информационной. Так, например, на содержание службы безопасности эти страны сегодня тратят в среднем до 25% годовой прибыли в год. У нас организации расходуют на эти цели менее 1%.

Процесс защиты представляет собой комплексное проектирование системы информационной безопасности, а после ее внедрения аттеста-

цию системы и проверку адекватности предложенных средств. К сожалению, в наших условиях очень часто развитие системы происходит хаотически. При этом важную роль играет уверенность в правильности применяемых частных решений по защите информации, как с точки зрения непосредственно возложенных на них задач, так и с точки зрения их соответствия ближайшим и более отдаленным перспективам развития ИС.

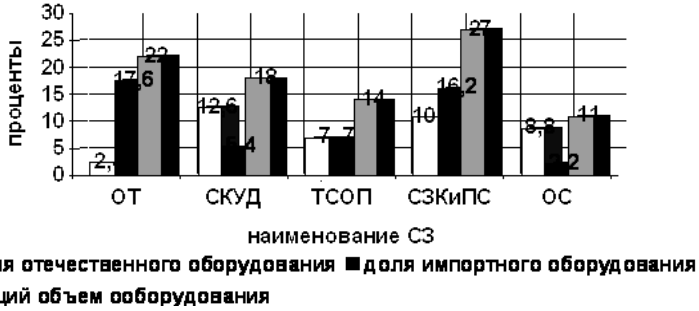
Я считаю, что одним из сложных этапов проектирования системы информационной безопасности является выбор средств защиты. Рано или поздно выясняется, что для организации охраны того или иного имущества и построения надежной системы безопасности необходимо подобрать технические средства, значит, нужна самая последняя и полная информация в области современных технологий, а ее, как правило, не хватает. Дело в том, что рынок информационных технологий, вследствие высочайших темпов его развития, находится под мощным воздействием маркетинговых механизмов, которые способны дать искаженное представление о свойствах продукта и критериях выбора. Таким образом, можно сказать, что при получении информационных и маркетинговых материалов от разработчиков или поставщиков необходимо, в первую очередь, выявить базу критериев, по которым оценивается то или иное средство защиты. Эти критерии можно разделить на два типа: общие критерии для средств защиты информации, такие как собственная защищенность, производительность, сертификация, стоимость; и функциональные критерии, зависящие от каждого конкретного средства. Отсутствие в информационных и рекламных материалах основных критериев или ввод лишних, незначительных позволяет судить об истинных качествах предлагаемого средства и достоверности маркетинговых заявлений.

Чтобы не допустить ошибки при выборе средств защиты и знать, на что именно обращать внимание при ознакомлении с маркетинговыми заявлениями необходимо определить требования к этим средствам. Основой такого определения должна быть следующая позиция: все средства защиты всего-навсего предоставляют собой инструментарий для реализации политики безопасности – набор управленческих решений, направленных на защиту информации, и установленных на их основе правил работы пользователей и администраторов ИС. Поэтому основные вопросы при выборе того или иного средства защиты информации должны звучать приблизительно так:

- для чего будет применяться средство?
- от каких угроз это средство будет ограждать, и в какой степени?
- какие правила работы с информационными ресурсами будут (могут быть) реализованы?

Помимо всего этого придется делать выбор в пользу импортного или отечественного средства. И не стоит выбирать российские марки только для того, чтобы поддержать отечественного производителя.

Хотелось бы обратить внимание на общий объем рынка технических средств. По оценкам, содержащимся в различных источниках информации, общий объем рынка технических средств безопасности в России на 2004 г. составил по порядку величины несколько сот миллионов долларов.



Объем рынка технических средств

Из них:

- охранное телевидение (ОТ) – 22% (доля импортного оборудования до 80%);
- системы контроля и управления доступом (СКУД) – 18% (доля импортного оборудования составляет до 30%);
- ТС охраны периметра (ТСОП) – 14% (доля импортного оборудования до 50%);
- системы защиты от краж и пожарные сигнализации (СЗКиПС) – 27% (доля импортного оборудования до 60%);
- охранные сигнализации (ОС) – 11% (доля импортного оборудования – до 20%).

Следовательно, одной из главных проблем, на мой взгляд, является выбор комплекса средств защиты. Этот комплекс не должен содержать средства, отвечающие за ликвидацию одной и той же угрозы – это может привести к неоправданным расходам. Помимо этого, нельзя оставлять без внимания угрозу с наименьшей вероятностью возникновения, иначе эффективность защищенной системы снизится до нуля.

Надо помнить всегда о том, что невозможно создать абсолютно надежную систему безопасности. В основном из-за того, что постоянно разрабатываются новые виды угроз, которым система не сможет противостоять, а также из-за того, что эффективность системы защиты зависит от обслуживающего персонала, а человеку свойственно ошибаться.

КАК МОЖНО ЗАЩИТИТЬ СВОЙ ОФИС ОТ ПРОСЛУШИВАНИЯ СВОИМИ СИЛАМИ

Н.А. Кокорева, студентка гр. 522-1 ФВС
ТУСУР, г. Томск

Электронная слежка противоречит российскому законодательству, это закреплено в соответствующих законах РФ. Несмотря на то, что существующие законы запрещают продажу и использование средств негласного съема информации, рынок ими, буквально, наводнен. Жучок можно купить на радиорынке, в салонах спецсредств (минуя официальную процедуру), заказать по Интернету или спаять самому. Стоимость самоделки, обычно, не превышает 1000 рублей вместе с приемником. А работают они ничуть не хуже промышленных изделий. Как защититься от прослушивания? Можно пригласить для обследования помещения специалистов. Как правило, стоимость «зачистки» помещения зависит от площади пола помещения. Расценки составляют в среднем от 10 до 25 долларов за квадратный метр. Проверяется все: пол, стены, потолок, предметы интерьера, строительных конструкций. Отдельно расценивается проверка телефонных линий и техники, подлежащей вскрытию: телефонных аппаратов, телевизоров, компьютеров и т.п.

Если же в силу ряда причин нет возможности пригласить специалистов, то вполне можно обойтись своими силами.

Самым эффективным подслушивающим устройством сегодня признан радиомикрофон. Это миниатюрный радиопередатчик, объединенный с микрофоном. Размеры радиомикрофона очень малы, но независимо от этого процесс установки весьма трудоемкий. Для этого требуется проведение целого ряда мер: предварительная разведка (изучение объекта, подходов, персонала) и определение метода заноса «жучка» в помещение. Маскировать «жучки», благодаря малым размерам, можно подо что угодно – от корзинок с цветами до настольных часов. Но чаще используют различные брусочки, палочки, которые легко подбросить под шкаф или тумбочку или сунуть в нишу стола.

Поскольку радиус действия «жучков» невелик, отсюда следует эффективный метод защиты от них. Необходимо вести конфиденциальный разговор на фоне музыки или постороннего акустического шума, это существенно затруднит подслушивание.

Еще один метод защиты связан с так называемым человеческим фактором. Если угроза подслушивания существует, необходимо установить режим пользования помещением. Посторонние люди – посетители, уборщица, представители ремонтных служб – не должны находиться одни в помещении для переговоров. При них должен быть человек, которому можно доверять. На ночь и в выходные помещение

должно опечатываться, а ключи – сдаваться в специальном пенале под подпись. В случае ЧП (прорыва водопроводных труб, неполадок с электропроводкой, угрозы пожара) вскрытие помещения должно производиться в присутствии представителя организации.

Еще один распространенный метод электронной слежки заключается в подслушивании телефонных переговоров. Обычный телефон – самый ненадежный элемент в системе информационной безопасности. Эксперты утверждают, что защитить телефонную линию от прослушивания практически невозможно. Причина кроется в легкости доступа к телефонным линиям на всем протяжении от объекта до телефонной станции. Единственный реально работающий способ представляет собой использование устройств, шифрующих телефонные переговоры, – скремблеров. Правда, они должны находиться у каждого, с кем ведутся важные разговоры. Если же необходим радиотелефон, эксперты рекомендуют использовать цифровые телефоны стандарта DECT, использующие алгоритмы шифрации, в свое время разработанные для военных нужд. Их использование резко снижает возможность радиоперехвата.

В таблице для ознакомления предоставлены основные сведения о таких устройствах.

Характеристика детекторов жучков

Название	Характеристика	Стоимость на 09.03.06 г. в рублях
«Antibug-Base»	Вес: 60 г. Размер: 60 × 15 мм. Производитель: Япония. Оптимальная модель для повседневного использования. Наличие антенн позволяет быстро определять точное место расположения «жучка»	3000
«Antibug–Business»	Диапазон частот: 50 – 3000 МГц. Питание: 2 × CR2032. Вес: 28 г. Размер 78 × 28 × 14 мм. Производитель: Тайвань	4500
«Antibug-Profi»	Диапазон частот: 10 – 3000 МГц. Питание: 9V (Крона). Вес: 280 г. Размер:138×75×22 мм. Производитель: Тайвань. Имеет внешнюю антенну, сегментный индикатор уровня сигнала и плавную регулировку чувствительности	6000

Конечно, существуют и другие технические средства подслушивания, гораздо более изощренные. Их называют «беззаходными», то есть не требующими проникновения на объект. Например, системы лазерного съема аудиоинформации с окон. Принцип работы лазерной системы таков. Любое акустическое колебание, создаваемое в помещении, приводит к колебаниям оконных стекол. Если направить лазер на поверхность такого стекла и принять отраженный от него модулированный луч, то он будет содержать в себе речевую информацию. Ее можно декодировать и услышать, о чем говорят за окном. Для того чтобы воспользоваться такими устройствами, нужно соблюсти ряд очень трудновыполнимых условий. Нейтрализовать «лазерную» угрозу просто. Можно создать, например, вибропомеху на поверхности стекол с помощью специальных устройств. Есть и более дешевый метод – повесить между стеклами непрозрачную шторку.

Еще один прогрессивный метод подслушивания основан на использовании стетоскопа (контактного микрофона). Он прикладывается к стене, и с его помощью можно услышать, о чем за ней говорят. Такие приборы изготавливаются на основе пьезокерамики, обладающей свойством преобразовывать механические колебания в электрические, которые затем усиливаются. Принцип работы пьезостетоскопа основан на восприятии виброколебаний стены. Лучшей звукопроникающей способностью обладают бетон или кирпичная кладка. Но если в стене есть воздушная прослойка, например обрешетка или стекловата, стетоскоп бессилен.

Нейтрализовать угрозу подслушивания можно еще одним путем: приобрести простые индикаторы электромагнитного поля и самостоятельно проверять помещения на наличие подслушивающих устройств.

Но все же самый надежный метод защиты – не болтать по телефону о делах, представляющих интерес для конкурентов.

Перечень методов обнаружения закладочных устройств и защиты от них без помощи специалистов не исчерпывается описанными в данной статье. Кроме того, специалистами разрабатываются новые методы поиска, появляются новые более совершенные поисковые приборы.

ОБЗОР УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ RSA KEON и КРИПТО-ПРО

С.И. Коковин, студент 4 курса; В.Д. Зыков, студент 4 курса
ТУСУР, каф. КИБЭВС, г. Томск, ksi@ms.tusur.ru

В настоящее время наблюдается заметно растущая тенденция использования государственными и коммерческими организациями сети

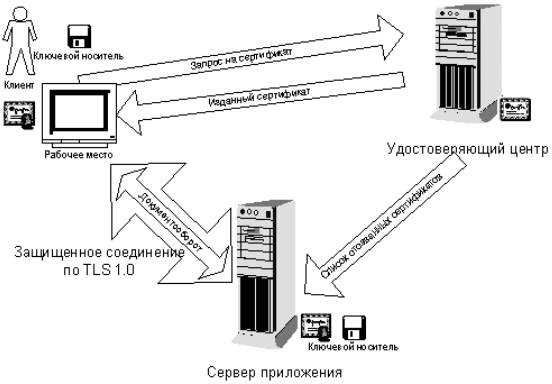
Интернет в качестве средства передачи данных. Однако вместе с положительными результатами такого перехода разработчики, владельцы и пользователи информационных систем неизбежно сталкиваются с проблемами защиты информации при ее передаче по общедоступным каналам связи. При этом первостепенную важность приобретает решение следующих трех основных задач:

- обеспечение конфиденциальности передаваемой информации;
- обеспечение целостности информации;
- обеспечение авторства электронных документов.

Для решения этих задач в последние десятилетия наибольшую популярность приобретает Инфраструктура отрытых ключей (Public Key Infrastructure, PKI). Данная инфраструктура представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих шифрование с открытым ключом, а также для управления ими. Программные комплексы, реализующие функции PKI получили наименование «удостоверяющих центров» или УЦ (Certification Authority, CA).

Из существующих на рынке УЦ можно выделить два продукта, наиболее распространенных в России:

- «Крипто-Про УЦ» – Крипто-ПРО;
- «RSA Keon» – RSA Security;



Принципиальная схема работы УЦ

Программный пакет RSA Keon фирмы RSA Security отличается модульностью, гибкостью и широкой совместимостью.

RSA Keon CA является мощным средством для подписания сертификатов пользователей и системных событий, а также выполняет функцию интегрированного хранилища сертификатов, данных о системных событиях и информации о статусе сертификатов. RSA Keon

CA может публиковать списки в любой LDAP-совместимый каталог или внешнюю базу данных для хранения сертификатов, и имеет встроенный модуль запрашивающий CRL непосредственно у УЦ (респондер), поддерживающий стандартный протокол онлайновой проверки статуса сертификатов (Online Certificate Status Protocol – OCSP).

С помощью решения RSA Keon CA можно создать удостоверяющий центр практически любого масштаба или объединить существующие удостоверяющие центры других производителей в более крупную инфраструктуру. RSA Keon CA основан на открытых стандартах и совместим с подавляющим большинством индустриальных систем и приложений. RSA Keon CA может создавать и поддерживать сертификаты и их расширения, основанные на стандарте X.509. С декабря 2002 г. в RSA Keon CA встроена поддержка криптопровайдера CryptoPro CSP, разработанного компанией Крипто Про и имеющего сертификат ФАПСИ.

Удостоверяющий центр RSA Keon CA поддерживает все три модели PKI (иерархическую, сетевую и гибридную). Кроме того, он позволяет изменять уже созданную инфраструктуру.

Центр регистрации (ЦР) RSA Keon RA имеет ту же архитектуру и выполняет те же функции, что и CA, за тем лишь исключением, что он не может подписывать сертификаты пользователей. Одобренные сертификаты выдаются пользователю либо Удостоверяющим, либо его Регистрационным центром.

Программный комплекс «Крипто-Про УЦ» фирмы Крипто-Про является специализированным программным комплексом, успешно прошедшим сертификационные испытания на предмет соответствия реализуемых функций функциям Удостоверяющего Центра, изложенным в Федеральном законе «Об электронной цифровой подписи» и требованиям по информационной безопасности по классу защиты «КС2».

Этот комплекс предназначен для выполнения организационно-технических мероприятий по обеспечению пользователей Удостоверяющего Центра как организации средствами и спецификациями для использования сертификатов открытых ключей в целях:

- контроля целостности передаваемых электронных документов;
- контроля целостности публичных информационных ресурсов;
- проверки подлинности взаимодействующих программных компонентов и конфиденциальности передаваемых данных;
- создания системы юридически значимой электронной цифровой подписи в системах электронного документооборота;
- обеспечения безопасности и разграничения доступа при взаимодействии субъектов АИС;

• создания иерархической системы управления ключами подписи субъектов АИС.

В состав программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» входят следующие программные компоненты:

Центр сертификации, предназначенный для формирования сертификатов открытых ключей пользователей и администраторов УЦ, списков отозванных сертификатов (Certification Revocation List, CRL), хранения эталонной базы сертификатов и CRL;

Центр регистрации, предназначенный для хранения запросов на сертификаты и сертификаты пользователей, а также для обеспечения интерфейса между УЦ и пользователями;

АРМ администратора;

АРМ разбора конфликтных ситуаций.

В качестве средства, реализующего криптографические функции (средства ЭЦП) используется КриптоПро CSP, разработанный в соответствии с Microsoft – Cryptographic Service Provider (CSP).

Заключение

В связи с тем, что все большее число правительственных организаций и крупных предприятий вводят в эксплуатацию УЦ для обеспечения криптографической защитой внутрикорпоративного документооборота, и защищенного документооборота при сдаче налоговой и иной отчетности через Internet, развитие инфраструктуры открытых ключей будет постоянно расширяться. На российском рынке прочные позиции занимает комплекс Крипто-Про и в 2004 году фирма Крипто-Про вошла в двадцать самых успешных предприятий в области обеспечения информационной безопасности, это дает повод полагать, что именно этот продукт будет использоваться в подавляющем большинстве случаев в ближайшее время.

СИСТЕМА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ФАЙЛАМ «ХАМЕЛЕОН»

А.С. Конончук, студент 3 курса каф. КИБЭВС
ТУСУР, г. Томск, lgamm@mail.ru

Одной из важных задач защиты информации является защита от несанкционированного доступа. На сегодняшний день существует множество средств защиты от НСД, такие как: DeviceLock – ЗАО «ДиалогНаука», Аккорд – ОКБ САПР, ШИПКА – ОКБ САПР и др.

Предлагаемая система защиты то НСД «Хамелеон» нацелено на обеспечение защиты от несанкционированного копирования информации, несанкционированного доступа к информации, хищения носителя защищаемой информации, несанкционированный физический доступ на объект информации в соответствии с ГОСТ Р 51275-99.

Принципы работы системы

Система, при указании защищаемого файла, вырезает из него 64-128 кБ, выбирая размер вырезаемой части случайным образом. При этом комбинации сочетаний вырезаемых битов варьируются от единичного бита в секторе до четырех вместе взятых секторов случайным образом. Кластеры, содержащие вырезаемые биты очищаются двойной записью в них случайных данных. При удалении бит система защиты сохраняет их относительные адреса. Затем система записывает вырезанные биты (далее ключевые) в некоторые (выбранные случайным образом) кластеры съемного носителя (дискета 3,5 либо USB Flash Disc), с последующим проверочным трехкратным чтением, и сохраняет уникальный идентификационный номер носителя, в файловой системе носителя не делается никаких отметок о записанных данных (они определяются как пустые). При хотя бы одной ошибке при проверочном чтении битов ключевого носителя система помечает их как не пригодные и использует только для записи маскирующих битов, процедура выбора физических адресов и записи с последующим проверочным чтением повторяется. Далее система сохраняет физические адреса ключевых битов на носителе. После чего остальная часть памяти носителя записывается маскирующими битами. Затем процедура установки защиты завершается.

При обращении к файлу управление передается системе защиты, которая в свою очередь проверяет уникальный номер носителя и загружает ключевые биты с внешнего носителя в оперативную память, проверяет электронную подпись файла и в случае положительного результата по мере исполнения файла восстанавливает его. Далее система следит за стоянием файла в ОЗУ компьютера. При выгрузке файла из памяти система перехватывает управление и вновь выбирает ключевые биты, производит процедуру переноса их из файла на внешний носитель и только потом записывает старые ключевые биты в сам файл. Таким образом, система постоянно контролирует «поврежденность» защищаемого файла на жестком диске и восстанавливает его только в ОЗУ.

Для достижения контроля над целостностью защищаемого файла при его хранении, используется цифровая подпись. Защищаемый файл подписывается каждый раз после окончания записи старых ключевых битов в файл.

Особенности работы системы

Система защиты «Хамелеон» отличается:

- динамичным ключом (формируется случайным образом при каждом завершении работы с защищаемым файлом);
- неработоспособностью защищаемого файла в отсутствии ключа (файл является не полным и восстановлению не подлежит);
- привязанным ключом (имея ключ к одному файлу совершенно невозможно подобрать ключ к другому, так как каждый файл имеет свой набор ключевых бит).

Выводы

Представленная система защиты исключает возможность использования защищаемого объекта без наличия ключевого носителя. Так же исключается возможность подбора или подмена ключевого носителя, так как ключевые биты хранятся по строго указанным адресам и привязаны к уникальному идентификационному номеру носителя. Контроль над целостностью защищаемого файла осуществляется электронной подписью.

Одним из главных вопросов при использовании данной системы является выбор ключевого носителя, так как ключевые биты, хранимые на нем, не подлежат дупликации в целях поддержки уровня защиты самого ключевого носителя. Следовательно, возрастают требования к надежности непосредственно ключевого носителя.

Следует отметить, что для данной системы защиты не предусмотрено применение электронной подписи всего файла, так как принцип работы системы заключается в намеренном контролируемом нарушении целостности защищаемого файла. Поэтому можно говорить только о целостности «поврежденного» файла.

Представленное средство защиты информации не может самостоятельно обеспечить в полной мере высоко уровня защиты, и предназначено для комплексного использования с другими средствами защиты информации.

ЛИТЕРАТУРА

1. ГОСТ Р 51275-99
2. www.antivir.ru
3. www.vniipvti.ru

РАЗРАБОТКА МЕТОДА ЗАЩИЫ ОТ НСД ХРАНИМОЙ И ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

А.С. Конончук, студент 3 курса каф. КИБЭВС
ТУСУР, г. Томск, lgamm@mail.ru

Одним из важнейших вопросов в современных системах защиты информации является защита от НСД. Наибольшее распространение получили методы защиты информации при помощи электронных ключей и электронно-цифровой подписи.

Задачей научной работы является разработка нового метода защиты от НСД хранимой и передаваемой информации, доказывающего наличие альтернативных методов, не использующих шифрование как основу защиты.

В ходе научной работы был разработан метод так называемого Динамического ключа (Dynamic Key). Суть метода заключается в том, что защищаемый объект является полным только в руках законного пользователя, а при передаче либо хранении защищаемой информации объект делится на две части: ключевую и основную. Фактически ключом являются обе части, так как метод деления таков, что невозможно восстановить объект, имея только одну из частей. Основная часть может храниться либо передаваться по открытому каналу. Другая же часть (ключевая) должна быть уже передана заранее либо храниться у законного пользователя на съемном носителе. Особенностью данного метода является то, что разделение полноценного объекта на нефункциональные части, как и его восстановление, должно происходить на низком (аппаратном) уровне. Что гарантирует невозможность восстановления основной части существующими техническими методами в отсутствие ключевой части. Ключевая часть в свою очередь, имея незначительные объемы, может быть замаскирована методами стеганографии. Либо храниться в другом (в случае передачи защищаемой информации пакетами) защищаемом объекте дополнительными битами, вставленными в случайные места. Ключевая часть при каждой операции с защищаемым объектом формируется заново, таким образом можно сказать, что ключевая часть является динамической. Проблема доступа нескольких пользователей к одному защищенному файлу разрешима, достаточно вести поэтапно:

1. запись на все ключевые носители одинаковой ключевой части;
2. при первом использовании текущей ключевой части формирование новой и запись ее (как резервной) на ключевой носитель без удаления из программы.
3. использование первой ключевой части до тех пор, пока на всех ключевых носителях не будет записано новой ключевой части;

4. переход на новую ключевую часть (удаление из объекта битов, соответствующих новой ключевой записи и последующее восстановление битов старой ключевой части);

5. переход ко второму этапу.

Задача системы защиты, основанной на предложенном методе, заключается в исключении целостного состояния объекта в любой момент времени, в который объект не используется законным владельцем.

Представленный метод защиты информации от НСД не использует фактического шифрования защищаемой информации. Принципом, лежащим в основе предложенного метода, является намеренное контролируемое фактическое нарушение целостности защищаемой информации в целях защиты от НСД. Для описания такого решения задачи защиты от НСД следует ввести понятие «условной целостности». Условная целостность говорит о том, что для защищаемой информации состояние целостности является достижимым только во время ее использования. В руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 году, требования к обеспечению целостности программных средств и обрабатываемой информации предъявляются ко всем перечисленным классам защищенности. Следовательно, возникает вопрос о классификации систем защиты информации, использующие условную целостность.

Стоит отметить, что контроль целостности остается необходимым, в целях обеспечения соответствующего уровня защиты автоматизированных систем, для чего требуется применение электронной подписи защищаемой информации. Что указывает на необходимость использования представленного метода в комплексе с различного рода существующими методами и механизмами защиты информации.

Так как предложенный метод не использует фактического шифрования защищаемой информации, возникает вопрос о разработке систем основанных на представленном методе как систем альтернативных криптографическим. Проблема вопроса заключается в том, что предложенный метод не предусмотрен существующими нормативными документами, что приводит к проблеме классификации систем, использующих данный метод.

Подводя итог необходимо отметить, что:

- необходимо исследование возможных способов реализации, для оценки эффективности применения данного метода;
- необходимо пересмотреть классификацию средств защиты информации с учетом возможного применения данного метода и других методов, основанных на данном;

• необходимо определение отношений понятий целостности и условной целостности.

Делая вывод можно сказать, что данный метод требует тщательного исследования и пересмотра существующих взглядов на методы защиты информации от НСД.

ЛИТЕРАТУРА

1. *Руководящий* документ Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации».
2. *Мещеряков Р.В.* Основы информационной безопасности: Методические указания по курсу «Основы информационной безопасности» для студентов специальности «0755 – Комплексное обеспечение информационной безопасности автоматизированных систем». ТУСУР. Томск. Изд-во ТУСУР, 2001.

ЗАДАЧИ, СВЯЗАННЫЕ С РАСПОЗНАВАНИЕМ РЕЧИ, И ОСНОВНЫЕ ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ ПРИ ИХ РЕШЕНИИ

Е.Ю. Костюченко, аспирант каф. КИБЭВС

ТУСУР, г. Томск, т. 8-923-405-55-59, blackimperator@ms.tusur.ru

Проблемы, связанные с распознаванием и машинной обработкой речи берут свое начало еще в 30 годах прошлого столетья. На тот момент необходимо было решать следующие основные задачи:

– фундаментальные (изучение принципов процессов речеобразования и речевосприятия);

– автоматизация управления, связанная с необходимостью освобождения рук оператора от управления автоматизированных процессов.

К 70 гг. XX столетия проблема автоматизации управления была практически полностью решена на том уровне, который был необходим в данное время. Это означало возможность управления процессами при помощи сильно ограниченного простейших команд (например, «вперед», «стоп» и т.д.), однако достаточного для эффективного решения поставленных задач.

Однако, движение науки и техники вперед поставило новые задачи перед исследователями речи. Эти задачи связаны в основном со снятием ограничений, например, управление процессами не только путем жестко ограниченного набора команд, возможность использования их сочетаний, независимость процесса распознавания от голоса, распознавание слитной речи и т.д. Кроме того, все большую значимость стали приобретать задачи, связанные с определением параметров самого диктора (например, определение пола диктора, идентификация диктора).

На настоящий момент времени основные задачи, связанные с распознаванием речи могут быть разделены на следующие группы:

– Распознавание речевого сигнала с целью определения точного способа кодирования;

– Распознавание речевого сигнала с целью определения его смыслового характера;– Распознавание сигнала с целью определения различных характеристик диктора.

Несмотря на большое количество работ, ведущихся в данных направлениях, полученные системы имеют ряд существенных недостатков:

– недостаточная точность распознавания;

– ограниченный объем словаря;

– ограниченное множество дикторов;

– высокая трудоемкость вычислений, невозможность работы в реальном времени.

При распознавании речи могут быть использованы следующие параметры:

– частоты расположения формант;– динамика изменения частоты форманты во времени;

– частота основного тона;

– динамика изменения интенсивности основного тона во времени;

– суммарная энергия спектра речевого сигнала;

– отношения интенсивностей гармоник к интенсивности основного тона;– длительность сегмента;– наличие/отсутствие вокализации на сегменте;– распределение интенсивностей по частотному спектру. Это далеко не полный список параметров, которые можно использовать. Однако, проблемы связаны не только с большим числом параметров, но и с тем, что довольно сложно организовать процесс точного определения этих параметров по речевому сигналу, особенно в реальном времени.

Основная цель данного цикла работ состоит в написании программного обеспечения, способного решать поставленные задачи, а именно осуществлять распознавание речи, проводить поиск слов в слитной речи, осуществлять автоматическую идентификацию диктора, автоматическое выделение параметров диктора, например, пола, дефектов речи, и т.д.

ЛИТЕРАТУРА

1. *Загоруйко Н.Г., Волошин Г.Я.* (ред.) Распознавание слуховых образов. Москва. 1970 г., 338 с.

МЕТОДЫ ОПРЕДЕЛЕНИЯ ИНФОРМАТИВНОСТИ ПАРАМЕТРОВ ПРИ РАСПОЗНАВАНИИ РЕЧИ

Е.Ю. Костюченко, аспирант каф. КИБЭВС
ТУСУР, г. Томск, т. 8-923-405-55-59, blackimperator@ms.tusur.ru

Одна из основных проблем в задачах, связанных с обработкой речи, состоит в том, что анализ сигнала очень часто, если не в большинстве случаев, должен осуществляться в реальном времени.

Сложности здесь возникают уже на этапе выделению ключевых параметров для анализа, поскольку в большинстве случаев это довольно трудоемкий процесс, и требует существенных затрат машинного времена.

Однако, даже после выделения ключевых параметров необходимо осуществить их анализ и по ним принять решение относительно распознавания элемента речи (звука, слога, слова и т.д.) или определения его принадлежности тому или иному диктору, параметров диктора, таких как пол, особенности речи и других. Для этого требуется осуществлять обработку значительного числа выделенных параметров.

Для сокращения времени, затрачиваемого на анализ параметров желательно предварительно произвести их ранжировку по критериям информативности, в зависимости от класса решаемых задач, и при анализе использовать только наиболее существенные из них, а не информативные просто отбросить.

Для этого необходимо определиться с критериями информативности, на основе которых будет осуществляться анализ. В данной работе будут рассмотрены некоторые из них.

1. Критерий Евклида.

Информационная эффективность l-го параметра Q_l определяется как $Q_l = I_l/\gamma_l$

$$I_l = \varepsilon_{\text{ср}}^{(1..l)} - \varepsilon_{\text{ср}}^{(1..l-1)},$$

$$\varepsilon_{ij} = \sqrt{\sum_{l=1}^{n} (\mu_i^{(l)} - \mu_j^{(l)})^2}, \quad \varepsilon_{\text{ср}} = \frac{\sum_{i=j+1}^{k} \sum_{i=1}^{k} \varepsilon_{ij}}{k(k-1)}$$

где $\mu_i^{(l)}$ – значение l-го параметра j-го образа; n – общее число используемых параметров; k – общее число образов; γ_l – параметр, характеризующий трудоемкость оценки l-й характеристики.

2. Критерий компактности, предложенный новосибирскими учеными:

$J = (D_{ij} + |D_i - D_j|) / (D_i + D_j)$.Компактность D_i образа i характеризуется средней длиной r ребер соединяющего их полного графаРазнесенность образов в пространстве характеристик оценивается через среднее расстояние между всеми парами точек из разных образов D_{ij}.

Видно, что при таком определении, чем больше получается параметр J, тем более информативным является набор параметров, по которым оценивались расстояния между образами.

3. Вероятностный критерий Байеса

$$K = \frac{\sqrt{\sum_{i=1}^{M} (P(A_i / b_k) - P'(A_i / b_k))^2}}{M},$$

$$p(A_j / b_k) = \frac{p(A_j)\, p(b_k / A_j)}{\sum_{i=1}^{M} p(A_i)\, p(b_k / A_i)},$$

где K – значение критерия; $p(A_j/b_k)$ – вероятность гипотезы о принадлежности реализации $b_к$ к j-му классу; $p(A_j)$ – априорная вероятность проявления j-го класса (A_j); $p(b_k/A_j)$ – условная вероятность проявления признаков реализации b_k у класса A_j.

В дальнейшем необходимо осуществить практическую ранжировку различных параметров по приведенным выше критериям информативности. После осуществления ранжировки можно будет сделать заключение об использовании того или иного набора параметров речевого сигнала для решения задач распознавания речевого сигнала и идентификации диктора.

ЛИТЕРАТУРА

1. *Загоруйко Н.Г., Волошин Г.Я.* (ред.) Распознавание слуховых образов. Москва. 1970, 338 с.
2. *Загоруйко Н.Г.* Методы распознавания и их применение М.: Сов. Радио, 1972.
3. *Загоруйко Н.Г.* Методы распознавания и их применение. М., 1970;

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.А. Мелокумов, студент гр. 521-2 каф. КИБЭВС
ТУСУР, г. Томск, Melokumov@mail2000.ru

Аудит информационной безопасности представляет собой комплекс работ, включающий исследование всех аспектов обеспечения информационной безопасности в организации, проводимое по согласованному с заказчиком плану в соответствии с выбранной методикой и критериями. Аудиторский отчет содержит описание текущего состояния информационной безопасности в организации и обнаруженных уязвимостях, а так же рекомендации по их устранению.

Аудит включает в себя следующие последовательные этапы выполнения работ:

1. инициирование и планирование;
2. обследование, документирование и сбор информации;
3. анализ полученных данных и уязвимостей;
4. выработка рекомендаций;
5. подготовка отчетных документов и сдача работ.

Аудит представляет собой комплекс мероприятий, в которых помимо самого аудитора, оказываются задействованными представители большинства структурных подразделений компании. Действия всех участников этого процесса должны быть скоординированы. Поэтому на этапе инициирования процедуры аудита должны быть решены следующие организационные вопросы:

- права и обязанности аудитора должны быть четко определены и документально закреплены в его должностных инструкциях, а также в положении о аудите;
- аудитором должен быть подготовлен и согласован с руководством план проведения аудита;
- в положении о внутреннем аудите должно быть закреплено, в частности, что сотрудники компании обязаны оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию.

Этап сбора информации аудита, является наиболее сложным и длительным. Это связано с отсутствием необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации.

Используемые аудиторами методы анализа данных определяются выбранными подходами к проведению аудита, которые могут существенно различаться.

Первый подход, самый сложный, базируется на анализе рисков. Опираясь на методы анализа рисков, аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной информационной системы (ИС), среды ее функционирования и существующие в данной среде угрозы безопасности. На качество результатов аудита, в этом случае, сильно влияет используемая методология анализа и управления рисками и ее применимость к данному типу ИС.

Второй подход, самый практичный, опирается на использование стандартов информационной безопасности. Стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Такими стандартами являются:

- руководящие документы Гостехкомиссии России;
- международные стандарты, включая ISO 17799, ISO 15408, BSI/IT Baseline Protection Manual и COBIT, SANS SCORE и другие;
- отраслевые стандарты, определяющие требования, специфичные для банковских, телекоммуникационных, торговых систем и т.п.;
- требования, сформулированные по результатам анализа рисков и специфичные для ИС заказчика.

От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для данной ИС. Необходима также методика, позволяющая оценить это соответствие.

Третий подход, наиболее эффективный, предполагает комбинирование первых двух. Базовый набор требований безопасности, предъявляемых к ИС, определяется стандартом. Дополнительные требования, в максимальной степени учитывающие особенности функционирования данной ИС, формируются на основе анализа рисков. Этот подход является намного проще первого, т.к. большая часть требований безопасности уже определена стандартом, и, в то же время, он лишен недостатка второго подхода, заключающего в том, что требования стандарта могут не учитывать специфики обследуемой ИС.

Рекомендации, выдаваемые аудитором по результатам анализа состояния ИС, определяются используемым подходом, особенностями обследуемой ИС, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении аудита.

В любом случае, рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности. При этом мероприятия по

обеспечению защиты организационного уровня практически всегда имеют приоритет над конкретными программно-техническими методами защиты.

Аудиторский отчет является основным результатом проведения аудита. Его качество характеризует качество работы аудитора. Структура отчета может существенно различаться в зависимости от характера и целей проводимого аудита. Однако определенные разделы должны обязательно присутствовать в аудиторском отчете. Он должен, по крайней мере, содержать:

- описание целей проведения аудита;
- характеристику обследуемой ИС;
- указание границ проведения аудита и используемых методов;
- результаты анализа данных аудита;
- выводы, обобщающие эти результаты и содержащие оценку уровня защищенности АС или соответствие ее требованиям стандартов;
- рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты.

ЛИТЕРАТУРА

1. www.techexpert.com.ua
2. www.infosec.ru
3. www.dsec.ru
4. *Мещеряков Р.В., Шелупанов А.А,* Специальные вопросы информационной безопасности. Томск.: Изд-во Института оптики атмосферы СО РАН, 2003. – 244 с.

СИСТЕМА ИНВЕНТАРИЗАЦИИ И ОБНАРУЖЕНИЯ УТЕЧЕК ИНФОРМАЦИИ ИЗ ЛОКАЛЬНЫХ СЕТЕЙ MICROSOFT

А.О. Мишурин; П.С. Ложников, к.т.н.
Сибирская государственная автомобильно-дорожная академия,
webmaster13@mail.ru

Сегодня актуальными являются задачи мониторинга и обнаружения в реальном времени попыток хищения информации из корпоративной сети организации. В данной работе в качестве похитителей будем рассматривать только «своих» пользователей, т.е. штатных сотрудников организации. Как запретить своим пользователям пересылку любой информации через Internet администраторам понятно. Для решения такой задачи сегодня существует очень много средств: межсетевые экраны, системы анализа содержимого почтовых сообщений и

т.д. В большинстве случаев, решаясь похитить информацию из корпоративной сети, пользователи пользуются обычными средствами переноса информации: дискетами CD/DVD-дисками, различными устройствами с flash-памятью или даже извлечением жесткого диска из системного блока. Конечно, решением этой проблемы может быть снятие дисководов, CD/DVD-пишущих приводов, отключение USB-портов и опечатка системных блоков. Только взамен администратор получит новую проблему – бесконечные обращения пользователей, чтобы внести какую-нибудь информацию в свои компьютеры.

В качестве демократичного решения поставленной задачи была разработана система для инвентаризации аппаратного обеспечения компьютеров (входящих в локальную сеть), позволяющая обнаруживать в реальном времени доступ к мобильным носителям информации, а также замену жесткого диска. Система поддерживает клиент-серверную архитектуру (рис. 1). Каждая часть системы выполняет определенный набор функций, рассмотрим их далее.

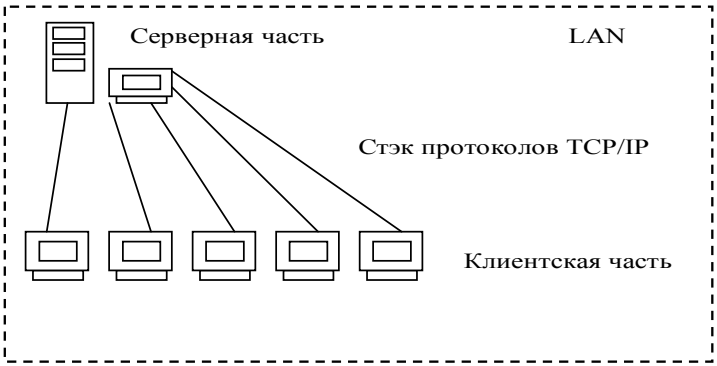


Рис. 1. Схема взаимодействия частей системы

Основные функции клиентской части системы:

- Сбор информации об аппаратном обеспечении на локальном компьютере;
- Обнаружение незаконного доступа к носителям информации (в соответствии с заданной конфигурацией) и отправка сообщения на сервер сигнализирующего данное событие;
- Выполнение инструкций полученных от сервера локальной сети.

Основные функции серверной части системы:

- Получение, обработка и хранение данных от клиентов;
- Анализ сигнализирующих сообщений и возвращение клиенту инструкции к действию (в соответствии с заданной конфигурацией).

Работа всех частей системы инвентаризации локальной сети представляет собой выполнение следующих действий. Через групповую политику операционных систем Microsoft Windows 2000/XP устанавливаются на клиентские компьютеры в автозагрузку модули агенты. При их первом включении начинается сбор информации об аппаратном обеспечении (рис. 2), после чего происходит подготовка и отправка (используя стэк протоколов TCP\IP) данных на сервер (в соответствии с заданной конфигурацией). Затем агенты переходят в режим ожидания событий незаконного доступа к носителям информации и получения инструкций от сервера. Клиент при обнаружении незаконного (в соответствии с настройками) доступа к носителям информации, отправляет сообщение на сервер, сигнализирующее данное событие. При получении сервером сообщения о незаконном доступе к носителям информации, генерируется ответная инструкция и отправляется клиенту. Клиент при получении ответа от сервера выполняет инструкции и может заблокировать использование определенного устройства (например, USB-порты).

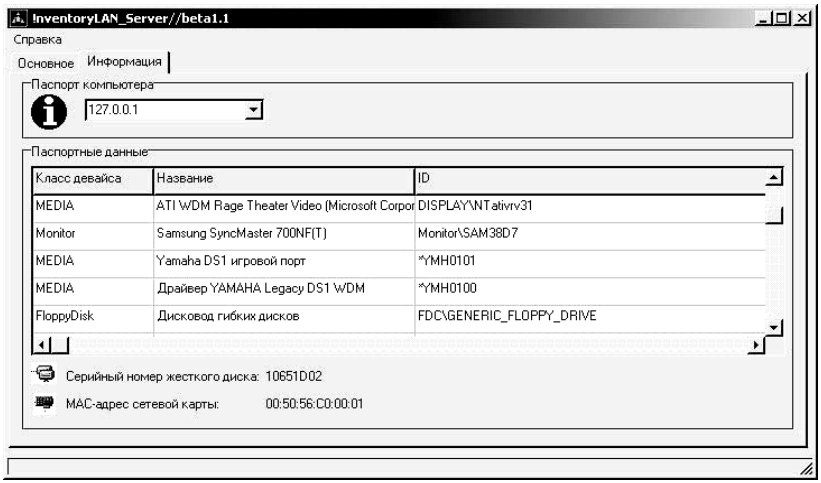


Рис. 2. Интерфейс серверной части, показывающей паспортные данные компьютера

Получить паспортные данные компьютеров можно на сервере (см. рис. 2) в разделе «Информация», выбрав соответствующий IP-адрес. При последующих загрузках клиентских компьютеров вновь получаемые паспортные данные сравниваются с имеющимися в базе данных. Если пользователь заменил, например, жесткий диск или сетевую карту, то администратор получит соответствующее предупреждение.

Данная система была реализована в среде разработки Borland C++ Builder 6.0. В качестве дальнейшего развития данной системы планируется реализация возможности удаленного получения паспортных данных компьютеров через Internet, посредством специально разработанного портала.

ЛИТЕРАТУРА

1. *Borland* C++ Builder 6. Для профессионалов / В.А. Шамис. СПб.: Питер, 2003. 798 с.
2. *Microsoft* Windows API. Справочник системного программиста. Второе издание, дополненное: Пер. с англ. / Ричард Саймон. К.: ООО «ТИД ДС», 2004. 1216 с.
3. *Компьютерные* сети. Модернизация и поиск неисправностей: Пер. с англ. / К. Закер. СПб.: БХВ-Петербург, 2004. 1008 с.

ИСПОЛЬЗОВАНИЕ GRSECURITY ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В ОС LINUX

Е.В. Пушкарева, студент 3 курса гр. 143-1

ТУСУР, г. Томск, janep@sib-page.ru

В связи с развитием технологий обеспечения защиты информации, один из самых простых и эффективных методов несанкционированного доступа является получение пароля суперпользователя на интересующей злоумышленника системе. Методы и сценарии атак на информационную систему с получением прав суперпользователя разнообразны и зачастую могут базироваться на ошибках конфигурирования системы и на ошибках в программном обеспечении.

В случае получения злоумышленником на информационной системе прав суперпользователя, появляется проблема обеспечения безопасности информации и информационных процессов от суперпользователя. Это вызвано тем, что суперпользователь обладает всеми правами в системе и может нарушить как конфиденциальность, так и целостность информации, находящейся на информационной системе.

Для реализации модели ограничения прав суперпользователя, можно воспользоваться системой ролевого доступа Rule Set Based Access Control (RSBAC). Таким образом, что каждый пользователь, в том числе и суперпользователь, может иметь доступ только для необходимой для работы информации. В случае использования операционной системы семейства UNIX, Linux, суперпользователь может выполнять

команду su имя_пользователя, для получения привилегий других пользователей. С другой стороны, так же необходимо обеспечить не только конфиденциальность и целостность данных, но и целостность операционной системы. Суть модели ограничения прав суперпользователя сводится к ограничению возможности изменений текущей конфигурации системы, изменение системных утилит и файлов, ограничение на ознакомление и изменение данных, принадлежащих другим пользователям, а так же, запрет получения прав других пользователей через использование системной команды su.

В качестве инструмента ограничение доступа, существуют такие системы как RSBAC, SELinux, Grsecurity. Последние две позволяют более гибкую настройку ролевого доступа и имеют систему обнаружения вторжения (Linux Intruder Detection System (LIDS)). SELinux самая строгая только при условии правильной настройки. Если ее недостаточно умело отрегулировать, например, если у администратора не хватает опыта, то данная система защиты будет не эффективна. Напротив, при правильной настройке (которая намного проще) системы Grsecurity и LIDS обеспечивают примерно такой же уровень безопасности, что и SELinux.

Основная цель GrSecurity – сократить до минимума конфигурацию системы, поскольку сложные системы часто настраиваются неправильно, что приводит к возникновению потенциальных дыр в системе безопасности.

Вот некоторые усовершенствования, вносимые GrSecurity в систему:

- Улучшенное chroot-окружение, не позволяющее процессу выйти за его пределы;
- OpenBSD-рандомизация TCP ISN (номер последовательности TCP-пакета) и PID (Process ID)
- ACL (MAC)
- RBAC
- Защита стека PaX.

В ходе реализации модели, суперпользователю root, было запрещено изменение содержимого директорий bin, etc, lib, sbin, usr, редактирование лог-файлов системы, доступ до файлов, не принадлежащих пользователю root, а также исполнение файлов в каталогах home, tmp, root, запрет доступа на чтение/исполнение до команды su.

ЛИТЕРАТУРА

1. http://opennet.ru
2. *Журнал* «CHIP | LINUX» №3, 2005 г
3. http://grsecurity.org/

ИДЕНТИФИКАЦИЯ АВТОРСТВА ТЕКСТА

А.С. Романов, студент 4 курса каф. КИБЭВС
ТУСУР, г. Томск, т.64-41-34, Alexis2004@yandex.ru

Целью данной работы является изучение существующих методов идентификации авторства текста.

Определение авторства текста является частью атрибуции текста. Атрибуцией называется сопоставление тексту соответствующих ему атрибутов, к числу которых относятся имя автора, дата создания, место создания, жанр произведения и т.д.

Одно из направлений идентификации авторства основывается на том, что каждый автор обладает набором специфических стилистических приемов, характерными языковыми особенностями (лексическими, грамматическими, фразеологическими), прослеживающимися на протяжении всего произведения, благодаря которым его можно опознать. Отдельно стоит выделить мнение о том, что каждый писатель имеет определенный набор слов, который он наиболее часто употребляет в своих произведениях, т.е. словарь, анализ которого может помочь в определении авторства.

Недостатком этого подхода является высокая вероятность подмены типичных особенностей индивидуального стиля автора. Кроме того, выявление отличительных черт авторского языка носит субъективный характер, так как зависит от личности исследователя.

Основоположником объективных методов можно считать Н.А. Морозова [1]. В отличие от предшественников, Морозов предложил использовать для исследований не редко встречающиеся лингвистические формы, а наоборот, слова, имеющие большую частоту употребления. Он полагал, что, анализируя частоту встречаемости языковых элементов в тексте можно получить характеристики писателей, по которым можно отличить их произведения от произведений других авторов и плагиата. Графическое представление распределения частоты встречаемости слов, сгруппированных в тот или иной грамматический класс, он назвал «лингвистическими спектрами». Стоит отметить, что основное внимание Морозов уделял служебным словам, таким как союзы, предлоги, местоимения и т.д.

Данный метод подвергался критике и обвинялся в несостоятельности [2]. Причиной этому послужило то, что метод существенно зависит от объема выборки анализируемого текста, самим же автором граница выборки, в пределах которой метод дает стабильный по надежности результат, определена не была. В последствие граница была определена в 5000 слов.

В методе, использующем цепи А.А. Маркова [4] для каждого автора по подлинным его произведениям вычисляются переходные частоты употребления пар букв, которые служат оценкой матрицы вероятностей перехода из буквы в букву. Для спорного текста оцениваются вероятности его написания каждым автором, и по полученным результатам делается вывод об истинном авторе.

Метод накопительных сумм А. Мортона [5], основывающийся на предположении о том, что каждый автор имеет набор привычек, которые он использует во всех своих произведениях. Анализируются такие характеристики как: длина предложения, количество слов, начинающихся с гласной буквы, количество служебных слов, короткие слова и т.д. Затем для них находятся средние значения и отклонения величины каждой вышеперечисленной единицы от этого среднего. Метод используется для проверки текста на однородность и хорошо подходит для выявления плагиата. Для определения написаны ли два текста одним и тем же автором их соединяют в один и находят накопительную сумму. Если авторы тестов разные, то вид результатов метода будет отличаться до и после точки соединения.

В.П. и Т.Г. Фоменко [6] был предложен метод опорных слов. Авторами была предложена характеристика, названная «авторским инвариантом». Предполагалось, что значение инварианта, с одной стороны, устойчиво к изменению стиля внутри произведений одного и того же автора и, с другой, чувствительно к авторскому стилю как таковому, кроме того, не может контролироваться автором сознательно. В результате исследований авторы обнаружили, что в качестве инварианта можно использовать частоту встречаемости служебных слов (14 союзов, 17 частиц и 38 предлогов).

Для определения авторства можно также использовать аппарат искусственных нейронных сетей. При этом на вход нейронной цепи подают некоторые характеристики текста, а на выходе формируют вектор принадлежности тому или иному автору.

Зачастую, небольшой объем текстов, действительно нуждающихся в атрибуции (в основном связанных с криминалистикой), не позволяет применять ни один из перечисленных методов, поэтому необходимо ввести дальнейшие исследования, направленные на поиск новых или совершенствование уже имеющихся методов, с помощью которых станет возможным работа с малыми объемами выборки. В настоящее время практически не существует неатрибутированных текстов большого объема.

Проблема определения авторства актуальна не только для привычных текстовых документов, но и для исходных текстов программ. Здесь задача усложняется тем, что в каждом языке программирования

есть свой жесткий, набор зарезервированных слов, несравнимый с многообразием естественного языка, существуют определенные правила и стандарты, накладывающие ограничения на названия идентификаторов подпрограмм, переменных, классов, использование отступов и комментариев, которым старается следовать большинство программистов. Таким образом, выявление индивидуальных черт авторов исходных текстов, на чем основано большинство методов определения авторства, весьма затруднено.

В дальнейшем планируется исследование методов определения авторства текста на практике, а также исследовать подходы к определению авторства исходных текстов программ.

ЛИТЕРАТУРА

1. *Морозов Н.А.* Лингвистические спектры: средство для отличения плагиатов от истинных произведений того или иного известного автора. Стилеметрический этюд // Известия отд. русского языка и словестности Имп. Акад. наук, Т. XX, кн. 4, 1915.
2. *Марков А.А.* Об одном применении статистического метода // Известия Имп. Акад. Наук. Серия VI. Т. X. N 4. 1916. с. 239.
3. *Марков А.А.* Пример статистического исследования над текстом «Евгения Онегина», иллюстрирующий связь испытаний в цепь // Известия Имп. Акад. Наук. Серия VI. Т. X. N 3. 1913. с. 153.
4. *Хмелев Д.В.* Распознавание автора текста с использованием цепей А.А. Маркова // Вестник МГУ. Сер. 9. Филология. 2000. № 2. С. 115–126.
5. *Morton A.Q.* The Authorship of Greek Prose // Journal of the Royal Statistical Society (A), 128, 1965. pp. 169–233.
6. *Фоменко В.П., Фоменко Т.Г.* Авторский инвариант русских литературных текстов. М.: Изд-во МГУ. 1996. с. 768–820.
7. *Мещеряков Р.В., Васюков Н.С.* Модели определения авторства текста.

ПРЕОБРАЗОВАНИЯ ФОРМАТИРОВАНИЯ КАК ПРОСТЕЙШИЙ МЕТОД ЗАЩИТЫ ИСХОДНОГО ТЕКСТА ПРОГРАММЫ

А.С. Романов, студент 4 курса каф. КИБЭВС

ТУСУР, г. Томск, т. 64-41-34, Alexis2004@yandex.ru.

Ни для кого не является секретом, что защита информации, а в частности защита программных продуктов, является на сегодняшний день актуальным вопросом.

Остро стоит вопрос о защите исходных текстов программ как интеллектуальной собственности автора. Достаточно сказать, что обязательным пунктом контракта на разработку программного продукта

часто является предоставление заказчику исходных текстов. Эта тема актуальна в связи с распространившимся движением программного обеспечения с открытым кодом (Open Sourse), когда программа распространяется с исходным текстом, а также в виду возможности целенаправленного воровства или потери носителя с исходными текстами.

Конечно, разобраться во множестве переменных, подпрограмм, их назначении и связи между собой человеку, не являющемуся автором будет очень не просто. Но эту задачу можно дополнительно усложнить.

Простейшим способом защиты исходных тестов являются преобразования форматирования. Рассмотрим их подробнее.

Практически каждый учебник по программированию содержит главу, в которой рассказано о стилях программирования и правилах оформления исходных текстов программ.

Их ключевыми моментами являются:

1. короткие, но емкие комментарии,
2. наличие отступов,
3. фиксированная ширина поля, за пределы которой желательно не выходить (обычно 80 символов),
4. использование осмысленных названий подпрограмм, переменных, типов, классов, формальных параметров, компонентов и т.д., отражающих их суть (например, понятно, что строковая переменная с именем FileName содержит имя файла),
5. использование осмысленных имен файлов проекта, форм, модулей и т.д., отражающих их суть.

Комментарий – это набор символов, которые игнорируются компилятором. Использование комментариев помогает понять назначение программы, отдельных ее частей и играет ключевую роль в анализе исходных текстов программ. Порой программисты комментируют программу не с целью облегчить жизнь тем, кто будет с ней разбираться, а для себя – чтобы не запутаться в написанном или быстро сориентироваться в ней спустя некоторое время, когда понадобится ее модифицировать. Стоит сказать, что не многие программисты уделяют внимание комментариям должным образом.

Отступы зрительно показывают подчиненность (иерархию) операторов, обычно выполняются с помощью нескольких (оптимально двух) знаков пробела. Правильное использование отступов являются ключевым методом обеспечения читаемости.

Продуманное использование комментариев и согласованное использование отступов может сделать чтение и понимание программы намного более приятным. Неправильное использование комментариев может серьезно повлиять на удобочитаемость программы. Можно предположить, что несоблюдение этих правил приведет к психологическому дискомфорту программиста, в руки которого попал исходный

текст программы, ведь и он, скорее всего, обучался по этим учебникам и в некоторой степени привык использовать описанные в них правила оформления. Таким образом, это можно использовать в качестве простейших методов защиты листинга программы.

Назначение этих методов – понизить читабельность исходного текста, дезориентировать программиста, в чьих руках находится проект, вызвать у него чувство сложности анализа текста при первом взгляде на него, затруднить его восприятие, а также сделать анализ трудоемким за счет неудобства и выполнения рутинных операций (расстановки символов табуляции, переноса строки и пробелов), а в идеале – заставить полностью отказаться от работ по дальнейшему анализу.

К таким методам относятся:

1. отсутствие каких-либо комментариев,
2. оформление сплошным текстом (без лишних пробелов, символов переноса строк, пустых строк, отступов),
3. использование бессмысленных идентификаторов (пользовательских имен переменных, подпрограмм, файлов и т.д.).

Для достижения худшей удобочитаемости новые имена должны отличаться одним символом. Например, asdfqw, asgfqw, asdgqw.

Все эти методы можно применить к конечному «исходнику» без внесения каких-либо серьезных изменений, касающихся смысловой нагрузки или особенностей реализации. В виду относительно легкой программной реализации этих методов процесс можно автоматизировать.

Возможен и обратный процесс – форматирование текста и расстановка всех недостающих символов. Существуют текстовые редакторы, автоматически форматирующие исходный текст при его открытии, а также специализированные программы, предназначенные для этого. Но абсолютно корректно работают не все из них. К тому же, если отформатировать программу будет несложно, то вернуть первоначальные имена идентификаторов и расставить комментарии программе будет не под силу.

Все вышеперечисленное будет полезно не только программисту, желающему защитить свои «исходники», но и заказчикам программ, которые хотят платить деньги за понятные и грамотно оформленные коды и заинтересованы в том, чтобы данные методы не применялись.

ЛИТЕРАТУРА

1. http://www.osp.ru/os/2001/07-08/040.htm – Приемы защиты исходных текстов и двоичного кода. Крис Касперски.
2. http://www.delphikingdom.com/article/coderules.htm – Стандарт стилевого оформления исходного кода DELPHI. Ткаченко А.В.
3. http://www.citforum.ru/security/articles/analysis/ – Анализ запутывающих преобразований программ Чернов А. В.

АУДИТ ОБРАЩЕНИЙ К ФАЙЛАМ И ОБЪЕКТАМ

С.В. Селиверстов, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск., e-mail: silvernet@ngs.ru

Администратор компьютера работающего под управлением Windows NT, имеет возможность управлять доступом к таким системным ресурсам, как каталоги, принтеры и разделяемые по сети объекты. Подсистема аудита информирует администратора об использовании общих ресурсов системы, об использовании ресурсов какими-либо процессами, в том числе и скрытыми, о запрещенных действиях пользователей (например, если кто-то пытается получить доступ к защищенным ресурсам), а также о частоте и о последствиях таких обращений. Собранная при помощи аудита информация может быть использована для профилактики проблем производительности системы, анализа нарушений политики безопасности, а также для последующего планирования вычислительной системы или сети.

Конечно же нельзя собирать всю информацию обо всем. Если отслеживаемые события происходят достаточно часто или на большом количестве объектов, то применение политики аудита может оказать существенное влияние на производительность системы и общую эффективность работы. А разбор неправильно настроенных журналов безопасности может превратиться в непосильную задачу, даже для опытного системного администратора. Поэтому, прежде всего, следует определить, какие цели преследуются при использовании подсистемы аудита, затем определиться, какие ресурсы отслеживать и какие действия над ними регистрировать, и потом применить определенную таким образом политику аудита на конкретных объектах.

В системе обеспечения информационной безопасности в составе программно-аппаратного комплекса защиты информации подсистема аудита должна занимать одно из ведущих мест. Она позволяет видеть, что происходило с системой в определенный момент времени и делать соответствующие выводы.

Подсистема файлового аудита представляет особый интерес, так как в большинстве операционных систем (если не во всех) единицей обрабатываемой информации является именно файл. Для событий файловой системы необходимо фиксировать такие параметры как совершенное событие, процесс, обращающийся к файлу, пользователь, время и результат выполнения события, а также некоторые другие необходимые параметры.

Надо заметить, что подсистема аудита не позволяет предотвратить, например, удаление или искажение файла, но она позволяет узнать, кто и когда это сделал для предотвращения таких ситуаций в дальнейшем или для поиска злоумышленников. Может быть хорошим

дополнением организационной системы защиты информации или применяемой политики безопасности.

Операционные системы семейства Windows NT имеют встроенные средства для сбора аудита, касающегося файловой системы.

Для обеспечения большей гибкости аудит настраивается и управляется на трех уровнях:

– включение и выключение аудита событий, происходящих в системе при помощи оснастки Локальная политика безопасности -> Политика аудита. Здесь можно выбрать результат для выполнения событий: успех или отказ;

– после того как аудит в системе включен, становятся доступны для мониторинга семь типов событий, фиксируемых по успешному или неудачному выполнению, среди которых есть также аудит доступа к файлам и каталогам;

– третий уровень доступен на уровне конкретных объектов. Переключатели управления параметрами находятся здесь в свойствах любых объектов NTFS, таких как файлы, каталоги и принтеры. Каждый объект имеет два списка управления доступом (Access Control List, ACL): разграничительный – (Discretionary ACL, DACL) и системный – (System ACL, SACL).

При правильной настройке и своевременном анализе данных аудита встроенные средства предоставляют администратору системы широкие возможности в анализе безопасности системы. Можно узнать, кто и когда обращался к определенному файлу, были ли попытки несанкционированного доступа или к каким файлам пытаются безуспешно обратиться некоторые приложения. Но есть и некоторые проблемы.

Хотя технологии безопасности в Windows NT являются достаточно надежными и широкораспространенными, они все-таки не являются универсальными: как для FAT-разделов диска, так и для различного рода съемных носителей подсистемы аудита обращений к файлам в системах семейства Windows NT (и особенно, в Windows9X) не существует в принципе. А существующая подсистема на томах NTFS не всегда позволяет восстановить полную картину событий в системе. Причем, остается проблема администрирования, когда от желания одного человека зависит содержимое журналов безопасности.

Программы, поставляемые сторонними разработчиками, несут в себе много полезных функций, но часто являются платными. Также они могут обладать противоречивым интерфейсом и непонятным представлением результатов (например, в виде списка системных функций и идентификаторов, определенных программистом и только одному ему известных).

В связи с этим может встать необходимость создания подсистемы аудита собственной разработки, закрывающей перечисленные недостатки и формирующей результаты аудита в удобной для анализа форме. Благодаря организации работы ядра операционной системы и современным средства программирования это можно сделать несколькими способами.

Во-первых, это – перехват запроса к драйверу файловой системы функцией IoAttachDeviceByPointer (работает для файловых систем FAT, NTFS, CDFS и для всех съемных носителей). В данном случае пишется драйвер режима ядра операционной системы по образцу файловой системы, который перехватывает обращения к драйверу файловой системы и посылает их на интерфейсную часть приложения. Кроме этого обрабатываются запросы FastIoDispatch, отвечающие за обработку функции DeviceIoControl, и операции закрытия, чтения и записи в устройство.

Не менее эффективным является перехват системных вызовов ядра ОС через прерывания Int2Eh, где номера системных вызовов соответствуют функциям файлового ввода-вывода, но тут появляется проблема с различием номеров системных вызовов в разных операционных системах.

Первый способ представляется наиболее предпочтительным, так как нет необходимости хранить таблицы соответствий вызовов для различных операционных систем (то есть более универсален) и работа драйвера на нулевом кольце защиты ядра ОС предоставляет больше ресурсов и возможностей.

Тем более что уже ушло в прошлое создание драйверов на Ассемблере. Теперь есть удобные и эффективные средства по созданию не менее эффективных драйверов на C/C++.

Таким образом, решение задачи сбора аудиторской информации сводится к продуманной постановке требований и целей, которые необходимо достичь в каждом конкретном случае для реально работающих систем.

ИССЛЕДОВАНИЕ АРХИТЕКТУРЫ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ

Е.А. Сопов, студент 1 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 66-92-19, the_sick@mail.ru

В настоящее время, в связи с развитием средств коммуникации и компьютерных сетей увеличивается применения электронного документооборота. Одним из средств защиты электронного документообо-

рота является применение шифрования и электронной цифровой подписи (ЭЦП). Основой для создания ЭЦП являются Удостоверяющие Центры.

Удостоверяющий центр (УЦ) – комплекс технических средств и организационно-технических мероприятий, предназначенный для обеспечения выполнения целевых функций Удостоверяющего центра как организации.

УЦ обеспечивает участников электронного документооборота ключевой парой (открытым и закрытым ключом) и сертификатом открытого ключа.

Участники – это юридические лица, которым требуется обеспечение достоверности целостности и авторства передаваемой информации через локальную или внешнюю сеть другим юридическим лицам, которые также являются участниками документооборота.

Наиболее важными компонентами УЦ являются: Центр Регистрации (ЦС), Центр Сертификации (ЦР) и Автоматизированное Рабочее Место (АРМ) администратора.

Центр сертификации предназначен для формирования сертификатов открытых ключей пользователей и администраторов УЦ, для создания списков отозванных сертификатов, и для хранения эталонной базы сертификатов и списков отозванных сертификатов.

ЦС взаимодействует только с одним или несколькими ЦР по отдельному защищенному каналу связи. ЦС отвечает за генерацию, создание, смену и введение в базу данных уникальной информации о ключах и сертификатах открытых ключей. ЦС формирует открытый ключ, изменяет базу и формирует список отозванных сертификатов только по запросам ЦР. ЦС отправляет результаты запросов ЦР.

Центр регистрации предназначен для хранения регистрационных данных пользователей, запросов на сертификаты и сертификаты пользователей.

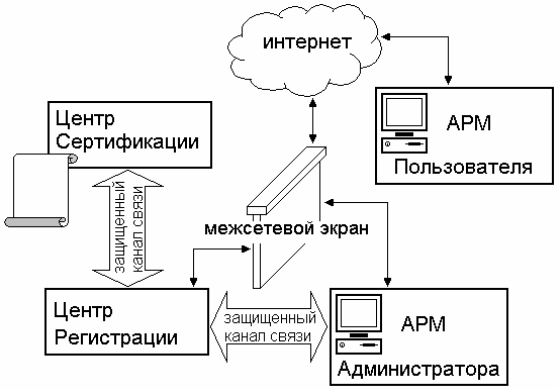
ЦР также взаимодействует с ЦС по локальному защищенному каналу связи. ЦР отвечает за управление шаблонами регистрации, за ведение базы данных о зарегистрированных пользователях, за оповещение о состоянии пользователей в системе, за протоколы работы ЦР.

Пользователь только после регистрации в ЦР, может получить в УЦ сертификат на свой открытый ключ.

Компонент АРМ администратора предназначен для выполнения организационно-технических мероприятий, связанных с регистрацией пользователей и взаимодействия с ЦР.

АРМ администратор взаимодействует с ЦР по локальному защищенному каналу связи. АРМ администратор отвечает за регистрацию

пользователей и генерацию служебных ключей и сертификатов пользователей, за проверку состояния запросов на формирование сертификатов и за просмотр протоколов ЦР. С помощью АРМ администратора можно просмотреть информацию о пользователях в базе данных ЦР.



Взаимодействие компонент УЦ

На рисунке представлена схема взаимодействия компонент УЦ между собой.

ПРИМЕНЕНИЕ PKI В РОССИИ И В МИРЕ

М.А. Сопов, инженер каф. КИБЭВС
ТУСУР, г. Томск, т. 416-000, 412-500 , sma@keva.tusur.ru

Распространение электронного документооборота остановить невозможно, все больше предприятий и информационных систем переводят свой документооборот в электронный вид, поэтому растет спрос на продукты и услуги в области ЭЦП (Электронной Цифровой Подписи). А ключевым продуктом здесь являются так называемые системы PKI (public key infrastructure).

PKI использует защитные механизмы, построенные как на основе криптографии с открытым ключом, так и на основе криптографии с общим секретным ключом. В последнем случае обмен секретными симметричными ключами или их выработка осуществляется безопасным образом за счет применения асимметричных криптографических механизмов и PKI.

России и за рубежом отношение к PKI различное. До последнего времени в России применялась только для управления электронным документооборотом с использованием ЭЦП, защита электронной почты, и лишь частично в других системах, в развитых зарубежных странах применение PKI давно вышло за рамки подобных задач, развивая построение VPN на основе PKI, защиту программных модулей и т.д.

Противоположные мнения о применении и доверии специализированным Удостоверяющим Центром сложились в России (рис. 1) и зарубежном (рис. 2). Если в Мире на предприятиях или в организациях строят собственные УЦ мало доверяя специализированным УЦ, то Российские компании и организации пользуются услугами, оказываемыми специализированными УЦ и мало строят их на базе своих организаций. При чем свои УЦ строят в основном государственные учреждения и банки, данную тенденцию можно объяснить тем, что Россия испытывает дефицит квалифицированных кадров в области защиты информации и в частности PKI.

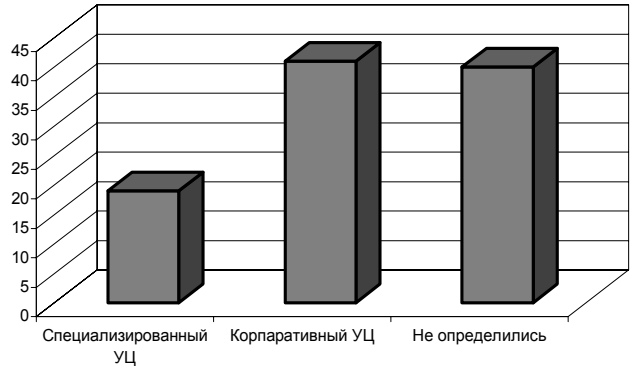


Рис. 1. Доверие Удостоверяющим Центрам в Мире

Противоположные мнения о применении и доверии специализированным Удостоверяющим Центром сложились в России (Рисунок 1) и зарубежном (рис. 2). Если в Мире на предприятиях или в организациях строят собственные УЦ мало доверяя специализированным УЦ, то Российские компании и организации пользуются услугами, оказываемыми специализированными УЦ и мало строят их на базе своих организаций. При чем свои УЦ строят в основном государственные учреждения и банки, данную тенденцию можно объяснить тем, что Россия испытывает дефицит квалифицированных кадров в области защиты информации и в частности PKI.

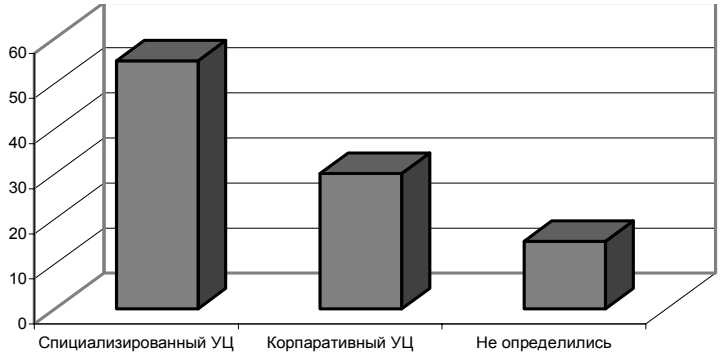


Рис. 2. Доверие Удостоверяющим Центрам в России

Программных продуктов реализующих PKI не так много, так как имеют сложную архитектуру. В мире в основном используются технологии компании Entrust (Entrust/PKI), Baltimore Technologies (UniCert), RSA Security (KEON) и Microsoft (Windows CA), причем в России в связи с тем что продукты данных компании очень дорогие, в основном используются KEON и Windows CA встроенный в Windows 2000 и 2003, на сегодняшний момент в Windows 2003 встроена российская криптография (ГОСТ 34.10-2001). Из Российских компаний наибольшее распространение на рынке получила компания КриптоПро с одноименным продуктом, компания Инфотекс (VipNet), Фактор (Дионис), МОП НИИ (Верба), компания ТопКросс с продуктом кросс-сертификации УЦ (ТС-УЦ) и другие компании создающие продукты криптографии с узкой и широкой направленностью.

Не смотря на столь различные направления развития и использования PKI в России и Мире, а также проблемы, которые существуют, внедрение PKI происходит все с большим темпом и начинает внедряться в жизнь простых граждан.

ЗАЩИТА ИНФОРМАЦИИ В ОПЕРАЦИОННОЙ СИСТЕМЕ MICROSOFT WINDOWS XP

С.В. Сорокин, студент 5 курса гр. 571-1 ФВС;
Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС
ТУСУР, г. Томск, т.89069563493, perun@ms.tusur.ru

Защита конфиденциальных данных от несанкционированного доступа очень важна в любой среде, где множество пользователей обращается к одним и тем же ресурсам. У операционной системы, как и у

отдельных пользователей, должна быть возможность защиты файлов, памяти и конфигурационных параметров от нежелательного просмотра и внесения изменений. Безопасность операционной системы обеспечивается такими очевидными механизмами, как учетные записи, пароли и защита файлов. Но она требует и менее очевидных механизмов – защиты операционной системы от повреждения, запрета непривилегированным пользователям определенных действий, предотвращения неблагоприятного воздействия программ одних пользователей на программы других пользователей или на операционную систему. Данная работа предназначена для изучения встроенных механизмов защиты данных от несанкционированного доступа, Так в операционной среде Microsoft Windows XP защита реализуется на следующих компонентах и базах данных:

– *Монитор состояния защиты.* Компонент исполнительной системы, отвечающий за определение структуры данных маркера доступа для представления контекста защиты, за проверку прав доступа к объектам, манипулирование привилегиями и правами, генерацию сообщений аудита безопасности.

– *Подсистема локальной аутентификации.* Процесс пользовательского режима, который отвечает за политику безопасности в локальной системе, а также за аутентификацию пользователей и передачу сообщений аудита безопасности в Event Log.

– *База данных политики LSASS.* База данных, содержащая параметры политики безопасности локальной системы. Она хранится в разделе реестра HKLM\SECURITY.

– *Диспетчер учетных записей безопасности.* Набор подпрограмм, отвечающих за поддержку базы данных, которая содержит имена пользователей и группы, определенные на локальной машине.

– *База данных SAM* База данных, которая в системах содержит информацию о локальных пользователях и группах вместе с их паролями и другими атрибутами. Она хранится в разделе реестра HKLM\SAM.

– *Active Directory.* Служба каталогов, содержащая базу данных со сведениями об объектах в домене. Active Directory хранит информацию об объектах домена, в том числе о пользователях, группах и компьютерах.

– *Пакеты аутентификации.* DLL-модули, выполняемые в контексте процесса Lsass и клиентских процессов и реализующие политику аутентификации в Windows. DLL аутентификации отвечает за проверку пароля и имени пользователя, а также за возврат LSASS детальной информации о правах пользователя, на основе которой LSASS генерирует маркер.

– *Процесс входа Winlogon*. Процесс пользовательского режима, отвечающий за поддержку SAS и управление сеансами интерактивного входа в систему.

– *GINA*(*Graphical Identification and Authentication*). DLL пользовательского режима, выполняемая в процессе Winlogon и применяемая для получения пароля и имени пользователя или PIN-кода смарт-карты.

– *Служба сетевого входа* (*Netlogon*) Windows-сервис, устанавливающий защищенный канал с контроллером домена, по которому посылаются запросы, связанные с защитой, или запросы на аутентификацию.

– *Kernel Security Device Driver* (*KSecDD*) Библиотека функций режима ядра, реализующая интерфейсы LPC (local procedure call), которые используются другими компонентами защиты режима ядра – в том числе шифрующей файловой системой (Encrypting File System, EFS) – для взаимодействия с LSASS в пользовательском режиме.

Защита объектов и протоколирование обращений к ним – вот сущность управления избирательным доступом и аудита. Защищаемые объекты Windows включают файлы, устройства, почтовые ящики, каналы, задания, процессы, потоки, события, пары событий, мьютексы, семафоры, порты завершения ввода-вывода, разделы общей памяти, LPC-порты, ожидаемые таймеры, маркеры доступа, тома, объекты WindowStation, рабочие столы, сетевые ресурсы, сервисы, разделы реестра, принтеры и объекты Active Directory.

Поскольку системные ресурсы, экспортируемые в пользовательский режим, реализуются как объекты режима ядра, диспетчер объектов играет ключевую роль в их защите. Для контроля за операциями над объектом система защиты должна быть уверена в правильности идентификации каждого пользователя. Именно по этой причине Windows требует от пользователя входа с аутентификацией, прежде чем ему будет разрешено обращаться к системным ресурсам. Когда какой-либо процесс запрашивает описатель объекта, диспетчер объектов и система защиты на основе идентификационных данных вызывающего процесса определяют, можно ли предоставить ему описатель, разрешающий доступ к нужному объекту.

Контекст защиты потока может отличаться от контекста защиты его процесса. Этот механизм называется олицетворением. Важно не забывать, что все потоки процесса используют одну и ту же таблицу описателей, поэтому, когда поток открывает какой-нибудь объект, все потоки процесса получают доступ к этому объекту.

Модель защиты Windows требует, чтобы поток заранее – еще до открытия объекта – указывал, какие операции он собирается выпол-

нять над этим объектом. Система проверяет тип доступа, запрошенный потоком, и, если такой доступ ему разрешен, он получает описатель, позволяющий ему выполнять операции над объектом. Диспетчер объектов регистрирует права доступа, предоставленные для данного описателя, в таблице описателей, принадлежащей процессу. Для идентификации объектов, выполняющих в системе различные действия, Windows использует не имена, а идентификаторы защиты SID. Для идентификации контекста защиты процесса или потока используется объект, называемый маркером доступа, которые являются лишь частью выражения, описывающего защиту объектов. Другая его часть – информация о защите, сопоставленная с объектом и указывающая, кому и какие действия разрешено выполнять над объектом. Структура данных, хранящая эту информацию, называется дескриптором защиты.

Для определения прав доступа к объекту используются два алгоритма:

– сравнивающий запрошенные права с максимально возможными для данного объекта.

– проверяющий наличие конкретных прав доступа.

Из всего выше сказанного можно сделать вывод, что Windows XP поддерживает большой набор функций защиты, соответствующий ключевым требованиям, как правительственных организаций, так и коммерческих структур.

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

В.Н. Свердлова, студент 4 курса каф. КИБЭВС

ТУСУР, г. Томск, т.8-906-199-90-95, dizzappearing@yandex.ru

Компьютерные преступления – это преступления, совершенные с использованием компьютерной информации, то есть информации, зафиксированной на машинном носителе в форме, доступной восприятию ЭВМ. Компьютерная информация может быть так же и объектом посягательств.

Компьютерные преступления условно можно подразделить на две большие категории – преступления, связанные с вмешательством в работу компьютеров (компьютер – предмет преступления), и преступления, использующие компьютеры как необходимые технические средства (компьютер – орудие преступления).

Все компьютерные преступления имеют ряд отличительных особенностей. Во-первых, это высокая скрытность (отсутствие видимого материального ущерба), сложность сбора улик по установленным фак-

там. Отсюда сложность доказательств при рассмотрении в суде подобных дел. Во-вторых, даже единичным преступлением может наноситься очень крупный материальный ущерб. В-третьих, совершаются эти преступления высоко квалифицированными специалистами, которые во многих случаях обладают большими знаниями в области информационных технологий, чем следственные органы. В-четвертых, область действий компьютерных преступлений ограничена только возможностями современных телекоммуникаций – место совершения преступления и место наступления его последствий далеко не всегда совпадают (часто в глобальных масштабах). Отсюда сложность правового регулирования подобных действий и необходимость принятия международных соглашений.

Уголовно наказуемыми в российском законодательстве считаются следующие виды преступлений (УК РФ):

- Неправомерный доступ к компьютерной информации (Ст. 272)
- Создание, использование и распространение вредоносных программ для ЭВМ (Ст. 273)
- Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (Ст. 274)
- Нарушения авторских и смежных прав (Ст.146)

Однако большого числа возбужденных по данным статьям (особенно по первым трем) уголовных дел не наблюдается в связи с нечеткостью формулировок и сложной доказуемостью, о чем было написано выше.

Допустим, неправомерный доступ к компьютерной информации наказуем по статье 272 УК РФ только в случае его преднамеренности, в случае наличия умысла правонарушителя. Действие этой статьи не охватывает случайный доступ или доступ в результате неосторожных действий. При существующих системах обработки информации, не всегда обеспечивающих достаточный уровень защиты, а так же при расследовании обстоятельств доступа возможно существенное затруднение в установлении умысла правонарушителя.

По статье 273 УК РФ вредоносными считаются все программы, приведшие к неблагоприятным или тяжким последствиям, а не только вирусы, «троянские кони», «логические бомбы» и т. д. В принципе, под это описание могут попасть все программы, написанные квалифицированными программистами вполне законно, но давшие сбой, который привел к нарушению технологического процесса, утере информации и другим неблагоприятным последствиям. Так как безошибочных программ практически не бывает, и надежность программного обеспечения пока значительно ниже надежности многих технических изделий, можно сделать вывод, что формулировка статьи нуждается в доработке.

Статья 274 УК РФ не предусматривает конкретных правил эксплуатации ЭВМ и сетей ЭВМ. Такие правила должны устанавливаться специально и в обязательном порядке доводиться до пользователей. Тем не менее, при отсутствии на предприятии четких ограничений на работу с ЭВМ достаточно сложно будет установить, что наступление неблагоприятных последствий связано именно с фактом нарушения правил эксплуатации.

По данным статистики около 90% программного обеспечения на российском рынке определяется как контрафактное, то есть такое программное обеспечение, изготовление или использование которого влечет за собой нарушение авторских прав (например, такое распространенное явление, как «взлом» программного обеспечения). Контролировать распространение подобных программ в сети Internet практически невозможно. К тому же статья 146 УК РФ предусматривает ответственность за незаконное использование контрафактных экземпляров в целях сбыта, то есть получения материальной выгоды. Но встречаются случаи широкого распространения незаконного программного обеспечения «из рук в руки» и путем бесплатного скачивания из сети Internet.

По всем вышеописанным статьям предусмотрены сравнительно небольшие сроки лишения свободы (максимальный – до семи лет по статье 273, п.2), и во многих случаях дело ограничивается штрафом. Подобные меры, на мой взгляд, недостаточны для существенного влияния на темпы развития компьютерной преступности. Такие преступления на уровне международного законодательства стоят на третьем месте после торговли наркотиками и оружием, потому что ущерб от них оценивается миллионами долларов.

Расследование компьютерных преступлений пока еще существенно затруднено в связи с отсутствием отработанных и систематизированных методик, недостаточной судебной практикой. Необходима правильная работа с компьютерной информацией в ходе экспертизы. Работать с изъятым компьютером должны только квалифицированные профессионалы во избежание утраты ценной доказательной информации по неосторожности или по незнанию. Допуск к компьютеру его владельца в ходе экспертизы не должен разрешаться. Необходимо как минимум совершить следующее: проверить компьютер на наличие вирусов и программных закладок, сделать резервную копию всей информации (в том числе временных файлов), сравнить дубли документов.

При проведении изъятия компьютеров необходимо так же изъять все периферийные устройства, магнитные носители информации и опечатать их с последующим установлением конфигурации оборудования, серийных и инвентарных номеров. Так же необходим сбор всей

технической документации, документации о сотрудниках, о порядке и правилах функционирования системы и т. д.

Таким образом, можно сделать вывод, что настоящее законодательство в области компьютерных преступлений нуждается в совершенствовании. Так же повлиять на рост подобной преступности могло бы создание специальных правоохранительных органов, специализирующихся на компьютерных преступлениях.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ СТАНДАРТА ГОСТ 28147-89

А.М. Терзи, студент 4 курса гр. 522-3 каф. КИБЭВС
ТУСУР, г. Томск, amt2001@inbox.ru

В Российской Федерации установлен единый стандарт криптографического преобразования данных для информационных систем. Он носит обязательный характер для государственных органов, организаций, предприятий, банковских и иных учреждений, чья деятельность связана с обеспечением информационной безопасностью государства. Для других организаций и частных лиц ГОСТ имеет рекомендательный характер.

В данной статье рассматривается особенность программной реализации стандарта ГОСТа в программной среде Pascal.

Представление узлов замены

Современные средства вычислительной техники позволяют оперировать минимальным объемом информации в 1 байт, что представлено в виде регистров. В стандарте ГОСТа описывается работа с некоторыми данными (узлы таблицы замены) размером в четыре бита. При реализации такого механизма наиболее технологичнее и предпочтительнее было бы использование однобайтовой структуры.

В оригинале замена промежуточных данных из узлов замены (УЗ) происходит в восемь этапов по четыре бита каждый. Рациональнее произвести эту замену в четыре этапа по восемь бит. Так можно достичь и лучшего быстродействия за счет меньшего обращения к памяти и упрощения самого алгоритма реализации данного этапа. Для этого предполагается заменить стандартные УЗ на «расширенные» УЗ. «Расширенные» УЗ представляет собой четыре массива, состоящих из 256 элементов по одному байту. Каждый массив представлен спаренной парой узлов. Если условно разделить одну из четырех частей «расширенных» УЗ на i участков (где $i = 16$) по 16 байт каждый, то старшим полубайтам i-го участка будет соответствовать i-й элемент

первого узла замены из пары, а *j*-ому младшему полубайту *i*-го участка будет противопоставляться соответствующий *j*-ый элемент из второго узла замены пары, где для каждого $i \quad j = \overline{1,16}$.

Таким образом, получается вместо восьми узлов всего 4 спаренных узла замены. Следует отметить, что при такой замене не происходит какого-либо нарушения в алгоритме работы ГОСТа.

Инициализация в этом случае будет проходить в два этапа. Первый состоит в заполнении оригинальных УЗ 4-битовыми значениями из введенного пользователем 64-байтной последовательности. Второй этап состоит в организации «расширенных» УЗ из полученной на первом этапе оригинальных УЗ.

Ключевая информация

При формировании ключевой информации желательно получить равновероятное распределение «нулей» и «единичек» для избежания получить слабые ключи. Для этого можно применить один из двух способов выработки ключевой информации:

1. Получить с помощью датчика случайных (псевдослучайных) чисел 512-ти битовые последовательности. Первую половину этой последовательности подвергнуть криптопреобразованию в режиме простой замены ГОСТа, где в качестве ключевой информации использовать вторую половину последовательности.

2. Использовать хэш-функцию, полученную в результате преобразования ГОСТ Р 34.11-94. В результате преобразования как раз и получается свертка размером 256 бит.

Структура данных

Целесообразней в качестве типа представления информации использовать свой собственный тип, поскольку стандарт довольно широко использует разбиения на различные блоки. С учетом специфики реализации алгоритма в среде Pascal, а также оптимизации, как по времени выполнения, так и по занимаемой памяти предлагается использовать в качестве такой структуры записи с вариантами. В качестве вариантов можно использовать следующие типы:

1. указатель на данные;
2. тип блока при криптопреобразовании;
3. тип счетчика.

В качестве указателя используется не типизированный указатель, т.к. ему можно присвоить любой указатель, например, указатель на массив символов. При криптопреобразовании используются блоки по 32 бита, поэтому здесь также можно использовать запись с вариантами, где в качестве первого варианта использовать два двойных слова, а в качестве второго массив байт. Счетчик необходим для быстрого и

эффективного перемещения по массиву, где шаг перемещения составляет один и более байт.

Таким образом, массив данных можно представить в памяти как блоки в 64, 32 и 8 бит. При всем этом разнообразии представления одного и того же массива данных физически мы работает с одной и той же памятью.

Процедуры и функции

Перед началом работы необходимо произвести инициализацию. В процессе инициализации формируются УЗ, происходит разбиение ключа на 8 частей, а также производится выбор режима криптопреобразования. В соответствии с этими требованиями на вход такой функции подаются значения последовательности ТЗ, ключа и номер режима.

В криптопреобразовании используются функции шифрования и расшифрования, производя то или иное действие согласно выбранному режиму на этапе инициализации. Входными данными здесь будут являться указатели на входной и выходной буферы данных, размеры буферов, а также значения других параметров (например, синхропосылки). Использование буферов избавляет от необходимости в пределах функции создавать такие буферы, что при некоторых организациях алгоритма (например, в виде динамической библиотеки) позволяет избежать проблемы обращения к памяти.

Основной шаг и базовый цикл криптопреобразования выполнены в отдельных процедурах чтобы не загромождать код.

Заключение

Данная реализация наглядно демонстрирует пример нестандартного подхода к алгоритму весьма стандартными средствами языка Pascal. Она может быть интересна как в учебных целях, т.к. представлена в модульном варианте так и для реального применения, хотя для этого необходимо внести ряд изменений в сам алгоритм реализации а также произвести оптимизацию по необходимым критериям.

ЛИТЕРАТУРА

1. *Андрей Винокуров* Алгоритм шифрования ГОСТ 28147-89.
2. *Архангельский А.Я.* Программирование в Delphi 7, 2003.
3. *Баричев С.Г. и др.* Основы современной криптографии, М.: Горячая линия – Телеком, 2002. 175с.
4. *Скляров Д.В.* Искусство защиты и взлома информации СПб.: БХВ-Петербург, 2004. 288 с.
5. *Шнайер Б.* Прикладная криптография. М.: Издательство ТРИУМФ, 2002. 816 с.

СОЗДАНИЕ И РАЗБОР ЦИФРОВЫХ СЕРТИФИКАТОВ

Т.А. Торгаев, студент 5 курс; О.И. Галкин, аспирант
ТУСУР, каф. КИБЭВС, г. Томск.

1. Инфраструктура открытого ключа (PKI)

Инфраструктура открытого ключа – это система, в которой пользователи аутентифицируются по методу шифрования с открытым ключом.

Существенными частями инфраструктуры являются цифровые сертификаты. При их работе используется принцип асимметричного шифрования: один из двух ключей шифрования доступен всем (открытый), другой держится в секрете (закрытый). Любые данные, зашифрованные одним ключом, могут быть расшифрованы другим, и наоборот.

Для проверки подлинности сертификата, он снабжается подписью, зашифрованной ключом владельца сертификата (тогда сертификат является самоподписанным), или ключом удостоверяющего центра.

2. Назначение программы CreateCert

Программа CreateCert написана в среде визуального программирования Microsoft Visual Studio 2003, предназначена для создания сертификатов и запросов на сертификацию. Специально для программы были разработаны «с нуля» классы для работы с ACH1 объектами: кодирование, декодирование, классы работы с полями сертификатов, процедуры ввода имен с помощью строки управления.

Программа применяется для создания и редактирования сертификатов. CreateCert позволяет создавать сертификаты стандарта X.509 [3]. Для сертификатов второй и третьей версии есть возможность создания дополнительных полей, таких, как уникальные идентификаторы владельца, поставщика и расширения. Программа позволяет работать со всеми расширениями, которые в рекомендациях [3] указаны как критические.

CreateCert также позволяет создавать самоподписанные запросы на сертификаты версии 1, 2 и 3 в формате PKCS#10.

3. Общие принципы функционирования

Сертификат хранится и пересылается в формате ACH1, поэтому в ходе разработки программы созданы классы для работы с ACH1 объектами. Кодирование и декодирование происходит в полном соответствии с правилами.

При разборе сертификата учитывается порядок расположения и тип полей. Все обязательные поля сертификата расположены в порядке, одинаковом для сертификатов всех версий. Необязательные поля имеют свой уникальный контекстный номер или представлены в заранее описанном формате и снабжены уникальными идентификаторами.

Создание класса сертификата позволило как создавать сертификаты, так и открывать существующие сертификаты для чтения и изменения. Сертификат X.509 состоит из трех частей: основной части сертификата, информации об алгоритме подписи и самой подписи основной части. Данными для вычисления подписи является первая часть сертификата, представленная в закодированном согласно ACH1 виде. Основная часть сертификата содержит следующие обязательные поля: версия, серийный номер, алгоритм подписи, наименование поставщика, период действия, наименование субъекта, информация об открытом ключе субъекта.

Версия сертификата представлена в виде целого числа и может быть равна 0 (первой версии), 1 (второй) и 2 (третьей). Серийный номер тоже представляется в виде целого числа, но ввиду большой его длины вводится как массив октет в шестнадцатиричной форме записи. Максимальная длина серийного номера в октетах (байтах) – 20.

Алгоритм подписи должен содержать ту же информацию, что и вторая часть сертификата. Он генерируется автоматически при сохранении сертификата.

Наименование поставщика представлено в виде последовательности полей, содержащих тип аттрибута и его значение. В программе, возможно, вводить основные поля: наименование, организация, подразделение, страна и город. Структура классов универсальна и позволяет добавлять другие поля. Период действия состоит из двух полей: начало и окончание действия.

Наименование субъекта, как и наименование поставщика, представлено в виде последовательности типов аттрибутов и их значений.

Информация об открытом ключе субъекта состоит из идентификатора алгоритма шифрования и ключа. Существует возможность, как загрузить ключ с носителя (ключ должен быть в формате PKCS#10), так и сгенерировать (и сохранить) новый ключ. Программой поддерживается ассиметричный алгоритм шифрования RSA, в будущем планируется ввод поддержки CryptoPro CSP 3.0.

Если версия сертификата равна 2 или 3, то основная часть может содержать дополнительные поля: уникальные идентификаторы поставщика и субъекта, расширения. Уникальный идентификатор содержит дополнительную информацию об открытом ключе. Если версия сертификата равна 3, то он может содержать дополнительное поле «расширения».

Расширения сертификата X.509 версии 3 представляют собой методы для управления сертификатами и связывания дополнительных аттрибутов с пользователями или открытыми ключами. Формат сертификата X.509 версии 3 допускает использование частных расшире-

ний. Каждое расширение состоит из двух или трех полей: идентификатор расширения (обязательное), критичность (не обязательное) и значение расширения (обязательное).

В программе реализованы следующие расширения: идентификатор ключа сертификационного центра, идентификатор ключа субъекта, использование ключа, расширенное использование ключа, основные ограничения и политики сертификата.

ЛИТЕРАТУРА

1. *ITU-T* Recommendation X.208;
2. *ITU-T* Recommendation X.209;
3. *RFC 3280* «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».

ОБНАРУЖЕНИЕ ПРОГРАММ – КЛИЕНТОВ P2P СЕТЕЙ

К.В. Вилкин, студент 5 курса КИБЭВС,
Г.В. Петрова, ассистент каф. КИБЭВС
ТУСУР, г. Томск, т. 41-44-76, kot_03@pisem.net

Последнее время большое распространение получили так называемые пиринговые сети, то есть сети, основанные на технологии P2P (peer-to-peer). Как известно большинство компьютерных сетей построены по принципу «клиент-сервер». В технологии P2P было предложено отказаться от сервера и соединить клиентов сети напрямую.

Использование данных сетей создает большие сложности сетевым администраторам предприятий, вследствие огромной нагрузки на Internet канал. Поэтому необходимо создать механизм, позволяющий решить данную проблему.

В данной работе был предложен метод поиска и идентификации P2P приложений, написаны программы, реализующие данные функции.

1. Сканирование портов

Проверка на наличие открытых портов самый простой и распространенный из способов обнаружения использования P2P приложений. Он основывается на том, что большинство P2P приложений работают на заданных по умолчанию портах.

Этот способ эффективен только в том случае, если пользователь не настраивает приложение таким образом, чтобы в программе использовались случайные порты. При сканировании и нахождении открытых портов в диапазоне от 1024 до 65535 о наличии P2P клиента можно судить весьма неоднозначно, тем более идентификацию приложений можно произвести, только заранее зная на каком порту (default) работает P2P приложение.

2. Анализ трафика

P2P приложению с децентрализованной структурой необходимо периодически отправлять большое количество командных пакетов разного типа. Анализируя UDP трафик различных P2P приложений, была обнаружена закономерность – пакеты одного типа часто имеют одинаковый размер. Поэтому, анализируя UDP пакеты, даже при отсутствии информации прикладного уровня, можно точно определить, какое P2P приложение используется.

У большинства P2P приложений не документированы все детали реализации, некоторые поставляются с закрытыми исходными кодами, поэтому структура UDP пакетов большинства приложений может быть нам точно не известна. Были выбраны несколько популярных децентрализованных P2P приложений и проведены наблюдения. Результаты подтвердили гипотезу о том, что все выбранные приложения для взаимодействия с внешним миром используют пакеты фиксированной длины. Для достоверной идентификации приложения достаточно перехватить 35 пакетов за одну минуту.

3. Описание программы

Перед использованием программ необходимо выявить предполагаемый источник проблемы. Если известно несколько компьютеров, на которых, возможно, стоит P2P приложение следует воспользоваться программой scan.exe.

Т.к. программа scan.exe, как и sniffer.exe и analise.exe являются консольными приложениями использовать их удобнее всего из системной консоли cmd.exe.

Перед запуском scan.exe необходимо указать три входных параметра:

Ip – адрес компьютера, подлежащего сканированию; Начальный порт диапазона сканирования; Конечный порт диапазона.

Например: scan.exe 192.168.0.1 13505 13507. 13506 – порт программы Shareaza.

В процессе выполнения программа выводит на экран информацию о наличии открытых портов. Номера портов по умолчанию P2P приложений представлены в отчете по НИРС в главе: Анализ открытых портов.

Если сузить поиск до нескольких компьютеров стандартными методами не удается, следует провести анализ трафика. Чтобы иметь наиболее полную картину, трафик лучше всего перехватывать с зеркального порта коммутатора.

Для перехвата пакетов следует воспользоваться «sniffer.exe». Тесты показали, что для получения лучших результатов программа должна выполняться 30 секунд. По завершении выполнения программы формируется 3 лог-файла:

Log.txt – все перехваченные пакеты;

Ip.txt – Отфильтрованные IP адреса UDP пакетов;

Size.txt – Отфильтрованные размеры UDP пакетов.

Для анализа лог-файлов используется утилита «analise.exe». После завершения работы программа выдаст информацию о присутствии или отсутствии программ-клиентов, их адреса, список подозрительных адресов.

Для получения более достоверных данных администратору системы имеет смысл менять время сбора пакетов, т.к. количество отсылаемых P2P приложением пакетов напрямую зависит от интенсивности его использования.

5. Заключение

Так как программа является учебной и целью реализации не является использование ее как коммерческого программного продукта, то в ней реализованы не все возможности и функции присущие коммерческим программным продуктам в этой области (например, программы являются консольным приложением, что не очень удобно для использования).

При постоянном обновлении сигнатур и в будущей доработке алгоритма, в соответствии с развитием клиентов, возможно, ее широкое применение в практических целях на предприятиях.

ЛИТЕРАТУРА

1. www.securitylab.ru;
2. М. Финков, Пиринговые сети: eDonkey, BitTorrent, KaZaA, DirectConnect – НИТ, 2006г;
3. Самоучитель C++ / Г. Шилдт – СПб: БХВ-Петербург, 2002 – 688с;
4. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/windows_sockets_start_page_2.asp. Документация Microsoft, относительно сетевых функций их ОС Windows Socket 2.

ОБНАРУЖЕНИЕ ИСПОЛЬЗОВАНИЯ ПИРИНГОВЫХ СЕТЕЙ

К.В. Вилкин, студент 5 курса, КИБЭВС.,

Г.В. Петрова, ассистент кафедры КИБЭВС

ТУСУР, г. Томск, 414-476, kot_03@pisem.net

P2P – это класс приложений, совместно использующих распределенные ресурсы (дисковое пространство и файлы, вычислительные ресурсы, пропускную способность и т. д.) К этому определению и относятся пиринговые сети.

Сфера применения данной технологии довольно обширна, но на данный момент успешны только четыре направления: файловые обменные сети (file-sharing), распределенные вычислительные сети,

службы сообщений (Instant-messaging), сети групповой работы (P2P Groupware).

В данной работе рассматриваются только файловые обменные сети.

Все файловые обменные сети делятся на две большие категории:

– Централизованные. Несмотря на то, что каждый участник файловой обменной сети является и клиентом и сервером, необходима инфраструктура для объединения разрозненных клиентов между собой в определенное сообщество. В простейшем случае, это мощные индексационные сервера. Это сети: Napster, BitTorrent, Direct Connect;

– Децентрализованные. После закрытия крупнейших централизованных файловых обменных сетей, стали выискиваться способы объединения участников без использования уязвимых индексационных серверов. И такие способы были найдены в специальных алгоритмах организации, хранения, распределения и поиска информации между всеми участниками сети. Хотя объем передаваемой служебной информации в них выше, надежность их гораздо выше. Это сети: Gnutella, Overnet, eDonkey, Emule Kad Network, BitTorrent Distributed DB.

Многие сетевые администраторы хотели бы обнаружить и попытаться заблокировать на своих межсетевых экранах P2P – трафик из-за создаваемой им высокой нагрузки на каналы (при интенсивном использовании пиринговые сети могут полностью блокировать Internet канал предприятия), последствиям для безопасности, вызванными неконтролируемым обменом файлами, а также возможными судебными исками со стороны владельцев авторских прав. Это не так просто, как может показаться. На данный момент не существует способа насильно остановить функционирование таких сетей, но обнаружить, возможно, и в последствии решить проблему организационными методами.

В данной работе проведено исследование принципов функционирования P2P сетей, и предложено несколько методов их обнаружения.

Методы обнаружения пиринговых сетей

На данный момент ведется разработка программы, предназначенной для обнаружения P2P сетей. В программе предусмотрены три метода обнаружения, рассмотренные ниже.

Перехват и анализ сетевого трафика на уровне протоколов

Суть данного метода в мониторинге трафика, проходящего через сеть, на предмет обнаружения определенных сигнатур, специфичных для P2P приложений.

Исходя из спецификаций протоколов и проведенных исследований, будут составлены сигнатуры пакетов, с которыми анализатор будет сравнивать трафик локальной сети. При успешной реализации данного метода станет возможным со 100% вероятностью определить использование P2P сетей.

Статистический метод

P2P приложению с децентрализованной структурой необходимо периодически отправлять большое количество командных пакетов разного типа. Анализируя UDP трафик различных P2P приложений, была обнаружена закономерность – пакеты одного типа часто имеют одинаковый размер. Поэтому, анализируя UDP пакеты, даже при отсутствии информации прикладного уровня, можно точно определить, какое P2P приложение используется.

У большинства P2P приложений не документированы все детали реализации, некоторые поставляются с закрытыми исходными кодами, поэтому структура UDP пакетов большинства UDP приложений может быть нам точно не известна. Были выбраны несколько популярных децентрализованных P2P приложений и проведены наблюдения. Результаты подтвердили гипотезу о том, что все эти приложения для взаимодействия с внешним миром используют пакеты фиксированной длины.

Сканирование портов

Проверка на наличие открытых портов самый простой и распространенный из способов обнаружения использования P2P приложений. Он основывается на том, что большинство P2P приложений работают на заданных по умолчанию портах.

Этот способ эффективен только в том случае, если пользователь не настраивает приложение таким образом, чтобы в программе использовались случайные порты. При сканировании и нахождении открытых портов в диапазоне от 1024 до 65535 о наличии P2P клиента можно судить весьма неоднозначно, тем более идентификацию приложений можно произвести, только заранее зная на каком порту (default) работает P2P приложение.

Заключение

В данной работе была проанализирована специфика работы пиринговых сетей, рассмотрены методы обнаружения работающего P2P приложения. Исходя из полученных результатов, самым эффективным методом считается анализ трафика на предмет обнаружения определенных сигнатур, специфичных для P2P приложений.

ЛИТЕРАТУРА

1. *Финков М.* Пиринговые сети: eDonkey, BitTorrent, KaZaA, DirectConnect – НИТ, 2006г;
2. www.bittorrent.com/protocol.html – Official BitTorrent Protocol Specification;
3. http://dcplusplus.sourceforge.net/wiki/[Client-Hub/Client-Client] – DC project protocols;
4. http://sourceforge.net/projects/pdonkey/- eDonkey/eMule Protocol Specification;
5. http://www9.limewire.com/developer/gnutella_protocol_0.4.pdf – 0.4 Gnutella Protocol Specification.

ПРОЕКТ ПО СОЗДАНИЮ CRYPT-ПРИЛОЖЕНИЯ

С.Л. Крыловский, студент 3 курса;
М.Г. Власова, студентка 3 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 8-903-951-1825,8-913-851-3569

Расширяющееся применение информационных технологий при создании, обработке, передаче и хранении документов требует в определенных случаях сохранения конфиденциальности их содержания, обеспечения полноты и достоверности.

Одним из эффективных направлений защиты информации является криптография, широко применяемая в различных сферах деятельности в государственных и коммерческих структурах.

Криптографические методы защиты информации являются объектом серьезных научных исследований и стандартизации на национальных, региональных и международных уровнях.

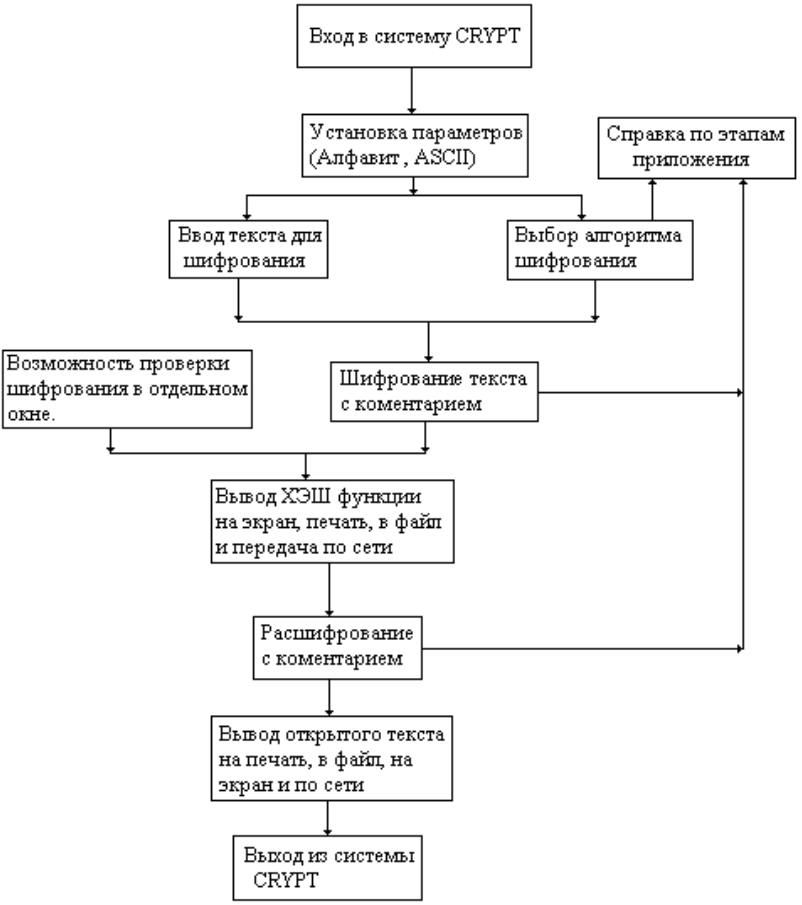
Поставленная задача состояла в создании универсального защищенного программного продукта для обучения студентов базовым методам защиты информации. Приложение должно быть эффективным, надежным, наглядным и простым в использовании. Создание этого приложения облегчит студентам обучение, в связи с автоматизацией сложных алгоритмов шифрования и расшифрования с помощью ЭВМ.

Для решения поставленной задачи использовался программный продукт Delphi 7[1]. Основной процесс работы приложения показан на рисунке.

При запуске приложения перед пользователем появляется форма «Шифрование и расшифрования сообщений». Установив параметры шифрования и заполнив поле «Текст для шифрования» необходимо выбрать алгоритм шифрования и нажать на кнопку «Шифровать». В поле «комментарии» с каждым шагом будет появляться результат шифрования. После этого в поле «Вывод» отобразится ХЭШ – функция. Результат можно вывести на печать, в файл или по сети. Для проверки шифрования можно включить окно сопровождения «Процесс» с возможностью корректировки ключа и т.д. На этапе расшифрования действия, производимые с Хэш-функцией, аналогичны этапу шифрования: контроль обратного ключа и т.п.

Для того чтобы просмотреть результаты на промежуточных стадиях необходимо выбрать в «Параметры»| «Число итераций» количество итераций, результаты которых будут представлены в окне «Процесс».

Выход из программы осуществляется выбором в меню «Файл»| «Выход». Информацию о программе можно получить в меню «Помощь» | «О программе». Справку можно получить выбором в меню «Помощь».



Процесс работы в системе CRYPT

Выводы. В процессе данной работы было спроектировано приложение CRYPT , реализующее выполнение необходимых операций шифрования и расшифрования, при этом студент может не только наблюдать результаты этих операций, но и вмешиваться в сам процесс: проверять правильность, исправлять ошибки в подборе ключей, а также контролировать процесс на каждом шаге его выполнения.

ЛИТЕРАТУРА

1. *Архангельский А.Я.* Программирование в DELPHI 7 – М.: Издательство «БИНОМ»,2005 – 1151 с.

СИСТЕМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ДОКУМЕНТОВ

Г.А. Юрков, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, т.77-40-91, yur_alex@rambler.ru

Объектом исследования является сайт предприятия-заказчика с возможностью интерактивного взаимодействия с документами, такими как создание, распечатка, пересылка и т.д. Поскольку доступ осуществляется по незашифрованному каналу, то создание эффективной системы защиты обязательно, так как налицо множество каналов утечки информации. Система защиты позволяет без лишнего программного обеспечения подписывать документы, проверять подпись оператора, использовать CryptoAPI, для подписи документов, тем самым не реализуя сам процесс подписи.

Для эффективного встраивания своего приложения в веб-форму для начала необходимо уделить много внимания выбору средств написания. Для этого неподходят многие подходы, такие как язык Java. Этот язык неподходит для таких целей поскольку не имеет обычных вызовов API функций в явном виде, так как это происходит, к примеру, во многих языках программирования. Для этой цели был использован подход с применением технологии ActiveX.

По своей сути платформа ActiveX – это адаптация существующих технологий Microsoft применительно к Web. Данная концепция базируется на механизмах OLE и COM – проверенных временем и ставших стандартами разработок для Windows. Поскольку само приложение должно вызывать функции CryptoAPI, то выбор был остановлен на языке C, эффективно и довольно быстро имеющий в своем арсенале средства для разработки данного приложения. CryptoAPI для этого предоставляет все необходимые средства по использованию как генерации ключей подписи, так и саму подпись, не обращая внимания на реализацию самих шифров и самой подписи.

Реализация всех алгоритмов (шифрования, цифровой подписи и т.п.) полностью выведена из состава самого Crypto API и реализуется в отдельных, независимых динамических библиотеках – «криптопровайдерах» (Cryptographic Service Provider – CSP). Сам же Crypto API просто предъявляет определенные требования к набору функций (интерфейсу) криптопровайдера и предоставляет конечному пользователю унифицированный интерфейс работы с CSP. Конечному пользователю для полноценного использования всех функций криптопровайдера достаточно знать его строковое имя и номер типа. Кроме задачи расширения одной из основных задач Crypto API является возможность однозначной идентификации передающей/принимающей стороны в протоколе передачи данных. Общепризнанным решением в дан-

ном вопросе является использование механизма сертификатов. Сертификаты как бы стали «цифровыми паспортами», несущими информацию о своих владельцах. Crypto API также полно реализует весь спектр функций работы с ним. Большинство функций Crypto API, работающих с передаваемыми данными, так или иначе, используют сертификаты в своей работе.

В программных решениях рано или поздно встает вопрос стандартизации передаваемых между приложениями данных. В сфере криптографии для решения данного вопроса уже давно и успешно применяет набор стандартов «PKCS», предложенный компанией RSA Security. В данном комплекте стандартов учитываются все возможные случаи, возникающие в криптографических приложениях. Предусмотрены стандарты для обмена сертификатами, зашифрованными и подписанными данными и многое другое. Crypto API, как основная библиотека для обеспечения работы с криптографическими данными в Windows, также достаточно полно поддерживает данный комплект стандартов и позволяет формировать криптографические приложения, которые могут быть обработаны в дальнейшем любыми программными продуктами.

Таким образом, все описанные средства и методы позволяют выполнить поставленную задачу. Использование сертификатов в данной системе позволяет автоматизировать процесс передачи ключей, не заботясь непосредственно об их хранении, передачи и т.д. Также необходимо отметить, что в данной системе присутствует возможность выбора криптопровайдера для подписи и проверка подписи «на лету».

ЛИТЕРАТУРА

1. *Страуструп Б.* «C++ для программистов», Справочное пособие, 2000.
2. http://citforum.ru/article/rsdn10.html – описание работы с сертификатами X.509 через CryptoAPI.
3. http://cybersecurity.ru – описание сертификата X.509.

ОБМАННЫЕ СИСТЕМЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.Д. Зыков, студент 4 курса;
С.И. Коковин, студент 4 курса ккаф. КИБЭВС
ТУСУР, г. Томск, iceman@ms.tusur.ru

Обычно, когда речь заходит об обмане в области информационной безопасности, сразу вспоминаются попытки злоумышленников использовать те или иные скрытые лазейки для обхода используемых средств защиты. Однако обман может сослужить хорошую службу не

только для злоумышленников, но и для защитников корпоративных ресурсов. Сразу необходимо отметить, что обман очень редко используется в качестве защитного механизма.

Существует несколько различных вариантов использования обмана в благих целях. Можно выделить следующие механизмы обмана:

1. сокрытие;
2. камуфляж;
3. дезинформация.

В той или иной мере эти механизмы используются в практике работ отделов безопасности. Однако, как правило, эти механизмы используются не для информационной, а для иных областей обеспечения безопасности (физическая, экономическая и т.д.).

В области информационной безопасности наибольшее распространение получил первый метод – сокрытие. Ярким примером использования этого метода в целях обеспечения информационной безопасности можно назвать сокрытие сетевой топологии при помощи межсетевого экрана.

Примером камуфляжа можно назвать использование Unix-подобного графического интерфейса в системе, функционирующей под управлением операционной системы Windows NT. Если злоумышленник случайно увидел такой интерфейс, то он будет пытаться реализовать атаки, характерные для ОС Unix, а не для ОС Windows NT. Это существенно увеличит время, необходимое для «успешной» реализации атаки.

Менее известным является метод дезинформирования. Принципиальное отличие дезинформирования от других механизмов обмана состоит в том, что другие методы направлены на затруднение обнаружения объекта с информацией среди других объектов, а дезинформирование – на создание ложного объекта, среди других объектов.

Дезинформирование в целях защиты информации можно использовать по-разному, в зависимости от способа атаки.

Например, в случае кражи автоматизированной системы (АС) или носителей с информацией, можно подделывать хранимые документы, тем самым навязывать злоумышленнику ложную информацию.

В случае различных атак на АС, можно использовать дезинформирование и камуфляж для эмулирования тех или иных известных уязвимостей, которых в реальности не существует. Использование подобных обманных систем приводит к следующему:

• Увеличение числа выполняемых нарушителем операций и действий. Так как заранее определить является ли обнаруженная нарушителем уязвимость истинной или нет, злоумышленнику приходится выполнять много дополнительных действий, чтобы выяснить это.

• Получение возможности отследить нападающих. За тот период времени, когда нападающие пытаются проверить все обнаруженные уязвимости, в т.ч. и фиктивные, администраторы безопасности могут проследить весь путь до нарушителя или нарушителей и предпринять соответствующие меры, например, сообщить об атаке в соответствующие «силовые» структуры.

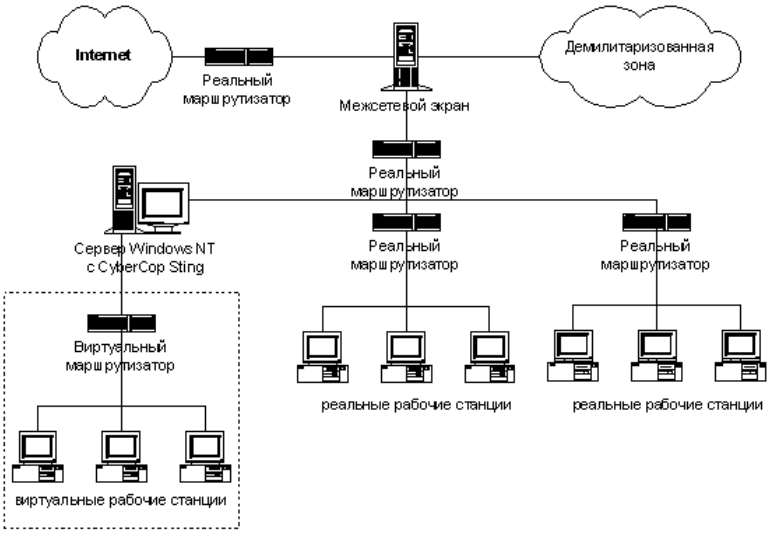
В настоящий момент широко известны две обманные системы, в той или иной степени, реализующие описанные выше методы. Первая из них – The Deception Toolkit (DTK) предназначена для работы под управлением различных Unix. Вторая – CyberCop Sting компании Network Associates, функционирует под управлением ОС Windows NT.

Набор инструментальных обманных средств (The Deception Toolkit, DTK) является первым средством, предназначенным для реализации механизма обмана злоумышленников, пытающихся проникнуть в сеть организации. Данное средство эмулирует несуществующие сервисы и порты. Создаваемые сканерами безопасности отчеты не смогут помочь злоумышленнику определить какие из обнаруженных уязвимостей являются реальными, а какие нет. Тем самым злоумышленнику придется тратить время и ресурсы на проверку всех обнаруженных уязвимостей, что позволит своевременно обнаружить такие попытки и противопоставить им эффективные средства защиты и, возможно, обнаружить злоумышленника.

CyberCop Sting «создает» виртуальную сеть на выделенном узле. Каждый из виртуальных узлов имеет один или несколько IP-адресов, на которые можно посылать сетевой трафик и получать вполне «реальный» ответ. В более сложных случаях виртуальный узел может выступать в роли ретранслятора пакетов на невидимый, но реальный компьютер, который и отвечает на все запросы злоумышленника.

Главное достоинство системы CyberCop Sting в том, что для моделирования «приманки» для нарушителя не требуется большого количества компьютеров и маршрутизаторов, – все реализуется на единственном компьютере (рисунок).

Применение обманных систем – это достаточно интересный и при правильном применении эффективный метод обеспечения информационной безопасности. Не стоит забывать, что обманные системы – это не панацея от всех бед. Они помогают в случае простых нападений, осуществляемых начинающими или неопытными злоумышленниками. Конечно, число действительно квалифицированных злоумышленников не так велико и поэтому использование обманных средств может помочь в большинстве случаев, тем не менее не надо забывать и про другие средства защиты. Можно порекомендовать использовать связку защитных средств «обманные системы – системы обнаружения атак», которая позволит не только обнаружить нападающего сразу же после первой попытки атаки, но и заманить его при помощи обманной



Применение системы CyberCop Sting для создания виртуального сегмента корпоративной сети

системы, тем самым, давая время на обнаружение злоумышленника и принятие соответствующих мер. Только комплексное применение всех этих средств наряду с организационными и законодательными мерами позволит обеспечить действительно надежную и эффективную защиту от злоумышленников.

ОСОБЕННОСТИ НАСТРОЙКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ БАНКОМАТОВ И ЭКВАЙРИНГА

И.А. Кондратьев, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, т. 8-913-824-73-69 , e-mail ilchik@sibmail.com

ЗАО Внешторгбанк Розничные услуги входит в группу ВТБ, являясь дочерним банком ОАО Внешторгбанк, специализируется на обслуживании физических лиц, индивидуальных предпринимателей, организаций малого бизнеса.

ЗАО Внешторгбанк Розничные услуги предлагает широкий спектр продуктов и услуг для частных лиц и предприятий малого бизнеса – потребительское кредитование, услуги дистанционного банкинга, ипотечное кредитование, кредитные карты с льготным периодом, срочные

вклады, аренду сейфовых ячеек, выпуск пластиковых карт, денежные переводы, ряд программ кредитования малого и среднего бизнеса и др.

Одним из приоритетных направлений в работе банка является развитие системы обслуживания пластиковых карт:

– увеличение числа клиентов-держателей пластиковых карт;

– расширение сети банкоматов и депозитарных машин;

– расширение сети приема безналичных платежей за товары и услуги по пластиковым картам.

В нашем банка для обеспечения связи банкоматов и процессинга используют следующие типы оборудования:

– модемы Zyxel для работы на выделенных линиях;

– коммуникационное оборудование фирмы NSG

– коммуникационное оборудование фирмы Cisco Systems

В настоящий период компания NSG производит и поставляет широкий спектр сетевого оборудования различной производительности:

– Мультипротокольные маршрутизаторы и коммутаторы пакетов;

– Устройства доступа к сетям Frame Relay (FRAD) и устройства сборки-разборки пакетов для сетей X.25 (PAD);

– Аппаратуру доступа в Internet, включая решения «последней мили» на основе xDSL;

– Оборудование X.25 для банкоматов и POS-терминалов;

– Интеллектуальные адаптеры для персональных компьютеров;

– Протокольные анализаторы, тестеры и др.

Большинство устройств NSG представляет собой многофункциональные шасси, снабженные универсальными портами для установки сменных интерфейсных модулей.

Для работы эквайринга в «ВнешТоргБанк Розничные услуги» применяется программное обеспечение «INPAS SmartAccess».

Необходимость решения проблем, связанных с использованием в карточных проектах разнотипного оборудования (сети кассовых аппаратов, таксофоны, GSM терминалы, специализированные платежные терминалы, ранее использовавшиеся для работы с другим процессинговым центром), и разнообразные внешние программно-аппаратные комплексы), приводит к спросу на дополнительные программно-аппаратные решения, осуществляющие различные варианты конвертации протоколов с предварительной обработкой транзакций как на коммуникационном, так и на прикладном уровне.

Программное обеспечение «INPAS SmartAccess верс.1.0.» (далее ПО «ISA» представляет собой 32-разрядное приложение, функционирующее в среде Windows и обеспечивающее взаимодействие терминального оборудования с процессинговыми центрами. ПО «ISA» вклю-

чает возможность сбора и обработки статистической информации и, в случае необходимости, автоматического формирования журналов операций и выгрузку данного журнала, если процессинговый центр, обслуживающий этот терминал, требует выполнения подобной операции.

ПО «ISA» представляет собой самостоятельный продукт, поддерживающий несколько типов входных протоколов и обеспечивающий возможность преобразования данных протоколов в один либо несколько других, используемых для авторизации процессинговыми системами. К внешним устройствам или системам, которые при помощи ПО «ISA» могут быть использованы при проведении платежей с использованием пластиковых карт, можно отнести любые устройства или системы, формирующие информацию, достаточную для проведения финансовой транзакции в форматах, поддерживаемых ПО «ISA» и обеспечивающие достаточный контроль за процессом их использования. Связь с процессинговым центром может осуществляется через порт RS-232, карту X.25 (EiconCard) или карту Ethernet с возможностью конфигурирования сценаиев установления соединения. Связь может устанавливается одновременно по нескольким каналам, если конфигурация ПО «ISA» предполагает такую возможность. Обеспечена возможность автоматического использования альтернативных вариантов соединения сервера с процессинговым центром в случае выхода из строя, либо чрезмерной загрузки основного канала связи.

ПО «ISA» настраивается для конкретного заказчика и обеспечивает выполнение всех операций согласно используемого протокола в объеме, реализованном в программном обеспечении и согласованном со службой автоматизации конкретного банка.

ЛИТЕРАТУРА

1. Руководство администратора «Программное обеспечение INPAS SmartAccess».
2. Диск поддержки продуктов NSG
3. http://www.nsg.ru
4. http://www.bankom.ru
5. http://www.nsr.ru
6. http://vtb24.ru

ПОДСЕКЦИЯ 9.3

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

SECRET DISK – ПРАВИЛЬНЫЙ ПОДХОД

В.В. Алехин, студент 3 курса
ТУСУР, г. Томск, avv@ms.tusur.ru

Уже много лет на рынке средств защиты информации присутствуют так называемые аппаратные ключи защиты. В наше время наиболее широкое распространение получили ключи выполненные в виде Usb-брелоков и смарт-карт.

Существует множество программно-аппаратных комплексов, созданных компаниями-разработчиками для хранения конфиденциальных данных. Наиболее простой и удобной программой для ежедневного использования на рабочем месте и дома является Secret Disk, разработанная компанией Aladdin.

Secret Disk включает в себя несколько приложений и электронный ключ, выполненный в виде смарт-карты или брелока e-token. Принцип работы прост. Программа генерирует личный ключ пользователя, записываемый в аппаратное устройство идентификации. Затем пользователь создает секретные диски, которые могут быть зашифрованы с помощью предложенных криптографических алгоритмов. Пользователь может выбрать любую удобную для него файловую систему. Информация, при обращении к диску, мгновенно шифруется/дешифруется с помощью личного ключа и пароля.

В ходе проделанных пользователем операций на жестком диске создается файл расширения .vd. Это и есть ваш секретный диск. Обращение к нему может быть произведено только при помощи программы Secret Disk и присутствии usb-ключа, либо смарт-карты. Без аппаратного ключа доступ к данным невозможен.

Файл секретного диска не может быть вскрыт злоумышленником без наличия аппаратного ключа владельца и знания его PIN-кода, но этот файл может быть им удален при обнаружении. Для этого ему необходимы лишь права администратора машины, на носителях которой хранится файл секретного диска. И, соответственно, все данные, которые находились на тот момент на секретном диске, будут безвозвратно утеряны. Для того, чтобы этого избежать, нужно регулярно выполнять резервное копирование файла секретного диска. Резервное копирование можно производить на другой магнитный носитель, либо на сервер Internet. Но эти копии так же могут быть обнаружены злоумышленни-

ком и ликвидированы. Чтобы этого не произошло владельцу Secret Disk нужно выработать систему, при использовании которой владелец сможет максимально обезопасить свою информацию.

Самое важное в мероприятиях по защите личной и конфиденциальной информации – это комплексный подход. В данной статье предлагается следующий:

После завершения работы с секретным диском пользователь при помощи соответствующего программного обеспечения производит запись .vd файла на CD/DVD RW (в зависимости от размера файла). Записанный диск можно хранить в любом месте, надежном с точки зрения владельца: банковский или домашний сейф, при себе, либо передать диск доверенному лицу. После записи диска необходимо удалить с жесткого диска файл секретного тома, предварительно отключив его в Secret Disk. Когда секретный диск вновь потребуется для изменения/обновления данных, копируем .vd файл с CD/DVD носителя на жесткий диск и, указав соответствующий путь, подключаем секретный диск в программе Secret Disk. Потом стираем перезаписывающийся CD/DVD диск и записываем на него файл секретного тома с уже измененными данными, снова проделывая описанные выше операции.

Данный подход позволяет оградить данные, хранящиеся на секретном диске от удаления, в случае обнаружения файла секретного диска злоумышленником.

ЛИТЕРАТУРА

1. *Скляров Д.В.* Искусство защиты и взлома информации. М.: Издательский дом «Питер», 2004. 288 с.
2. *Сидоренко Ю.* Secret Disk на страже данных, Компьютерное обозрение. № 26. Киев.

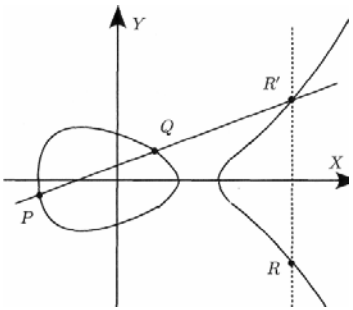
РЕАЛИЗАЦИЯ И ИССЛЕДОВАНИЕ МЕТОДОВ УВЕЛИЧЕНИЯ ЭФФЕКТИВНОСТИ РАБОТЫ КРИПТОЯДРА

Д.А. Бергер, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 8-903-953-48-24, e-mail dmitry@rdc.tomsk.ru

Эллиптические кривые давно изучались в математике, но их использование в криптографических целях было впервые предложено Коблицом и Миллером в 1985 году. Пятнадцать лет интенсивных исследований этих систем подтвердили их полезные свойства и привели к открытию множества эффективных методов их реализации. С 1998 г. использование эллиптических кривых для решения криптографиче-

ских задач, таких, как цифровая подпись, было закреплено в стандартах США ANSI X9.62 и FIPS 186-2, а в 2001 г. аналогичный стандарт, ГОСТ Р34.10-2001, был принят и в России.

Основное достоинство криптосистем на эллиптических кривых состоит в том, что по сравнению с «обычными» криптосистемами они обеспечивают существенно более высокую стойкость при равной трудоемкости или, наоборот, существенно меньшую трудоемкость при равной стойкости. Это объясняется тем, что для вычисления обратных функций на эллиптических кривых известны только алгоритмы с экспоненциальным ростом трудоемкости, тогда как для обычных систем предложены субэкспоненциальные методы. В результате тот уровень стойкости, который достигается, скажем, в RSA при использовании 1024-битовых модулей, в системах на эллиптических кривых реализуется при размере модуля 160 бит, что обеспечивает более простую как программную, так и аппаратную реализацию.



Вид эллиптической кривой

Кривая третьего порядка, задаваемая уравнением вида $y_2 = x_3 + ay_2 + c$, называется эллиптической кривой. Общий вид кривой представлен на рисунке.

На множестве точек вводится операция сложения. Для сложения точек P и Q (рисунок) необходимо провести через них прямую. Симметричное отображение третьей точки пересечения прямой с эллиптической кривой R является результатом операции. При удвоении точки секущая превращается в касательную. Точки с координатами (x, y) и $(x, -y)$ являются обратными по отношению к операции сложения. Сумма таких точек равна особой бесконечно удаленной от эллиптической кривой точке, принимаемой за нулевой элемент.

В криптографических приложениях используются эллиптические кривые, заданные над кольцом вычетов Zp. Множество точек эллиптической кривой вместе с нулевой точкой образуют Абелеву группу.

Операция умножения точки на скаляр вводится как многократное сложение точки самой с собой:

Для создания криптографических алгоритмов, использующих эллиптические кривые, необходима эффективная реализация операций модулярной арифметики больших чисел, в частности модулярная редукция, сложение, вычитание, умножение, инверсия.

Исследования показали, что реализация операций сложения, удвоения и умножения на скаляр точек эллиптической кривой в аффин-

ных координатах проблематична, так как, например, при умножении требуется большое число инверсий – самых длительных операций. Переход от аффинных координат в проективные $P(x, y) \rightarrow P(X, Y, Z)$ позволяет полностью избавиться от данных операций. При этом прямое преобразование происходит тривиально: $X = x$, $Y = y$, $Z = 1$. А обратное – требует одной инверсии и двух умножений: $x = X/Z^2$, $y = Y/Z^3$. Сложение точек в аффинных координатах эквивалентно 16 обычным умножениям, а удвоение – 10.

Для умножения точки на число целесообразно использовать некоторые адаптированные для аддитивного случая алгоритмы экспоненциации, например алгоритм с окном фиксированного размера (3–4 бита) или алгоритм с представлением экспоненты в троичной системе счисления (–1, 0, 1).

Основные характеристики, положенные в основу при проектировании блока работы с большими числами:

– отказ от повсеместного использования динамической памяти;

– использование чисел фиксированного размера;

– изначальное профилирование на использование модулярных операций;

– использование специализированных алгоритмов редукции;

– использование ассемблера в наиболее важных для скорости выполнения местах.

Таким образом, библиотека создавалась с расчетом на использование в конкретных условиях ГОСТ Р34.10-2001.

Были реализованы следующие операции:

– сложение и вычитание с применением ассемблера;

– логический сдвиг;

– классический алгоритм деления;

– алгоритм редукции Барретта с предвычислением;

– модулярное умножение;

– частичное умножение (быстрое вычисление старшей или младшей части результата);

– вычисление НОД по бинарному алгоритму Евклида;

– инверсия по бинарному расширенному алгоритму Евклида.

При реализации блока работы с группой точек эллиптической кривой широко использовались особенности работы библиотеки больших чисел. В блоке происходит сквозное преобразование координат, то есть аффинные координаты во внешнем представлении преобразуются в проективное внутреннее представление и обратно. Такая архитектура позволяет существенно увеличить производительность основных операций и является удобной при реализации алгоритмов электронной цифровой подписи с использованием эллиптических кривых.

Описанные выше блоки будут в дальнейшем использованы в составе криптоядра, реализующего процедуры электронной цифровой подписи по ГОСТ Р34.10-2001. Прогнозируемое на основе опытных данных время генерации и проверки подписи составляют примерно 33 и 66 мс соответственно (Intel P4 3.06 ГГц). По данным показателям разрабатываемая система приближается к существующим решениям и, возможно, опередит их.

ЛИТЕРАТУРА

1 *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. 328с.

2 *Menezes A., P. van Oorschot, Vanston S.* Handbook of Applied Cryptography, CRC Press, 1996.

ЗНАЧИМЫЕ ЛИЧНОСТНЫЕ КАЧЕСТВА КИБЕРПРЕСТУПНИКА

И.В. Давыдов, аспирант; К.Н. Филькин, аспирант

ТУСУР, каф. КИБЭВС, г. Томск, davidoffi@mail.ru; astron@ngs.ru

Мы живем в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства – от решения проблем национальной безопасности, здравоохранения и управления транспортом до торговли, финансов, и даже простого межличностного общения. Человек был уязвим всегда, но стал беззащитен вдвойне – не только в реальной жизни, но и в киберпространстве, в мире, моделируемом с помощью компьютеров. Общество поставило себе на службу телекоммуникации и глобальные компьютерные сети, не предвидя возможностей для злоупотребления этими технологиями. Сегодня жертвами киберпреступников могут стать не только люди, но и целые государства. При этом безопасность тысяч пользователей может оказаться в зависимости от нескольких преступников. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности, например, в глобальной сети Интернет, являются самыми быстрыми на планете.

Внедрение современных информационных технологий привело, к большому сожалению, к появлению новых видов преступлений, таких как компьютерная преступность и компьютерный терроризм – кибертерроризм.

Для эффективной борьбы с этим нарастающим явлением необходимо принимать неотложные меры. Одной из таких мер может послужить построение модели киберпреступника, что впоследствии позволит построить эффективную модель противодействия.

Классификация лиц, совершающих преступления в сфере компьютерной информации, неоднократно рассматривалась в криминалистической литературе. В их числе обычно особо выделяется группа так называемых «хакеров». Эти лица характеризуется в криминалистической литературе как профессионалы высокого класса, использующие свои интеллектуальные способности для разработки способов преступных посягательств на компьютерную информацию (преимущественно «взломов» систем компьютерной защиты и безопасности).

Как показывает проведенное Головиным А.Ю. эмпирическое исследование большинство «хакеров» – это в 32,9% изученных случаях молодые люди в возрасте от 16 до 30 лет. В этой возрастной группе «хакеры» составляют около 80%, на их долю приходится приблизительно 30% всех случаев незаконного удаленного доступа к компьютерной информации.

Также данные свидетельствуют о том, что в 78,4% случаев лица, совершающие компьютерные преступления – мужчины. Среди субъектов преступления преобладают лица с высшим и неоконченным высшим техническим образованием – 52,9% (иное высшее и неоконченное высшее образованием имеют 20% субъектов компьютерных преступлений, средне-специальное техническое образование –11,4%, иное образование – 15,7%).

Анализ личности киберпреступника позволяет выделить следующие немаловажные личностные качества киберпреступника, такие как: профессионализм в области компьютерной техники, знание уголовного законодательства в области обеспечения информационной безопасности и смежных областях (мошенничество, кража, изготовление подделок и т.д.), принадлежность к организованным преступным группам, а также социальное положение в обществе и киберпространстве. Вышеперечисленные факторы в большей степени влияют на мотивацию принятия решения для преступной деятельности в сфере компьютерных технологий. Таким образом, по поведению киберпреступника в сети и по совершенному киберпреступлению, а именно по оставшимся следам, можно сделать вероятностные выводы о его профессиональном образовании, о его познаниях в области информационного права, о его принадлежности к какой-либо организованной группе, о его социальном положении и т.д. Данные выводы окажутся просто необходимыми для оперативно-розыскных мероприятий, поскольку позволят

значительно сузить круг подозреваемых лиц. А это, несомненно, скажется на эффективности проводимых действий, и затраченном времени.

Так, например, беспардонная дерзость киберпреступника в сочетании с высоким профессионализмом очень часто свидетельствует об отсутствии познаний в уголовном законодательстве и ответственности за совершенные деяния. О принадлежности к какой-либо группе можно узнать, например, по индивидуальному набору киберпреступника, который будет содержать помимо «инструментов» специфическую информацию о какой-либо группе (организованные группы размещают информацию о своей деятельности с целью запугивания). Социальную принадлежность можно установить в случае «виртуального контакта», т.е. по стилю речи киберпреступника, его предпочтения и т.п.

В сочетании с другой информацией полученной о личности киберпреступника (от провайдеров, сетевых администраторах и т.п.) круг подозреваемых лиц будет значительно уменьшен. В результате, время, затраченное на поиск киберпреступника, будет сведено до минимума и количество следов будет максимально, что приведет к существенному росту раскрываемости.

ЛИТЕРАТУРА

1. *Shinder D.L.* Scene of the Cybercrime: Computer Forensics Handbook, Chapter 1, Facing the Cybercrime Problem Head On, Center for Strategic and International Studies, Washington, D. 2002.
2. *Вехов В.Б.* Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники. М.: ЦИ и НМОКП МВД России, 2000. 64 с.
3. *Голубев В.А.* Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий. http://www.crime-research.org/library/Golubev0104.html.
4. *Криминалистическая* методика расследования отдельных видов преступлений: Учебное пособие в 2-х частях. Ч. 2: / Под ред. А.П. Резвана, М.В. Субботиной. М.: ИМЦ ГУК МВД России, 2002. 232 с
5. *Криминалистика.* Учебник. Изд. 2-е, доп. и перер. / Под редакцией д.ю.н, профессора Закатова А.А., док. юрид. наук, профессора Смагоринского Б.П. М.: ИМЦ ГУК МВД России, 2003. 432 с.
6. *Егорышев А.С.* Криминалистический анализ лиц, осуществляющих неправомерный доступ к компьютерной информации. / Южно-уральские криминалистические чтения. Сборник научных статей: Выпуск 10 / Под редакцией И.А. Макаренко. Уфа: РИО БашГУ, 2002. С. 76–81.
7. *Головин А.Ю.* Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации. http://www.crime-research.org/library/Golovin.htm

СОЗДАНИЕ МОДЕЛИ БЕЗОПАСНОСТИ ИЕРАРХИЧЕСКИХ РАСПРЕДЕЛЕННЫХ СИСТЕМ

К.Н. Филькин, аспирант; И.В. Давыдов, аспирант
ТУСУР, каф. КИБЭВС, г. Томск, fkn@kibevs.tusur.ru

Описание событий информационной безопасности и создание методологии противодействия преступлениям в сфере информационных технологий сопряжено с необходимостью создания модели информационной безопасности.

Исследуются распределенные иерархические системы. Выбор данного класса систем связан с тем, что большинство организаций имеют именно иерархическую структуру с распределенными ресурсами. Многоуровневую иерархическую структуру можно определить путем указания нескольких существенных характеристик, присущих всем иерархическим системам. К ним относятся: последовательное вертикальное расположение подсистем, составляющих данную систему (вертикальная декомпозиция); приоритет действий или право вмешательства подсистем верхнего уровня; зависимость действий подсистем верхнего уровня от фактического исполнения нижними уровнями своих функций.

Разрабатываемая модель безопасности распределенных иерархических систем состоит из модели злоумышленника, модели распределенной системы, модели атаки и модели защиты (рис. 1).

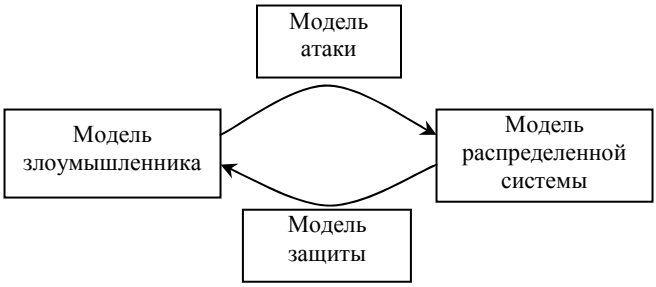


Рис. 1. Компоненты моделирования

Модель распределенной иерархической системы представлена комплексом описаний страт, эшелонов и слоев. Стратификация связана с тремя свойствами иерархических систем: вертикальной декомпозицией, приоритетом действий и взаимосвязью характеристик качества функционирования систем.

Страты определяют цели моделирования (рис. 2). При изучении вопросов информационной безопасности можно выделить две страты иерархической распределенной системы, функционирование которых наи-

более важно. Первая представляет собой компьютерную сеть, а вторая – организационную структуру. Как правило, различные разработки обеспечения защиты информации касаются либо той, либо иной системы: либо вопросы организационно-правовых аспектов, либо практические вопросы защиты вычислительных комплексов от нарушения целостности, доступности и конфиденциальности. Для второй страты многоэшелонная система состоит из пяти эшелонов (сотрудники, отделы, отделения, регионы, центр). Иерархия слоев представляет собой совокупность вертикально расположенных решающих подсистем; функциональная иерархия состоит из трех слоев (выбора, обучения и самоорганизации).

В качестве модели злоумышленника рассматривается модель, описывающая состояние самого злоумышленника. В первую очередь модель рассматривается как «черный ящик». Данное представление является качественным. Она не дает количественного значения протекающим процессам, но проста и прозрачна для понимания. Злоумышленник описывается как субъект, атакуемая система является объектом. По сути, данная модель описывает процесс преобразования мотивации субъекта и свойств объекта в совершаемые действия, т.е. уже проведение атаки. Затем производится декомпозиция «черного ящика».

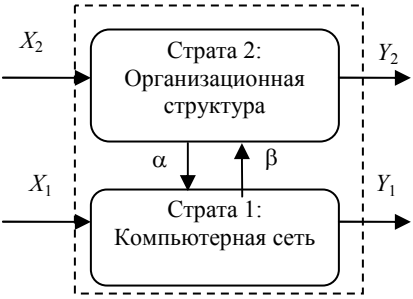


Рис. 2. Стратифицированное представление иерархических систем

После этого модель злоумышленника представляется аналогичной модели распределенной системы, тем самым подчеркивается воздействие (возможность воздействия) нарушителя на каждый элемент системы.

Модель атаки описывается стохастическими грамматиками. Предполагается, что нападение состоит из отдельных атак (Attacks), которые в свою очередь основаны на некотором сценарии, состоящем из последовательности шагов (steps). Сама атака направлена на прекращение или снижение работоспособности системы, что определяется некоторой вероятностью.

Разрабатываемая модель защиты имеет цель максимально снизить значение данной вероятности успешного проведения атаки злоумышленником.

ЛИТЕРАТУРА

1. *Месарович М., Мако Д., Такахара Я.* Теория иерархических многоуровневых систем. Пер. с англ. под ред. И.Ф. Шахнова. М.: Издательство «Мир»,1973. 344 с.
2. *Месарович М., Такахара Я.* Общая теория систем: математические основы. Пер. с англ. Э.Л. Наппельбаума. М.: Издательство «Мир»,1978. 312 с.

ФОРМИРОВАНИЕ УПРАВЛЯЮЩЕГО АВТОМАТА АКТИВНОЙ ЗАЩИТЫ КОМПЬЮТЕРА

А.В. Грасмик, студент 3 курса каф. КИБЭВС;
Е.А. Мошников, студент 3 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 66-39-38, q666Alexus666@mail2000.ru

Постановка задачи

В настоящее время существует немало средств защиты компьютеров от информационных угроз (брандмауэры, антивирусы и др. средства защиты), однако практически все они обеспечивают лишь пассивную защиту и часто не обеспечивают комплексную защиту, т.е. сплоченность данных программных продуктов в единое целое. Данные программы действуют только для обнаружения и ликвидации последствий угроз и имеют достаточно жесткую архитектуру, что не позволяет действовать против неизвестных факторов. В вопросах создания «интеллектуальной» защиты уже были сделаны шаги, попытки перенести иммунологические процессы природы (как совершенного поведения защиты и выживания) на математический аппарат и кибернетику, однако пока данные работы несут лишь теоретический характер, а хотелось бы получить рабочую систему защиты. Поэтому цель нашей работы сформировать управляющий центр безопасности в компьютере, т.е. построить автомат управления другими автоматами, такими как:

– следящий;
– проверяющий;
– запоминающий;
– «киллер» (ликвидирующий);
– самодиагностический.

Решение

Возможно, нам не удастся сформировать полностью работающий центр безопасности в связи с недостачей других автоматов, зато попытаемся сформировать алгоритм его работы, те основы построения, которые впоследствии позволят довершить данную работу.

Под алгоритмом работы управляющего автомата мы понимаем методы связи и управления другими автоматами и самое главное – это способ выбора необходимого противодействия угрозам, наиболее действенного, а так же возможность уменьшения времени восприятия степени угроз, и последующей реакции.

Для этого мы используем методы итеративного научения и искусственного интеллекта в кибернетике, сформированные десятки лет назад. Основой для выбора действий системы против конкретной угрозы будет присвоение своеобразного рейтинга для каждого возможного ответного действия (или задание вероятностей выбора). Действие с максимальным рейтингом (вероятностью) будет активировано управляющим автоматом. Если же совершенное действие не привело к положительным результатам, то рейтинг (вероятность) данного действия уменьшается на определенный коэффициент, соответственно – увеличивается у остальных действий. Иначе, если действие устранило угрозу, то происходит обратный процесс, увеличения рейтинга для данного действия и уменьшения у других. Однако когда появляется новая угроза и она обнаружена, то всем возможным действиям присваиваются равные рейтинги, и выбор произойдет произвольно, возможно, неудачно, но в процессе проб и ошибок четко сформируются рейтинги. Задание таких рейтингов должно сократить время на выбор действий, а также уменьшить необходимость пользователя в элементарных ситуациях. Формулы выбора могут быть линейными, экспоненциальными или более сложными (последние два способа задания формул являются приближениями к основе искусственного интеллекта)

Подобные алгоритмы могут широко применятся при появлении различных угроз:

– защита от вирусов, троянских программ, программных закладок и т.п.;

– контроль непроверенных приложений;

– контроль TCP/IP обмена, а так же контроль ненадежных узлов, серверов и т.п.

– контроль доступа и разрешенных действий в локальной сети.

Данный автомат должен быть, насколько это возможно, автономным, т.е. работать самостоятельно в соответствии с указаниями пользователя, но не быть впоследствии неуправляемым, да это и невозможно, ведь для ряда неизвестных (новых) проблем необходимо решение пользователя. Так же автомат должен анализировать эффективность своих действий (насколько это возможно).

В общем, управляющий автомат должен объединить уже имеющиеся средства для достижения единой цели – безопасности.

ЦИФРОВЫЕ ИММУННЫЕ СИСТЕМЫ КАК ОДНО ИЗ НАПРАВЛЕНИЙ РАЗВИТИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Старицын, студент 3 курса; А.И. Кривенчук, студент 3 курса; М.С. Ковалевский, студент 3 курса
ТУСУР, каф. КИБЭВС, г. Томск

Как известно, иммунитет – особое свойство многоклеточных организмов, в норме предназначенное для защиты от инфекций и иных внешних неблагоприятных воздействий. Рассмотрим некоторые виды угроз, от которых защищается многоклеточный организм в целях сохранения своей жизни: от проникновения во внутреннюю среду травмирующих собственные клетки субстанции из внешней среды, от внешних веществ, уже проникших во внутреннюю среду, от собственных поврежденных клеток или выполняющих свою биологическую программу клеток.

Рассмотрим некоторые функций иммунитета – распознавание агента(клетка, которая влияет на организм негативным образом), производить регенерацию поврежденных тканей и выведение продуктов распада антигена, на действие агента формирует иммунный ответ. Если рассмотреть вычислительную систему(ВС), то она тоже подвержена угрозам, аналогично тем, что указывались выше. Эти угрозы для ВС имеют свою специфику(вирус, несанкционированный доступ, закладки, сбои программ и т.д.).

Организм защищается от злокачественных воздействий с помощью иммунитета. Основываясь на защитных свойствах иммунитета биологического, можно попытаться разработать иммунитет искусственный, направленный на защиту ВС, а именно разработать цифровую иммунную систему(ЦИС).

Предполагается, что ЦИС будет внедрена в ВС и все взаимодействия с самой системой будут проходить через ЦМС. Если произошло, какое – либо воздействие, то ЦМС распознает это воздействие и если это воздействие нежелательно для данного процесса, то ЦМС его нейтрализует или уничтожает. Цифровая иммунная система в ВС будет нести функцию защиты от внешнего воздействия, которое может привести к нежелательной работе ВС.

Таким образом, разработка цифровой иммунной системы может быть перспективной областью развития средств информационной защиты ВС.

ПРОЕКТ ПО СОЗДАНИЮ ПРИЛОЖЕНИЯ ДЛЯ ИДЕНТИФИКАЦИИ АВТОРА НЕИЗВЕСТНОГО ТЕКСТА С ПОМОЩЬЮ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

С.Л. Крыловский, студент 3 курса; М.Г. Власова, студент 3 курса; М.С. Ковалевский, студент 3 курса КИБЭВС

ТУСУР, г. Томск, т. 8-903-951-1825,8-913-851-3569

Сеть нейронов, образующая человеческий мозг, представляет собой высокоэффективную комплексную, параллельную систему обработки информации. Она способна организовать свои нейроны таким образом, чтобы реализовать восприятие образа, его распознание во много раз быстрее, чем эти задачи будут решены самыми современными компьютерами. Так распознание знакомого лица происходит в мозге человека за 100–120 мс, в то время как компьютеру для этого необходимы минуты и даже часы.

Обычно НС оперирует цифровыми, а не символьными величинами. Большинство моделей НС требуют обучения. В общем случае, *обучение* – такой выбор параметров сети, при котором сеть лучше всего справляется с поставленной проблемой. Обучение – это задача многомерной оптимизации, и для ее решения существует множество алгоритмов.

Искусственные нейронные сети – набор математических и алгоритмических методов для решения широкого круга задач. Выделим характерные черты искусственных нейросетей как универсального инструмента для решения задач:

1. НС дают возможность лучше понять организацию нервной системы человека и животных на средних уровнях: память, обработка сенсорной информации, моторика.

2. НС – средство обработки информации:

а) гибкая модель для нелинейной аппроксимации многомерных функций;

б) средство прогнозирования во времени для процессов, зависящих от многих переменных;

в) классификатор по многим признакам, дающий разбиение входного пространства на области;

г) средство распознавания образов;

д) инструмент для поиска по ассоциациям;

г) модель для поиска закономерностей в массивах данных.

3. НС свободны от ограничений обычных компьютеров благодаря параллельной обработке и сильной связанности нейронов.

Задача состояла в создании универсального приложения для распознавания автора неизвестного текста с помощью ИНС и ее обучения. Приложение должно быть эффективным, надежным, наглядным и простым в использовании. Оно может применяться в области достоверности информации: подтверждение авторства, цифровой подписи и т.д.

Для решения поставленной задачи использовался программный продукт Delphi 7[1]. Основной процесс работы приложения показан на рис. 1

Рис. 1. Процесс работы в приложении

При запуске приложения перед пользователем появляется форма с блоком «Введите текст». Установив параметры распознавания и заполнив поле «Текст распознавания» необходимо нажать на кнопку «Распознать». После нажатия на кнопку если текст будет не распознан, то появится сообщение «Текст не распознан. Попробуйте изменить параметры распознавания или обучите сеть». Если выбрать «Обучение сети», то произойдет дополнение словарей или БД-параметров, а также модификация БД-авторов. В поле «комментарии» с каждым шагом будет появляться результаты обучения. После этого в поле «Вывод»

отобразится результат обучения: какие авторы добавлены, и какие параметры модифицированы. Результат можно вывести на печать, в файл или по сети. На этапе распознавания, производимые с неизвестным текстом расчеты также можно проследить. Выход из программы осуществляется выбором в меню «Файл» | «Выход». Информацию о программе можно получить в меню «Помощь» | «О программе». Справку можно получить выбором в меню «Помощь».

Выводы. В процессе данной работы было спроектировано приложение, реализующее выполнение необходимых операций обучения и распознавания с помощью НС, при этом пользователь может не только наблюдать результаты этих операций, но и вмешиваться в сам процесс: проверять правильность и контролировать процесс на каждом шаге его выполнения.

ЛИТЕРАТУРА

1. Архангельский А.Я. Программирование в DELPHI 7. М.: Издательство «БИНОМ», 2005. 1151 с.

ОПТИМИЗАЦИЯ АСИММЕТРИЧНОГО АЛГОРИТМА ШИФРОВАНИЯ ДАННЫХ RSA НА ОСНОВЕ ВОЗМОЖНОСТЕЙ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ

М.М. Медведева, студентка 5 курса ФВС;
Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС
ТУСУР, г. Томск, e-mail: poohy@ngs.ru

Целью работы является оптимизация криптоалгоритма RSA на основе возможностей современных технологий.

В настоящее время без использования криптографии немыслимо решение задач по обеспечению безопасности информации, связанных с конфиденциальностью и целостностью, аутентификацией и невозможностью отказа от авторства. Обладание достоверной и качественной информацией позволяет добиться больших преимуществ во многих сферах человеческой деятельности. В связи с этим приобретает большое значение сокрытие информации, подтверждение ее достоверности и другие меры по ее защите с целью недопущения доступа к жизненно важной информации со стороны злоумышленников.

В криптографии известны два основных типа алгоритмов, основанных на использовании ключей: симметричные алгоритмы и ассиметричные алгоритмы (алгоритмы с открытым ключом). Надежность этих алгоритмов полностью зависит от ключа (или ключей), а не от

самих алгоритмов. Это означает, что алгоритм может быть опубликован и проанализирован. Программные продукты, использующие этот алгоритм, могут широко распространяться. Причем знание самого алгоритма злоумышленником не имеет значения – если он не знает конкретный ключ, он не сумеет прочесть сообщения.

На данный момент существует множество различных систем криптографической защиты информации. Одним из наиболее ярких представителей достаточно большого семейства алгоритмов с открытым ключом является алгоритм криптографической защиты данных RSA.

Безопасность алгоритма RSA основана на трудоемкости разложения на множители (факторизации) больших чисел. Открытый и закрытый ключи являются функциями двух больших простых чисел, разрядностью более 100–200 десятичных цифр. Предполагается, что восстановление открытого текста по шифртексту и открытому ключу равносильно разложению числа на два больших простых числа. Именно работа с большими числами приводит к существенному недостатку асимметричных алгоритмов – невысокой скорости работы. Большое число сложных математических вычислений при шифровании и дешифровании информации приводит к тому, что при программной реализации симметричный алгоритм DES работает примерно в 100 раз быстрее RSA.

Однако сегодня возможности современных технологий позволяют оптимизировать алгоритм RSA и тем самым увеличить скорость его работы, таким образом попытаться устранить основной недостаток работы криптоалгоритма. Для оптимизации RSA используются такие технологии, как MMX, SSE, SSE2 и 3DNow!.

Сущность SSE (Streaming SIMD Extensions, раньше MMX2) состоит в появлении в процессорах Pentium семидесяти новых SIMD-инструкций, оперирующих со специальными 128-битными регистрами XMM0-XMM7. Каждый из этих регистров хранит четыре вещественных числа одинарной точности. Таким образом, выполняя операцию над двумя регистрами, SSE фактически оперирует четырьмя парами чисел. То есть благодаря этому процессор может выполнять до 4-х операций одновременно. Вследствие чего, программно реализованный алгоритм RSA получает двукратный прирост производительности, тем самым уменьшается в несколько раз реальное время шифрования и дешифрования данных.

Команды MMX используют регистры сопроцессора, но представляют собой команды целочисленного типа. Их 64-разрядные операнды

могут содержать восемь упакованных байтов, или четыре упакованных 16-разрядных слова, или два упакованных 32-разрядных двойных слова, или же одиночное 64-разрядное слово учетверенной длины. То есть различные по длине данные мультимедиа упаковываются в одно 64-разрядное слово, и над ним производится некое общее действие.

Эта методика называется одиночной командой с множественными данными (SIMD), и ориентирована на алгоритмы и типы данных, которые характерны для программного обеспечения мультимедиа. Примеры включают MPEG-декомпрессию, оценку и компенсацию движения (учет изменения изображения в кадре), преобразование цветового пространства, наложение текстуры, двумерную фильтрацию, умножение матриц, быстрое преобразование Фурье, дискретное косинус-преобразование и т.д. В сущности, то, что объединяет эти процессы – потенциальный параллелизм вычислений. Поэтому MMX – команды разработаны прежде всего для того, чтобы максимально эксплуатировать такой параллелизм, который приводит к повышению производительности программного продукта.

Инструкции технологии 3DNow! предназначены для ускорения обработки 3D в приложениях. Процессор может выполнять по две инструкции технологии 3DNow! за такт. Так как каждая инструкция технологии 3DNow! работает с упакованными данными (два 32-битных элемента 64-битных данных), то за такт вычисляются четыре операции с плавающей запятой. Все инструкции технологии 3DNow! работают с теми же регистрами, что и инструкции технологии MMX.

В итоге можно сказать о том, что RSA используется буквально везде: в Интернете, локальных сетях, специальных системах обмена данными, кредитных картах и т. п. Кроме того, этот алгоритм был использован при разработке других технологий, например, таких, как электронная цифровая подпись (ЭЦП), а также оказался «узаконенным» в нескольких десятках как международных, так и национальных стандартах разных стран. Поэтому весьма актуальным на сегодняшний день является увеличение производительности программного продукта на основе возможностей современных микропроцессоров, что позволит уменьшить реальное время шифрования и дешифрование в RSA.

ЛИТЕРАТУРА

1. http://developer.intel.ru/design/Pentium4/prodbref/
http://security.compulenta.ru/crypto/

РАЗРАБОТКА ЛАБОРАТОРНОГО ПРАКТИКУМА ПО ДИСЦИПЛИНЕ «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

М.М. Нурмахмадов, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 8-923-403-0831, e-mail mnm903@mail.ru

Безопасность информации – это способность системы ее обработки обеспечить в заданный промежуток времени возможность выполнения заданных требований по величине вероятности наступления событий, выражающихся в утечке, модификации или утрате данных, представляющих ту или иную ценность для их владельца. При этом считается, что причиной этих событий могут быть случайные воздействия либо воздействия в результате преднамеренного НСД человека-нарушителя.

Особенностью информационной безопасности автоматизированных систем (АС) является ее практическая направленность. Большинство положений сначала реализовывалось в виде конкретных схем и рекомендаций, а уж затем обобщалось и фиксировалось в виде теоретических положений или методических рекомендаций. Другой особенностью информационной безопасности АС была на первых этапах развития значительная зависимость теоретических разработок от конкретных способов реализации АС, определявшихся проектными программными или аппаратными решениями.

Если вы используете персональный компьютер, например, все ваши меры обеспечения безопасности, могут заключаться лишь в том, чтобы не забывать закрыть на замок комнату, в которой установлен ваш компьютер. Но даже если вы являетесь единственным санкционированным пользователем, то система может функционировать в совместно используемой среде (например, на компьютере, работающем в составе компьютерной сети).

Данная работа посвящена разработке лабораторного практикума для практической реализации студентами теоретических основ компьютерной безопасности, так как именно информация (лекции, статьи и.т.д.) по основам компьютерной безопасности, которую можно встретить везде, в том числе в интернете, доступна для большинства людей. В работе изложены практические основы компьютерной безопасности(анализ угроз безопасности, разработка политики безопасности и ее последующее сопровождение), в том числе предложены несколько лабораторных работ по этому курсу.

Основной целью выполнения лабораторного практикума является ознакомление студентов на кафедре КИБЭВС с теоретическими вопросами в области компьютерной безопасности, усвоения их и применения полученных знаний на практике, а также закрепление и углуб-

ление полученных студентами знаний по вопросам компьютерной безопасности.

В итоге работы определены требования к структуре, выполнению и написанию лабораторных работ, а также приведены несколько лабораторных работ. Сформулирован примерный перечень лабораторных работ, возможно семинарских занятий по дисциплине «Теоретические основы компьютерной безопасности».

Примерный перечень тем лабораторных работ:

1. Парольная защита;
2. Субъектно-объектная модель;
3. Модуль проверки описания;
4. Модель распространения прав доступа Take-Grant;
5. Мандатные политики безопасности;
6. Домены безопасности;
7. Стандарты в области защиты информации в автоматизированных системах.

ЛИТЕРАТУРА

1. *Девянин П.Н., Михальский О.О.* Теоретические основы компьютерной безопасности, Радио и связь, 2000.
2. *Сычев Ю.Н.* Информационная безопасность. Учебное пособие. 2004.
3. Г*рушо А.А, Тимонина Е.Е.* Теоретические основы защиты информации. М.: Издательство Агентства «Яхтсмен». 1996. 192 с.
4. http://random.wahack.org.ru – политика компьютерной безопасности.

АНАЛИЗ АСПЕКТОВ БЕЗОПАСНОСТИ СЕТЕВЫХ СЕРВЕРОВ СУБД

С.А. Пахандрин, И.М. Шагманов, В.В. Алехин,
студенты 3 курса каф. КИБЭВС
ТУСУР, г. Томск, xxmop@mail.ru

В настоящее время рынок программного обеспечения имеет высокую динамику роста. Следовательно, множество программных решений во многом схожи, но при этом, специализируются в рамках своей предметной области. В связи с этим, перед пользователем возникает дилемма выбора программного продукта для решения поставленной задачи или целого комплекса задач.

В данной статье был проведен анализ реализации безопасности в различных СУБД. Среди наиболее ярких представителей систем управления баз данных можно отметить: Microsoft Access, Borland dBase, Borland Paradox, Microsoft Visual FoxPro, а также баз данных

Microsoft SQL Server, Oracle, InterBase Server, MySQL Server, используемые в приложениях, построенных по технологии «клиент-сервер». В данной работе будут рассмотрены только сетевые СУБД.

MS SQL Server

Одно из преимуществ MS SQL Server, в том что он использует в своей работе сервисы безопасности Windows NT. Это предусматривает использование механизмов аутентификации Windows NT для обеспечения безопасности всех пользовательских соединений. Стандартный режим безопасности предполагает, что на MS SQL Server будут заводится самостоятельные login и соответствующие им пароли.

В режиме аутентификации Windows NT используется система безопасности Windows NT и ее механизм учетных записей. Этот режим позволяет SQL Server использовать имя пользователя и пароль, которые определены в Windows, и тем самым обходить процесс подключения к SQL Server. Таким образом, пользователи, имеющие действующую учетную запись Windows, могут подключиться к SQL Server, не сообщая своего имени и пароля. Когда пользователь обращается к СУБД, последняя получает информацию об имени пользователя и пароле из атрибутов системы сетевой безопасности пользователей Windows.

В смешанном режиме аутентификации задействованы обе системы аутентификации: Windows и SQL Server. При использовании системы аутентификации SQL Server, отдельный пользователь, подключающийся к SQL Server, должен сообщить имя пользователя и пароль, которые будут сравниваться с хранимыми в системной таблице сервера. При использовании системы аутентификации Windows пользователи могут подключиться к SQL Server, не сообщая имя и пароль.

В MS SQL Server обеспечивает многоуровневую проверку привилегий при загрузке на сервер. Сначала идентифицируются права пользователя на установление соединения с выбранным сервером (login name и пароль) и выполнение административных функций: создание устройств и баз данных, назначение прав другим пользователям, изменение параметров настройки сервера и т.д. Максимальными правами обладает системный администратор.

InterBase Server

InterBase предоставляет развитые средства для управления безопасностью в своих базах данных. Существенные отличия от других СУБД то, что данные о пользователях хранятся не в самой базе данных, а в не ее – в особой базе данных пользователей lSC4.gdb. Дело в том, что реализация ограничений, налагаемых на объекты базы данных, осуществлена в InterBase на уровне сервера базы данных, а не

самой базы данных. Это означает, что внутри базы данных данные никак не шифруются и не защищаются.

Следствием вынесения информации о пользователях и проверки прав доступа к базе данных на уровень сервера является то, что, физически скопировав базу данных на другой сервер, мы можем воспользоваться паролем администратора этого сервера и получить полный доступ к информации в базе данных, обойдя, таким образом, все ограничения на доступ к данным. Это является на наш взгляд большим минусом.

В InterBase хорошо развита система пользователей и ролей. Как уже было отмечено, данные о пользователях хранятся в файле lSC4.gdb. Каждому пользователю назначаются права, в тоже время он может являться участником определенной роли. Т.е. все ограничения, которые наложены на определенную роль, будут применимы и к пользователю данной роли.

MySQL Server

Программа MySQL выполняется в виде системного сервиса или демона, поэтому необходимо учитывать средства безопасности, предоставляемые операционной системой или сетевым программным обеспечением.

Пользователи идентифицируют себя по имени, паролю и адресу узла. Пользовательские имена и пароли MySQL не связаны напрямую с именами и паролями операционной системы. Просто большинство клиентов MySQL по умолчанию берет имя пользователя, которое было указано при регистрации в системе. Это довольно удобно, хотя и не является обязательным правилом.

Пользовательские имена и пароли могут быть длиной до 16 символов. Пароль разрешается оставлять пустым. Это самый низкий уровень безопасности. Он допустим только в том когда доступ ограничивается по каким-то другим критериям, например адресу узла. Перечень привилегий хранится в базе данных mysql. При установке сервера создается 5 системных таблиц: column_priv (привилегии отдельных столбцов), db (привилегии всей базы данных), host (привилегии всех пользователей того или иного узла), tables_priv (привилегии отдельных таблиц), user (глобальные привилегии). В таблице user описываются глобальные права доступа и хранятся пользовательские пароли.

При попытке подключения к серверу программа MySQL обращается к таблице user и проверяет, имеет ли пользователь право на подключение. Имя, пароль и адрес узла пользователя должны соответствовать как минимум одной записи таблицы. Если этого не происходит, программа отказывает пользователю в запросе. Но даже когда подключение легитимно, пользователю может быть разрешено выполнять

лишь ограниченный набор SQL инструкций. Права доступа к данным контролируются остальными четырьмя таблицами базы mysql.

В данной статье мы привели основные особенности каждого сервера СУБД, показали, как организуется раздача прав доступа к БД.

ЛИТЕРАТУРА

1. *Аткинсон Л.* MySQL. Библиотека профессионала. М.: Издательский дом «Вильяме», 2002. 624 с.
2. *Скляр А.А.* Введение в InterBase. М.: Горячая линия–Телеком, 2002. 517 с.
3. http://citforum.ru

ОБЪЕКТНО-ОРИЕНТИРОВАННАЕ СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ И ЗАЩИТА БАЗ ДАННЫХ

А.В. Старицын, студент 3 курса; А.С. Рюхова, студент 5 курса
ТУСУР, каф. КИБЭВС, г. Томск

Объектно-ориентированные системы управления базами данных являются третьим поколением в области представления и управления данными. ООСУБД в настоящее время доказывают свою значимость перед реляционными СУБД (второе поколение), которые хорошо показали себя в области деловых приложениях.

ООСУБД раскрывают свои возможности перед «большими» приложениями, таких как:

- Автоматизация проектирования;
- Автоматизация производства;
- Автоматизация разработки программного обеспечения;
- Офисные информационные системы и мультимедийные системы;
- Цифровое издательство;
- Геоинформационные системы;
- Интерактивные и динамические Web-узлы.

В ходе следования реляционных систем управления баз данных были найдены недостатки, например, такие как однородность структуры данных, ограниченный набор данных и некоторые другие.

Объектно-ориентированный подход является одним из новых решений к созданию программного обеспечения, который считается перспективным для решения некоторых классических проблем разработки ПО. Базовым понятием объектно-ориентированной технологии является то, что все программное обеспечение должно всегда, когда это возможно, создаваться на основе стандартных и повторно используемых компонентов. Традиционно создание программного обеспече-

ния и управление базами данных представляли собой совершенно разные дисциплины. Технология создания баз данных была сконцентрирована в основном на статических концепциях хранения информации, тогда как технология создания программного обеспечения моделировала динамические аспекты программного обеспечения. С появлением третьего поколения систем управления базами данных эти две дисциплины слились воедино, что позволяет параллельно моделировать данные процессы обработки данных.

Объектно-ориентированное направление дает возможность:

▪ Определение системы на основе объектов упрощает создание программных компонентов, которые очень достоверно эмулируют область их применения, облегчая таким образом понимание особенностей системы и ее проектирование.

▪ Благодаря инкапсуляции и сокрытию информации использование объектов и сообщений способствует модульному программированию, поскольку реализация одного объекта зависит не от внутренних способностей других объектов, а только от их реакции на те или иные сообщения. Более того, условием модульности накладывается принудительно, поэтому позволяет создавать более надежное программное обеспечение.

▪ Использование классов и механизма наследования способствует разработке повторно используемых и расширяемых компонентов при создании новых или модернизации существующих систем.

Так как ООСУДБ является новой областью взаимодействия с данными, то она подвержена угрозам (утрата целостности, потеря доступности, похищение и фальсификация данных и др.). Данные являются ценным ресурсом, доступ которому необходимо строго контролировать и регламентировать. Защита баз данных должна охватывать используемое оборудование, программное обеспечение, персонал и собственно данные.

ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

А.А. Шелупанов, зав. каф. КИБЭВС, д.т.н., профессор;
А.В. Шокарев, аспирант каф. КИБЭВС
ТУСУР, г. Томск, т. 41-46-38, saa@keva.tusur.ru,
stranger@adm.yrg.kuzbass.net

Интерес к стеганографии, в переводе означающей тайнопись, появился с давних времен. С развитием компьютерных технологий появи-

лось новое направление – компьютерная стеганография, в задачи которой входит сокрытие информации в различных файлах, таким образом, чтобы сам факт сокрытия оставался не замеченным.

К данному моменту компьютерная стеганография включает в себя несколько областей исследования:

1. Встраивание информации с целью ее скрытой передачи;
2. Встраивание цифровых водяных знаков (ЦВЗ), в частности для защиты авторских прав на электронную продукцию, такую как видео, аудио и графические файлы в электронном виде (Watermarking);
3. Встраивание заголовков (captioning);
4. Встраивание идентификационных номеров (fingerprinting).

Наибольший интерес вызывают ЦВЗ. Они применяются как для маркирования электронных файлов, так и для встраивания и передачи различной информации по каналам связи. ЦВЗ также могут быть трех видов:

1. Хрупкие – разрушаются при незначительной модификации контейнера;

2. Полухрупкие – могут быть устойчивыми к определенным воздействиям на контейнер, и быть не устойчивыми к другим;

3. Робастные – устойчивы к различного рода воздействиям;

В связи с этим можно выделить актуальную теоретическую и практическую задачу по применению ЦВЗ, которая состоит в аутентификации пользователя при условии устойчивости к комплексному навязыванию ложных сообщений нарушителем и воздействию случайных и преднамеренных ошибок в каналах связи. В ходе поиска решения данной задачи возможно использование методов контроля подлинности на основе ЦВЗ и применении как одного так и нескольких видов цифровых водяных знаков.

Обобщенная модель системы представлена на рис. 1:

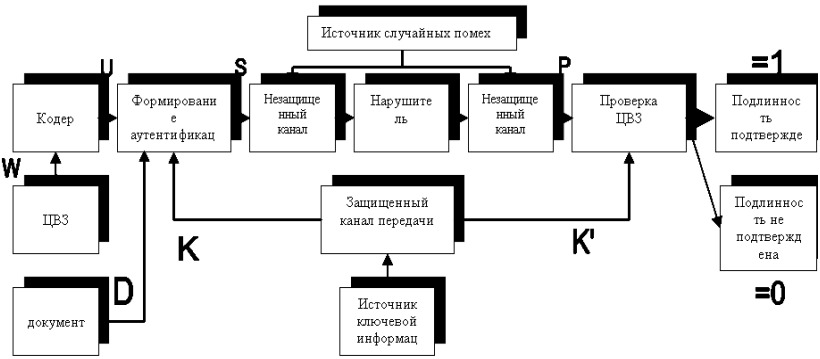


Рис. 1. Обобщенная модель аутентификации пользователя на основе ЦВЗ

Отправитель создает документ D, накладывает цифровой водяной знак *W*, индивидуальный для каждого отправителя, который преобразовывается в кодере к удобному виду для встраивания в заверяемое сообщение. Алгоритм формирования такой конструкции водяного знака *U* представим в виде

$$U = F(D, W) \tag{1}$$

Затем в формирователе заверенных сообщений конструкция водяного знака встраивается в документ, используя конфиденциальный ключ *K*:

$$X = \Psi(U, D, K) \tag{2}$$

В канале связи на заверенное сообщение *X* воздействуют нарушитель, а также случайные и преднамеренные помехи. В результате этого воздействия на приеме в устройство проверки водяных знаков поступает модифицированное сообщение *Y*. По алгоритму обнаружения водяного знака формируется оценка водяного знака вида:

$$W' = G(Y, W, K') \tag{3}$$

Подлинность документа определяется в соответствии с этой оценкой. Возможны решения вида $W' = 1$ (подлинность сообщения подтверждена) или $W' = 0$ (подлинность сообщения не подтверждена). Также возможны и другие решения вида $0{,}5 \le Wj' \le 1$ (*j*-й фрагмент скорее всего подлинный) или $0 \le Wj' < 0{,}5$ (*j*-й фрагмент скорее всего навязан или искажен помехами передачи). При формировании оценки водяных знаков могут возникнуть ошибки их обнаружения получателем сообщения.

Данная схема имеет следующий вид.

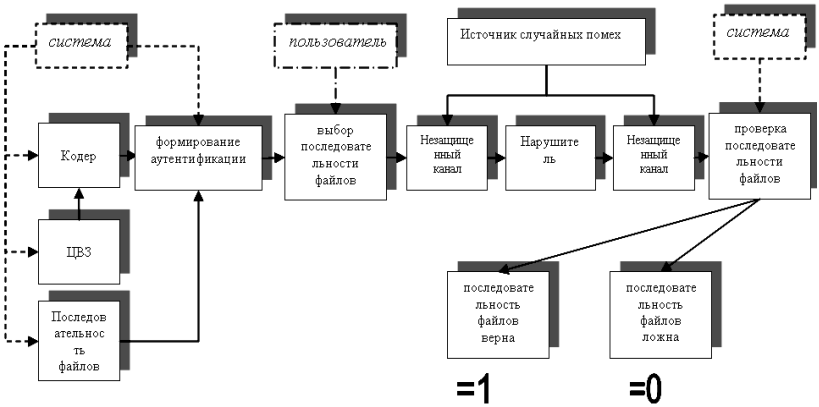


Рис. 2. Модель аутентификации пользователя на основе ЦВЗ для доступа к защищенным ресурсам

На основе представленной схемы можно получить отличную модель аутентификации пользователя. Идея, которой состоит во встраивании в несколько графических файлов данных о пользователе (имя и пароль) для доступа к определенным ресурсам, что позволяет избежать привычного ввода имени пользователя и пароля.

В данной схеме под ЦВЗ понимается встраивание определенной информации о пользователе и его пароле к определенному ресурсу. Далее информация кодируется и встраивается в последовательность графических файлов. Пользователь выбирает определенную последовательность файлов и подтверждает свой выбор. Система из этой последовательности извлекает ЦВЗ, в которых содержаться имя пользователя и пароль, если последовательность верна то пользователю открывается ресурс, в обратном случае доступ к защищенному ресурсу будет закрыт, до тех пор, пока последовательность будет правильной.

В данной модели можно ввести ограничение на количественный выбор последовательности, то есть если, к примеру, последовательность была выбрана не правильно несколько раз то доступ пользователя блокируется автоматически. Так же можно использовать различные способы встраивания водяных знаков, либо различные типы (хрупкие, полухрупкие, робастные) для каждого файла из последовательности, причем методы для встраивания могут выбираться в произвольной последовательности.

По сравнению с криптографическими системами аутентификации, система аутентификации пользователей на основе ЦВЗ имеет следующие особенности:

–заверяемое сообщение и встроенный в него ЦВЗ взаимозависимы, то есть при разрушении первого разрушается и второй, а если водяной знак сохранил свою целостность, то и принятое сообщение ее не потеряло;

–при приеме искаженного фрагмента сообщения получатель может, не отказываясь от всего сообщения в целом, отказаться лишь от данного фрагмента.

В отличие от сравнительных методами, методы контроля подлинности на основе водяных знаков обладают существенными достоинствами:

–высокой устойчивостью к удалению аутентификатора заверенного сообщения без разрушения самого сообщения;

–обнаружением несанкционированного копирования заверенных сообщений;

–согласованность с источниками сообщений, обладающими существенными статистическими зависимостью и памятью, такими как изображение и звуковой сигнал.

Цифровые водяные знаки еще полностью не исследованы и в недалеком будущем будут найдены и другие области применения, касающиеся защиты информации и систем доступа к такой информации.

ЛИТЕРАТУРА

1. *Petitcolas F.A., AndersonR.J., KuhnM.G.* Information hiding – a survey // Proceeding of the IEEE. Vol. 87. № 7. 1999. pp. 1062–1078.
2. *Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В.* Основы компьютерной стеганографии. М.: Радио и связь, 2003.
3. *ГОСТ РФ 28147-89.* Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Госстандарт СССР.
4. *ГОСТ РФ 34.10-94.* Информационная технология. Криптографическая защита информации. Электронная цифровая подпись. М.: Госстандарт РФ.
5. *Оков И.Н.* Криптографические системы защиты информации. СПб.: Типография ВУС, 2001. 236 с.
6. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. М.: Солон-Пресс, 2002.

НЕЙРОННЫЕ СЕТИ КЛЕТОЧНЫХ АВТОМАТОВ КАК ОДИН ИЗ ПОДХОДОВ К ПОСТРОЕНИЮ ЦИФРОВОЙ ИММУННОЙ СИСТЕМЫ

А.В. Старицын, студент 3 курса; И.М. Шагманов, студент 3 курса
ТУСУР, каф. КИБЭВС, г. Томск.

Клеточные автоматы и нейронные сети являются развивающимися областями науки. Для нас важно, что нейронные сети могут научаться, а клеточные автоматы могут автоматически генерировать процессы, необходимые для функционирования динамических систем. Объединение этих двух направлений дает круг возможностей для создания динамической системы накопления, распознавания и генерации процессов. Если задействовать клеточные автоматы и нейронные сети, то можно построить цифровую иммунную систему, которая будет иметь свое самоуправление, накопление информации, самообучение и самозащиту.

Рассмотрим математическую модель цифровой иммунной системы. Пусть $A=(A^{(1)},A^{(2)},A_i^{(3)})\ \ i=1,2,...,n$ – иерархическая нейронная сеть клеточных автоматов, где $A^{(1)}$ – командный элемент, $A^{(2)}$ – координатор, $A_i^{(3)}$ – автоматы-исполнители. Графическая модель цифровой иммунной системы показана на рис. 1.

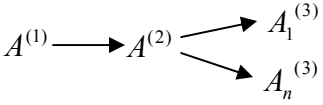


Рис. 1. Графическая модель цифровой иммунной системы

В общем случае автомат $A^{(1)}$ должен достигать набор целей, в простейшем случае – распознавания информационных объектов. Координатор $A^{(2)}$ распределяет конкретные задачи, необходимые для выполнения цели(декомпозицию цели на совокупность конкретных задач делает командный элемент и передает эту декомпозицию координатору). Кроме того, автомат $A^{(2)}$ перераспределяет задания автоматам-исполнителям по мере выполнения или своих заданий.

Рассматриваются автоматы-исполнители двух типов:

а) В-автоматы – критерий максимального вознаграждения;

б)М-автоматы – критерий минимального времени обучения.

В зависимости от успеваемости решения конкретной задачи тем или иным типам автоматов-исполнителей, координатор $A^{(2)}$ может увеличить долю автоматов-исполнителей данного типа в команде автоматов, решающей данную задачу.

Задача распознавания информационных объектов заключается в нашем случае в установке меток безопасности на информационные объекты, а именно, метки: а) «безопасный»; б) «условно безопасный»; в) «потенциально безопасный»; г) «незначительно опасный»; д) «опасный».

Дальнейшая работа с информационными объектами, получившими те или иные метки, заключается в решении задач слежения и/или блокирования (уничтожения) командами автоматов-исполнителей, формируемых автоматом-координатором.

ЛОКАЛИЗАЦИЯ ОШИБОК ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ С КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ В СИСТЕМЕ ЭОКС

А.А. Тегай, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, т. 8-906-947-30-42,

e-mail Headbreaker@ms.tusur.ru

Система ЭОКС – «Электронная Отчетность по Каналам Связи» – это система электронного документооборота по сети Интернет с использованием средств криптографической защиты информации, предназначенная для информационного обмена между налогоплательщиками и налоговыми органами.

Система ЭОКС позволяет:

- представление бухгалтерской и налоговой отчетности в налоговые органы – через сеть Интернет;
- оперативное обновление всех форм отчетности – через сеть Интернет;
- получение информации с доски объявлений налоговой инспекции – через сеть Интернет;
- получение сведений об использовании налоговых обязательств перед бюджетами – через сеть Интернет;
- защита всей передаваемой информации от несанкционированного просмотра и искажения средствами криптографической защиты информации, сертифицированными ФАПСИ;
- формирование электронных документов, подтверждающих факт и срок сдачи отчетности.

При работе с электронной отчетностью по каналам связи используется программный продукт НПП «Фактор-ТС» – клиентская программа электронной почты DiPost v.2.500 007C. Программа DiPost предназначена для обмена зашифрованной и юридически значимой информацией между абонентами системы ЭОКС (Электронная Отчетность по Каналам Связи). Почтовая система DiPost предоставляет возможность абонентам системы ЭОКС обмениваться между собой информацией, подписанной электронной цифровой подписью (ЭЦП) отправляющего абонента и зашифрованной открытым ключом получателя сообщения.

Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, чтобы было невозможно без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровые подписи используются для того, чтобы подтвердить, что сообщение пришло действительно от данного отправителя (в предположении, что лишь отправитель обладает секретным ключом, соответствующим его открытому ключу).

Модуль криптографической защиты информации выполняет шифрование файлов и их защиту с помощью электронно-цифровой подписи. Этот модуль автоматически вызывается программой «DiPost» в процессе подготовки файлов отчетности к отправке. Модуль имеет сертификат на право использования для защиты информации, не содержащей сведений, составляющих государственную тайну.

Проблемы защиты содержания электронных документов, однозначной идентификации абонентов системы, защиты электронных документов от несанкционированных изменений решаются с использованием средств криптографической защиты информации, в состав которых входят средства электронной цифровой подписи и шифрования.

При передаче электронных документов, имеющих юридическую силу, абонент после подготовки документа подписывает его электронной цифровой подписью (ЭЦП) с использованием своего закрытого ключа, закрывает содержание документа с использованием открытого ключа получателя и отправляет его.

В результате работы с программой DiPost многие пользователи не знают, как реагировать на ошибки, возникающие в программе. Ошибки повторяются, и пользователи не могут с ними справиться. Ошибки могут быть связаны с шифрованием писем, расшифрованием писем, при работе с ключами абонентов, при работе с личными ключами пользователей или при работе с адресной книгой программы, которая непосредственно связана с базой данных открытых ключей абонентов. Пользователи обращаются за помощью к специалистам, но не всегда получается вовремя и точно определить источник ошибок и способ их устранения.

Для изучения источников ошибок необходимо знать структуру ключевой информации.

Ключевая информация: открытый ключ, закрытый ключ, ключ центра сертификации, файл базы данных открытых ключей.

Открытый ключ – это ключ, предназначенный для шифрования.

Закрытый ключ – это ключ, предназначенный для дешифрованя.

Файл базы данных открытых ключей – файл программы DiPost, в котором содержится вся открытая ключевая информация об абонентах системы ЭОКС.

В данный период проведены исследования возможных ошибок криптографического модуля программы DiPost. Ошибки изучались на основе экспериментов проводимых с программой и с ключевой информацией, предназначенной для шифрования и подписывания писем пользователей. Ошибки создавались искусственно изменением каких-либо полей в файлах ключевой информации. Ошибки, выявленные при работе с ключевой информацией и работой криптографического модуля, показывают, что возможны различные ситуации в работе с программой DiPost.Все полученные опытным путем ошибки классифицировались и разрабатывались рекомендации по их устранению. Также реализована программа, в которой по виду ошибки выдается рекомендация по устранению этой ошибки.

Программа может быть полезна любому пользователю программы DiPost и поможет сэкономить время при обнаружении ошибки. Не будет необходимости связываться со специализированными центрами для устранения ошибки. Также возможно применение программы в самих специализированных центрах для выявления источника ошибок и помощи своим абонентам в преодолении трудностей с работой в программе DiPost, чтобы отчетность абонентов происходила в срок и без трудностей.

ЛИТЕРАТУРА

1. *Руководство* пользователя почтовой системы «Криптограф» / Иванов П.В. – Казань, 2005.–с. 6 – 14.
2. *Технология* ДИОНИС. DiPOST Crypto. Москва, 2002. с. 10–27.
3. *Технология* ДИОНИС. Центр генерации Ключей. Москва, 2002. с. 5.
4. *Технология* ДИОНИС. Руководство администратора. Москва, 2002. с. 5–15.

САМОКОНТРОЛЬ ЦЕЛОСТНОСТИ ПРИЛОЖЕНИЙ

Р.А. Цецульников, студент 5 курса гр. 521-1 каф. КИБЭВС
ТУСУР, г. Томск, fandelphi@ngs.ru

Цель работы – написать программу, которая проверяет свою целостность и содержит свою контрольную сумму.

Задачу разобьем на две части. Это делается для того, чтобы не хранить в защищенном файле процедуры коррекции контрольных сумм.

– Первая – защищенная программа, которая будет проверять свою контрольную сумму, и содержать в себе константу со значением этого CRC.

– Вторая – программа, которая будет прописывать контрольную сумму в скомпилированный код готового исполняемого файла первой программы и выполнять необходимую коррекцию, чтобы эта контрольная сумма соответствовала действительности.

Из данных мы имеем:

– Контрольную сумму исполняемого файла защищенной программы – это та CRC, которую будет иметь файл после всех операций над ним.

– Смещение в исходном файле ячейки, хранящей контрольную сумму. По этому смещению вторая программа запишет туда CRC.

Прописать контрольную сумму в определенное место защищенного файла так, чтобы она соответствовала тому, что получит сама защищенная программа при проверке самой себя.

Ячейка исходного защищаемого выполняемого модуля, в которой хранится контрольная сумма (назовем ее B1), должна быть статической непрерывной переменной, объявленной в области кода или данных программы. За этими четырьмя байтами идут еще четыре байта (назовем их B2), которые будут использованы для коррекции CRC файла после того, как мы в файл пропишем число, определяющее его CRC. Реверсно выполнять алгоритм CRC (считать CRC файла от его результата к его началу, проходя алгоритм CRC в обратном направлении, то есть получить CRC в заданной точке), имея файл и его CRC, но при условии прохождения алгоритма в обратном направлении с конца файла через неизменяемые байты до последнего корректировочного байта.

Реверсное выполнение алгоритма, разделил на три типа:

– Первый вычисление начального CRC, имея конечный CRC и буфер.

– Второй это поиск последовательности байт, которые приведут к нужному CRC, если его начать с определенного CRC. Дальше нам потребуется именно второй вариант алгоритма вычисления CRC.

– Третий, он собственно разновидность второго, это восстановление последовательности байт буфера CRC которого считали, имея конечный CRC и длину буфера.

Перед компиляцией первой (защищенной) программы кладем в эти 8-байт (B1 и B2) уникальную сигнатуру. DW 0ABABh,0ABABh//– сюда мы будем писать CRC-32; DW 0CDCDh,0CDCDh//– четыре подгоночных байта для восстановления CRC-32

Алгоритм подготовки входных данных

1) Вычисляем контрольную сумму, начиная со значения C0, от начала файла F0 до конца корректировочного блока B2. Запоминаем ее в C1.

2) Начиная со значения C1, продолжаем расчет CRC до конца файла F0. Сохраняем его в CE. Это будет CRC исходного файла, которую мы и пропишем в нашу ячейкуB1.

3) Прописываем CE в B1. За этим блоком идет четыре поправочных байта. Их мы скоро будем вычислять.

4) Рассчитываем CRC измененного файла для измененного блока B1 (красного цвета), до начала блока с корректировочными байтами B2 не включая поправочное байты! В файл должны быть внесены все изменения, чтобы осталось записать только корректировочные байты.

В итоге нас интересуетC1 – CRC к которой должен быть приведен фрагмент файла F1 от начала файла до конца блока B2 C2 – CRC в точке перед началом блока B2 которая получилась после внесения изменений в блок B1, мы записали туда CRC файла. Подчеркнуто специ-

ально, потому что пример несколько неудачен: конец блока B1 сливается с началом блока B2.

Алгоритм подбора корректировочных байт. Способы его реверсирования, вычисления последовательности байт которые дают нужный CRC из некоего стартового значения CRC. Нам нужен второй вариант алгоритма реверсирования, о котором уже упоминалось выше – поиск последовательности байт приводящих CRC к нужному значению.

Вычисления последовательности байт по исходному и конечному CRC:

– CrcFrom – новый CRC, который имеем в начале корректировочного блока

– CrcTo – CRC, который нужно получить в конце корректировочного блока

– lpData – указатель на буфер, куда будут сохранены четыре корректировочных байта

В результате был создан программный продукт, который позволяет проверять свою целостность и хранить свою контрольную сумму.

ЛИТЕРАТУРА

1. *Ross N.* Williams Элементарное руководство по CRC алгоритмам обнаружения ошибок, 1993.
2. *Sergey R.* CRC, и как его восстановить, 1999.

ДОПОЛНИТЕЛЬНАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПО СТАБИЛЬНОСТИ ИХ РАБОТЫ В СИСТЕМЕ НА ОСНОВЕ ДАННЫХ ШТАТНОГО АУДИТА

А.В. Юхненко

Сибирская государственная автомобильно-дорожная академия, ane4ka@e-mail.ru

Штатный аудит – один из сервисов безопасности в защищенных операционных системах, его работа заключается в регистрации событий, которые могут представлять опасность для операционной системы. Необходимость подсистемы аудита в современных операционных системах очевидна: постоянно разрабатываются новые способы атак на операционные системы, сразу обнаружить которые и предотвратить не всегда возможно. В таких случаях с помощью журнала аудита можно выяснить, когда и кем была начата атака, каким образом она осуществлялась.

Большинство сервисов безопасности нацелено на то, чтобы не допустить злоумышленника к объекту защиты (видео наблюдение, идентификация, аутентификация пользователей), но что делать, если зло-

умышленником является законный пользователь системы, обнаружение которого почти невозможно стандартными средствами?

В разработанной программе предполагается использование данных штатного аудита для дополнительной аутентификации пользователей, смысл которой заключается в том, что для каждого пользователя составляется его «типовой портрет работы в системе» (рис. 1). Если происходит подозрительная активность, не свойственная данному пользователю корпоративной сети, то программа фиксирует отличия от его эталонных показателей работы и предупреждает администратора. Администратор может проанализировать действия пользователя и сделать вывод об их правомерности.

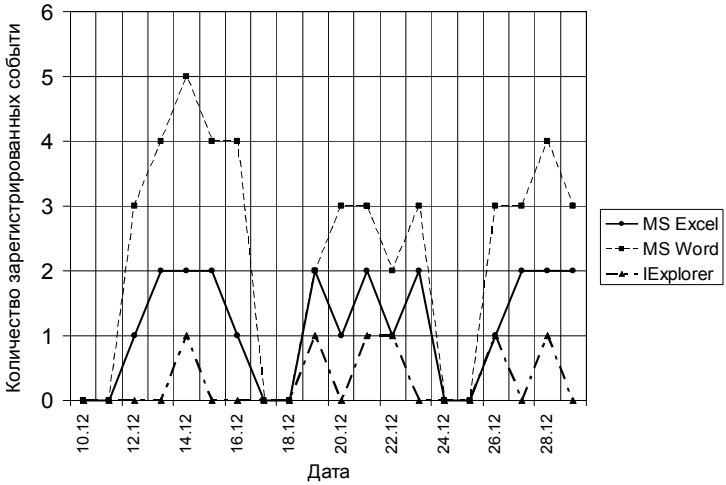


Рис. 1. Типовой «портрет» работы Пользователя-1 в системе, сформированный за 15 дней

На рис. 1 и 2 приведены примеры работы двух пользователей, работающих в одном подразделении. Системой сформированы три графика, характеризующие интенсивность работы пользователей с самыми используемыми приложениями Microsoft: Excel, Word, Internet Explorer в течение двух недель.

Как видно из графиков, даже при использовании самых распространенных приложений у пользователей наблюдаются различия в интенсивности их использования. Есть также приложения, запускаемые только определенными пользователями, такие события являются более информативными для их дополнительной аутентификации.

В составе программы есть модуль для работы с журналами безопасности Windows 2000/XP/2003, который позволяет обрабатывать

статистику событий штатного аудита и выявлять новые информативные признаки для различия пользователей. Разработанная программа использует для анализа данные журнала безопасности, конвертированные в файл формата «.txt», поэтому интересующие события (результат выборки/выборок) всегда можно отобразить в виде диаграммы Microsoft Excel. Анализ данных штатного аудита производится не в реальном режиме времени, а после накопления некоторого числа событий.

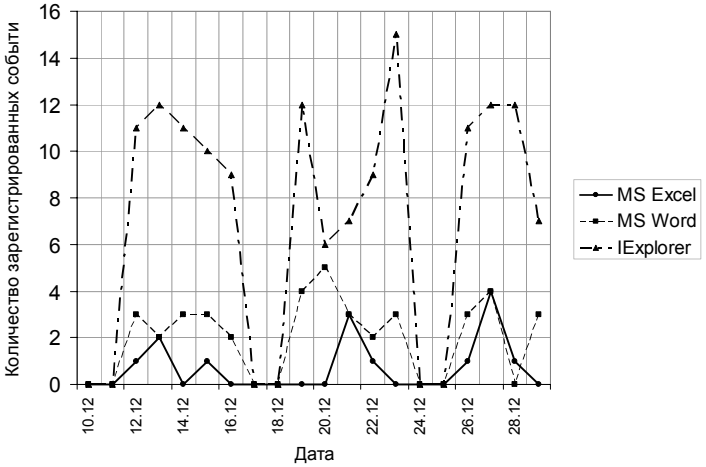


Рис. 2. Типовой «портрет» работы Пользователя-2 в системе, сформированный за 15 дней

Решения, принимаемые описанной программой, являются исключительно рекомендательными для администраторов корпоративных сетей. Сегодня, как правило, администраторы не используют весь спектр регистрируемых событий штатного аудита. Связанно это в первую очередь, из-за неудобств работы с журналом аудита данных операционных систем (Security Events), а также сложностью механизмов перекодировки и анализа событий штатного аудита. Обычно на практике в журналах аудита регистрируются события, которые позволяют администраторам обеспечивать лишь контроль за аутентификацией и изменением списков пользователей. Поэтому разработанная программа позволит более эффективно использовать возможности штатного аудита в повседневной работе.

ЛИТЕРАТУРА

1. *Ложников П.С.* Расширенный аудит событий в операционных системах Microsoft Windows / П.С. Ложников // Информационная безопасность. 2005. № 5. С. 35.

2. *Соколов Е.В.* Анализ различных способов наблюдения за событиями, связанными с файловой системой в ОС Windows NT/2000. http://bezpeka.com/ru/lib/ sec/syst/art393.html
3. *Проскурин В.Г.* Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / В.Г. Проскурин, С.В. Крутов, И.В. Мацкевич И.В. М.: Радио и связь, 2000. 168 с.

ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ МАГИСТРАЛЬНЫМ ТРУБОПРОВОДОМ

Д.Д. Зыков, аспирант каф. КИБЭВС;
А.А. Шелупанов, зав. каф. КИБЭВС, д.т.н, профессор
ТУСУР, г. Томск, т.41-34-26, d-zykov@ngs.ru

По всему миру различные компании предлагают GSM решения для задач учета энергоресурсов, навигации, телеметрии, логистики, безопасности и др. [1,2]. Однако нет примеров использования GSM для управления сложными промышленными объектами (например, магистральными трубопроводами для перекачки нефти и нефтепродуктов).

Рассмотрим систему телемеханики линейной части магистрального трубопровода. Как правило, такая система включает несколько контрольных пунктов (КП), установленных на трубопроводе через каждые 10-15 км, и один диспетчерский пункт (ДП) (рис.).

Схема системы телемеханики с использованием сети связи стандарта GSM

В телемеханических системах (ТС) могут передаваться все или только некоторые виды контрольной и управляющей информации. При передаче информации лишь о значениях параметров объектов ТС называется системой телеизмерения (ТИ); в системе телесигнализации

(ТС) передается преимущественно информация о том, в каком из возможных состояний (обычно из двух) находится контролируемый объект; в системе телеуправления (ТУ) передаются только команды управления. В комбинированных ТС осуществляется передача информации нескольких видов, например измерительной и сигнализирующей (ТИ – ТС), управляющей и сигнализирующей (ТУ – ТС). В комплексных ТС возможна передача контрольной и управляющей информации всех видов (ТУ – ТС – ТИ).

В рассматриваемой системе от ДП к КП передаются команды управления (ТУ), а в обратном направлении – данные, необходимые для контроля (ТИ и ТС). Таким образом, данная система является комплексной телемеханической системой.

Данные ТУ, ТС и ТИ имеют разные свойства (таблица).

Свойства данных, передаваемых в системе телемеханики

	ТИ	ТС, ТУ
Объем	Большой	Маленький
Время доставки	Не критично	Должно быть минимальным
Надежность доставки	Стандартные требования	Повышенные требования

На сегодняшний день сотовые операторы могут предложить следующие основные услуги: SMS, режим Data call и режим GPRS [3]. По своим характеристикам для передачи ТИ подходит режим Data call, а ТС и ТУ целесообразно передавать посредством SMS.

Исследования существующих систем телемеханики на основе GSM показали, что эти системы не являются комплексными системами телемеханики и в них, как правило, используется только один вид сервиса, предоставляемый оператором GSM. Более универсальные из применяемых в настоящее время разработок позволяют выбрать один из сервисов GSM для передачи информации, но одновременная работа Data call и передача/прием SMS в них не реализованы.

Таким образом, в настоящее время не разработаны комплексные системы телемеханики на основе GSM, и необходимо исследовать возможность создания такой системы. Перечислим основные задачи, которые требуется решить при разработке системы.

Во-первых, новая система должна обеспечивать одновременный прием и передачу разных видов телемеханических данных (ТИ, ТС, ТУ). Т.к. для разных видов данных целесообразно использовать различные виды сервисов GSM, то фактически необходимо обеспечить одновременно прием/передачу SMS и работу Data call.

Во-вторых, необходимо обеспечить информационную безопасность новой системы, важнейшими аспектами которой в данном случае являются:

1) обеспечение целостности данных;
2) обеспечение конфиденциальности;
3) обеспечение аутентичности.

ЛИТЕРАТУРА

1. *Company* portrait. Sensile Technologies SA, 2003. 1 p.
2. *Потемкин В.В., Кузнецов В.С., Бондаренко Д.В.* Опыт применения GSM-технологий в распределенных системах автоматизации по учету // http://www.wws.donin.com/news/20032502/opr_teplovoz.htm
3. *Хуторной С.В.* Сотовые модемы фирм Fargo Telecom и DAI Telecom в автоматизированных системах управления и мониторинга // Автоматизация в промышленности. № 8. 2004.

УЧЕБНО-ПРОГРАММНЫЙ КОМПЛЕКС ПО ПАРОЛЬНОЙ ЗАЩИТЕ

С.С. Черняк, П.С. Ложников, к.т.н.

Сибирская государственная автомобильно-дорожная академия, omsk27thnorth3-6@mail.ru

Сегодня парольная защита является одним из звеньев любой политики информационной безопасности. Она является посредником между компьютерной системой и человеком, обеспечивая последнему доступ к защищаемым информационным ресурсам. Тенденции развития информационных и телекоммуникационных технологий показывают, что при создании программного обеспечения безопасность становится одним из главных ориентиров. Но все усилия производителей программного обеспечения, администраторов, выполняющих его установку и поддержку, могут оказаться бесполезными, если пользователи не будут фундаментально понимать важности парольной защиты.

Пустые пароли, состоящие из одних цифр, пароли, совпадающие с именем учетной записи – все это еще широко распространено в повседневной практике. И как правило успешные атаки на компьютерные системы становятся возможными из-за того, что парольная защита оказывается самым слабым звеном.

Предлагаемый программный комплекс призван показать пользователям математические основы парольной защиты, а также ненадежность простых паролей на примере учетных записей пользователей операционной системы Microsoft Windows 2000/XP (рис. 1).

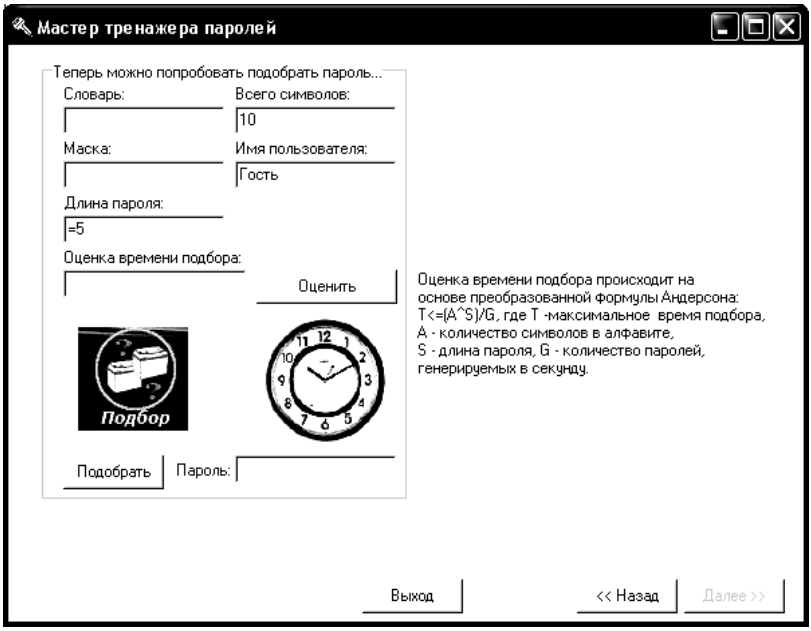


Рис. 1. Учебно-программный комплекс по парольной защите: Мастер оценки времени подбора паролей

В первую очередь, пользователю демонстрируются примеры подборов паролей наиболее распространенных на практике ситуаций: подборы по словарю, «пароль = учетная запись + пароль», «пароль = учетная запись справа налево» и др. Объясняется термин «безопасное время жизни пароля», которое рассчитывается с использованием формулы Андерсона. Также имеется возможность самому побывать в роли хакера, пробуя подбирать пароли к учетным записям операционной системы Windows 2000/XP. Поскольку хакер может использовать не только тотальный перебор для подбора пароля, но и подбор по словарю, по маске, по ограниченному алфавиту, что существенно может сократить время подбора пароля – в учебно-программном комплексе предусмотрен специальный тренажер, реализующий такие возможности.

Тренажер способен подбирать пароли к учетным записям пользователей операционных систем Microsoft Windows 2000/XP/2003 любой длины и сложности, выводить оценочное время подбора пароля, рассчитанное по формуле Андерсона. Предусмотрены возможности задания длины пароля меньше либо больше какого-то значения, выбора учетной записи пользователя, к которой будет подбираться пароль, из

всего списка зарегистрированных пользователей в операционной системе. По ходу работы тренажер дает справочную информацию по парольной защите.

Учебно-программный комплекс реализован в среде C++ Builder 6.0. Демонстрационная версия данного тренажера, установленная на компьютере с процессором Intel Pentium IV 1,8 ГГц и 512 Мб ОЗУ, способна подбирать пароли, состоящие из пяти цифр, к учетным записям пользователей менее чем за минуту. Подбор пятисимвольного пароля, составленного из букв латинского алфавита, занимает не более десяти минут. При этом, используя маску, в которой известен лишь один символ пароля, время подбора сокращается почти вдвое.

Разработанный учебно-программный комплекс может быть также интересен системным администраторам операционных систем Microsoft Windows 2000/XP/2003. В нем содержится описание политик паролей и политик блокировки учетных записей, определяющих надежность парольной защиты данных операционных систем.

ЛИТЕРАТУРА

1. *Borland* C++ Builder 6. Для профессионалов / В.А. Шамис. СПб.: Питер, 2003. 798 с.
2. *Мельников В.* Защита информации в компьютерных системах –М.: «Финансы и статистика», 1997 –368 с..
3. *Холингвэрт Дж., Баттерфилд Д., Сворт Б. и др.* C++Builder 5. Руководство разработчика, том 2. Сложные вопросы программирования: Пер. с англ. М.: Издательский дом «Вильямс», 2001. 832 с.

ФОРМУЛИРОВАНИЯ ТРЕБОВАНИЙ И РЕАЛИЗАЦИЯ СИСТЕМЫ ЭЛЕКТРОННОЙ КАНЦЕЛЯРИИ

П.А. Мельниченко, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, т. 8-906-947-57-64, e-mail mel26@ms.tusur.ru

Формулирование требований к системе

Электронная канцелярия является своего рода надстройкой над системой защищенной и достоверной передачи информации.

Данная система должна обеспечивать набор функций и соответствовать ряду требований, чтобы был соблюден регламент обмена сообщениями, и соблюдено требование конфиденциальности.

Такая система должна быть организована по принципу Клиент-Сервер, где сервер предоставляет клиенту определенный сервис при соблюдении клиентом правил общения, подтверждения и формирования сообщений.

Требования к системе в целом перекладываются, таким образом, на сервер, который является центральным звеном системы и следит за соблюдением правил пользования и общения клиентских приложений.

Серверная часть

На серверную часть возлагается несколько основных функций:

1) Транспорт;
2) Хранение сообщений;
3) Управление учетными записями пользователей;
4) Управление открытыми ключами пользователей;
5) Аутентификация пользователей;
6) Формирование подтверждений;
7) Ведение журналов;
8) Целостность сообщений, подтверждение личности отправителя;
9) Защита передаваемой информации от несанкционированного доступа.

Транспорт

Серверная часть должна обеспечивать транспорт системы, т.е. служить частью, через которую происходит отправка, временное хранение и доставка сообщений.

С точки зрения реализации это означает, что сервер системы должен быть доступен из сетей общего пользования (Интернет) и отвечать требованию доступности.

Хранение сообщений

Сервер системы должен обеспечивать временное хранение передаваемой информации. Она должна быть легко доступна для получателя, отвечать требованию целостности.

С точки зрения реализации это означает, что должна присутствовать база данных передаваемых сообщений, из которой пользователь-получатель имеет возможность получить адресованную ему информацию в любой момент времени и в которую пользователь-отправитель имеет возможность поместить передаваемую им информацию.

Управление учетными записями пользователей

Серверная часть должна хранить информацию о пользователях, зарегистрированных в системе. Таким образом, в обороте информации могут участвовать только пользователи, которые известны системе, ознакомлены с правилами пользования ею и несущие ответственность за действия, совершаемые ими.

Управление открытыми ключами пользователей

Безусловно, в рамках системы для подтверждения целостности информации, удостоверения личности отправителя, соблюдения регламента обмена сообщениями должен присутствовать такой компонент, как СКЗИ.

Для корректной работы этого компонента требуется гарантированное и своевременное распространение ключевой информации (открытых ключей пользователей) внутри системы.

Выполнение этого требования возлагается на серверную часть.

Аутентификация пользователей

Как было сказано выше, к пользованию системой должны быть допущены только пользователи, зарегистрированные в ней.

Удостоверение личности пользователя при попытке получить или отправить сообщение в рамках системы возлагается на серверную часть, так как именно она является транспортом системы и местом временного хранения передаваемой информации.

Формирование подтверждений

Для соблюдения регламента обмена сообщениями требуется формирование служебных сообщений, подтверждающих прием сообщения в обработку системой (сообщение получено и будет доставлено получателю), доставку сообщения получателю, сохранение всех временных штампов происшедших в системе событий.

Так как доставку, прием к доставке, отслеживание событий внутри системы осуществляет серверная часть, она должна формировать служебные сообщения пользователям, чтобы информировать их о происшедших событиях и обеспечить юридически значимые доказательства факта передачи информации.

Ведение журналов

Все события, происходящие в системе должны журналироваться для подтверждения того или иного события. Журналы должны быть доступны обслуживающему персоналу системы и содержать информацию в легко воспринимаемом виде.

Целостность сообщений, подтверждение личности отправителя

Информация, передаваемая в рамках системы должна отвечать требованию целостности. Источник информации должен быть подтвержден во избежание подделки источника.

Защита передаваемой информации от несанкционированного доступа

Передаваемая информация должна быть защищена от несанкционированного доступа, так как может содержать коммерческую, государственную или иную тайну. Для защиты от данного вида угроз целесообразно использовать криптографическую защиту, основанную на принципе двухключевой (открытый и закрытый ключ) информации. Таким образом, требование об управлении открытыми ключами пользователей конкретизируется и делится на две части: управление открытыми ключами проверки подписей сообщений и управление открытыми ключами шифрования сообщений.

Клиентская часть

Клиентская часть должна быть полностью совместима с серверной частью и обеспечивать поддержку всех возможностей, предоставляемых системой.

Аспекты защищенного документооборота.

Для реализации системы защищенного документооборота на территории РФ на основе концепции данной площадки, необходимо учесть несколько требований. Для возможности сертификации данного продукта и использования его в государственных учреждениях (налоговая инспекция и др.) необходимо соблюдать правила, установленные ГОСТом. В частности это ГОСТы шифрования и ЭЦП. Но трудность состоит в том, что алгоритм шифрования ГОСТ 89го года является симметричным, что крайне неудобно и ставит под сомнение некоторые принципы построения данной системы. Так же для генерации ключей необходим сертифицированный Центр Генерации Ключей, услуги которых так же оплачиваются или должны входить в перечень услуг компании, поддерживающей данную систему.

Реализация системы

Система, отвечающая вышеперечисленным требованиям, реализована на каф. КИБЭВС ТУСУРа и в данный момент проходит тестирование и отладку.

Сервер реализован для использования на платформе Win32 с ОС Windows NT/2000/XP, так как выполнен в качестве службы Windows. Это позволяет использовать механизм управления службами Windows, который отвечает за постоянную работу службы и обработку ошибок в ходе ее выполнения.

Транспорт системы осуществляется посредством TCP/IP соединений между клиентом и сервером.

Хранение сообщений пользователей, управление учетными записями, хранение ключевой информации, журналирование событий осуществляется посредством хранения нужной информации в БД под управлением СУБД MySQL 4/5.

Аутентификация пользователей системы проводится путем проверки наличия у пользователя закрытого ключа формирования электронно-цифровой подписи, соответствующего открытому ключу, опубликованному на сервере.

Формирование подтверждений осуществляется сервером при выполнении обработки сообщений от пользователей (прием/отправка).

Серверная часть ведет подробные журналы всех выполняемых действий, которые сохраняются на жестком диске в легко воспринимаемом виде.

Проверка целостности и подтверждение личности отправителя сообщений и подтверждений осуществляется посредством обязательного присутствия электронно-цифровой подписи в каждом сообщении, переданном внутри системы.

Защита передаваемой информации осуществляется посредством шифрования сообщений по алгоритму ГОСТ 28147-89 при использовании сертифицированного CSP Крипто-Про.

Клиентская часть предоставляет интерфейс ко всем функциям, предоставляемым сервером.

ЛИТЕРАТУРА

1. http://www.gdm.ru - Проблемы создания системы защищенного документооборота. Щербаков А. Ю
2. Закон РФ «Об электронно-цифровой подписи».
3. Монитор. 1995. N1. А.Ю.Винокуров. ГОСТ не прост..., а очень прост.
4. ЭЦП ГОСТ Р.34.10-2001
5. http://www.cryptography.ru Russian Scientific Network. ЭЦП ГОСТ Р 34.10-2001 (ГОСТ Р 34.10-94).

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Э.А. Сергиенко, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, т. 44-17-99 , e-mail edik@sibmail.com

Неблагоприятная криминогенная обстановка, недобросовестная конкуренция, активизация действий террористов заставляют общество повернуться лицом к проблеме обеспечения безопасности, одним из важнейших аспектов которой является информационная безопасность.

Основные надежды специалисты связывают с внедрением интегральных подходов и технологий. Необходимым условием реализации интегрального подхода является блокирование всех технических каналов утечки и несанкционированного доступа к информации, поэтому для создания эффективных систем безопасности, в первую очередь, необходимо исследовать возможные каналы утечки и их характеристики. Исследование стоит производить имеющимися в наличии программно-аппаратными средствами, а так же следует использовать математические расчеты (различные методики оценки), сделать оценку защищенности информации от утечки по каналу ПЭМИН.

При выявлении технических каналов утечки информации необходимо рассматривать всю совокупность компьютерного оборудования,

включающую технические средства обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п. Следует учитывать также вспомогательные технические средства и системы (ВТСС), такие как оборудование открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др.

Среди каналов утечки заметную роль играют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода, кабели, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции, проходящие через помещения, где установлены основные и вспомогательные технические средства.

Речевая информация является одним из основных источников получения данных о финансовой, научно-исследовательской, производственной деятельности организации, то есть сведений, не подлежащих широкой огласке (иногда и вовсе секретной). Несмотря на значительно возросшую роль автоматизированных информационных систем (АИС), речевая информация в потоках сообщений по-прежнему носит превалирующий характер (до 80% всего потока). Говорящий человек, среда распространения акустических, виброакустических и электромагнитных колебаний, линии распространения электрических колебаний, технические средства обнаружения и обработки указанных колебаний образуют канал несанкционированного доступа к сведениям, подлежащим защите.

Для ее перехвата лицо, заинтересованное в получении информации («противник»), может использовать широкий арсенал портативных средств акустической речевой разведки, позволяющих перехватывать речевую информацию по прямому акустическому, виброакустическому, электроакустическому и оптико-электронному (акустооптическому) каналам. Для противодействия утечке информации по перечисленным каналам существует ряд организационных и технических мер, которые не раз описаны в соответствующей литературе и в правовых актах. Попробуем оценить и систематизировать данную информацию, а так же применить ее на практике в данном проекте.

Цель работы – проведение анализа угроз утечки речевой конфиденциальной и секретной информации из выделенного помещения (ВП); анализ защищенности выделенного помещения от утечки информации по акустическому каналу с помощью оценочных расчетов; проведение инструментального поиска закладных устройств в помещении; проведение инструментального контроля защищенности компьютера; разработка рекомендаций по повышению уровня защищен-

ности ВП. После проведения исследований необходимо сделать вывод об актуальных для данного выделено помещения каналов утечки и дать рекомендации для повышения уровня защищенности выделенного помещения от утечки информации.

При выполнении работы исходными данными являются:

– теоретические сведения по защите информации;

– планы помещений, подлежащих защите;

– специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР). Утверждены решением Государственной технической комиссии при Президенте Российской Федерации от 23 мая 1997г. №55;

– методики оценки возможностей иностранных технических разведок (МВТР - 2010). Утверждены решением Государственной технической комиссии при Президенте Российской Федерации от 26 мая 2000 г. №16.

А так же производится:

– анализ объекта защиты на наличие угроз безопасности информации;

– выбор методик исследования объекта;

– непосредственное исследование объекта;

– рекомендации реализующие комплекс мер по защите ВП от утечки информации по техническим каналам;

– организационные меры повышения уровня защищенности ВП;

– рекомендации для повышения уровня защищенности ВП от утечки информации через акустический и виброакустический каналы;

– рекомендации для повышения уровня защищенности от утечки информации через канал акустоэлектрических преобразований; рекомендации для повышения уровня защищенности от утечки информации через ПЭМИ компьютера;

ЛИТЕРАТУРА

1. *Зайцев А.П.* Технические средства обеспечения информационной безопасности. Учебное пособие для вузов. ТУСУР, Каф КИБЭВС. Томск: ТМЦДО, 2004г. 199с.
2. *Торокин А.А.* Основы инженерно технической защиты информации. М.:Издательство «Ось-89», 1998. 336 с.
3. *Методики* оценки возможностей иностранных технических разведок (МВТР - 2010). Утверждены решением Государственной технической комиссии при Президенте Российской Федерации от 26 мая 2000г. №16.
4. http://www.razvedka.ru Сайт посвященный промышленному шпионажу и борьбе с ним.
5. *Мещеряков Р.В., Шелупанов А.А., Белов Е.Б., Лось В.П.* Основы информационной безопасности. Томск.: ТУСУР, 2002. 350 с.

СОДЕРЖАНИЕ

ПОДСЕКЦИЯ 9.2

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ПОДСЕКЦИЯ 9.3

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Научное издание

Научная сессия ТУСУР – 2006

Посвященной 75-летию Ф.И. Перегудова,

Материалы докладов
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
4–7 мая 2006 года, Томск, Россия
В пяти частях

Часть 3

Печатается без редактирования по текстам, предоставленными авторами

Верстка **В.М. Бочкаревой**

Дизайн обложки **В. Глушко**

Издтельство «В-Спектр»
Сдано на верстку 04.04.2006. Подписано к печати 25.04.2006.
Формат $60\times84^{1}/_{16}$. Печать трафаретная.
Печ. л. 12,79. Усл. печ. л. 11,89.
Тираж 150 экз. Заказ 14.

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