VI Белорусско-российская научно-техническая конференция

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

21 - 22 мая 2008 г.

МИНСК

Министерство образования Республики Беларусь
Государственный центр безопасности информации РБ
Федеральная служба технического и экспортного контроля РФ
Белорусский государственный университет информатики и радиоэлектроники
НИИ Технической защиты информации РБ
Академия управления при Президенте РБ
Объединенный институт проблем информатики НАН РБ

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

МАТЕРИАЛЫ ДОКЛАДОВ И КРАТКИЕ СООБЩЕНИЯ

VI Белорусско-российской научно–технической конференции

21–22 мая 2008 г., Минск

Минск

2008

РЕДКОЛЛЕГИЯ СБОРНИКА

В.Ф. Голиков, Г.В. Давыдов, В.А. Ивкович, В.К. Конопелько, В.А. Лабунов, Л.М. Лыньков, В.И. Новиков, А.М. Прудник

Технические средства защиты информации: Материалы докладов и краткие сообщения VI Белорусско-российской научно-технической конференции. 21–22 мая 2008 г. Минск, Беларусь. Минск, БГУИР. 2008. 100 с.

Издание содержит материалы докладов и краткие сообщения по техническим средствам защиты информации: организационно-правовому обеспечению защиты, средствам обнаружения и подавления каналов утечки информации, программно-аппаратным средствам защиты в компьютерных и телекоммуникационных сетях и в банковских технологиях.

НАУЧНЫЙ ПРОГРАММНЫЙ КОМИТЕТ

М.П. Батура	*д.т.н., проф., ректор БГУИР, председатель программного комитета;*
Л.М. Лыньков	*д.т.н., проф., зав. каф. защиты информации БГУИР, зам. председателя программного комитета;*
В.Н. Алексеев	*зам. начальник управления Федеральной службы технического и экспортного контроля РФ;*
В.В. Анищенко	*зам. ген. директора Объединенного института проблем информатики НАН РБ;*
В.Г. Булавко	*директор Центра НАН Беларуси;*
В.Ф. Голиков	*д.т.н., проф., зав. каф. БНТУ;*
А.Н. Горбач	*начальник отдела ГЦБИ при Президенте РБ;*
В.И. Захаров	*к.т.н., зав. лаб. Российского государственного технологического университета им. К.Э. Циолковского;*
В.М. Колешко	*д.т.н., проф., зав. каф. интеллектуальных систем БНТУ;*
В.К. Конопелько	*д.т.н., проф., зав. каф. СиУТ БГУИР;*
А.П. Кузнецов	*проректор по научной работе БГУИР;*
В.А. Лабунов	*д.т.н., проф., акад. НАН Беларуси;*
С.В. Маслов	*первый зам. нач. ГЦБИ при Президенте РБ;*
Н.И. Мухуров	*зав. лаб. Института электроники НАН Беларуси;*
И.Г. Назаров	*нач. отдела Федеральной службы технического и экспортного контроля РФ;*
В.И. Новиков	*зав. каф. управления информационными ресурсами Академии управления при Президенте РБ;*
А.В. Сидоренко	*д.т.н., проф., БГУ;*
Ю.С. Харин	*член-корреспондент НАН Беларуси;*
А.В. Хижняк	*нач. каф. Военной академии РБ;*
О.В. Чурко	*директор НИИ технической защиты информации.*

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Л.М. Лыньков	*д.т.н., зав. каф. ЗИ БГУИР, председатель оргкомитета;*
А.М. Прудник	*к.т.н., доц. каф. экологии БГУИР, зам. председателя оргкомитета;*
В.А. Богуш	*д.ф.-м.н., зав. каф. метрологии и стандартизации БГУИР;*
В.Ф. Голиков	*д.т.н., проф., зав. каф. БНТУ;*
Г.В. Давыдов	*к.т.н., зав. НИЛ БГУИР;*
В.А. Ивкович	*нач. патентно-информационного отдела НИЧ БГУИР;*
В.К. Конопелько	*д.т.н., проф., зав. каф. СиУТ БГУИР;*
В.Ф. Томилин	*зам. проректора по НИЧ БГУИР.*

СОДЕРЖАНИЕ

Секция 1. Технические средства обнаружения и подавления каналов утечки информации

Секция 2. Программно-аппаратные средства защиты информации в компьютерных и телекоммуникационных сетях

Секция 3. Проектирование и производство элементов и компонентов для систем защиты информации

Секция 4. Организационно-правовое, методологическое и образовательное обеспечение защиты информации

СЕКЦИЯ 1. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

ВИБРОАКУСТИЧЕСКИЙ КАНАЛ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

О.Ю. КОНДРАХИН

Ограждающие строительные конструкции помещений совершают незначительные колебания под воздействием акустических волн. Для перехвата информации, переносимой этими колебаниями, не обязательно регистрировать акустические колебания, переизлученные этими конструкциями, достаточно зафиксировать колебания собственно строительных конструкций. Так, например, под воздействием звука $P_{ак}$=70 дБ (обычный разговор) кирпичная стена толщиной 0,5 м совершает вибрационные колебания с ускорением $a \approx 3 \cdot 10^{-5} g$. При таких условиях использования современных технических средств разведки может быть прослушан даже шепот. Сегодня профессионалы любят использовать стетоскопы, которые избавили от утомительного сверления отверстий в ограждающих конструкциях. Конструктивно они состоят из вибродатчика с нанесенной на него мастикой для прикрепления к ограждающей конструкции, инженерным коммуникациям, блока усиления с регулятором громкости и головных телефонов. Размеры датчиков составляют ≈2,2×0,8 см, диапазон принимаемых частот ≈300–3000 Гц, вес ≈100 г, коэффициент усиления ≈20 000. С помощью подобных средств можно прослушивать через стены толщиной до 1 м. Кроме свойств вибродатчика, на качество шума влияют толщина и материал изготовления стен, уровень шумов и вибраций в обоих помещениях, правильное место выбора расположения датчика и т.д.

Однако, так как не всегда возможно постоянно находиться в соседнем помещении, вибродатчик оснащается проводным, радио- и другими каналами передачи информации, которые аналогичны тем, которые используются с микрофонами. Преимущество вибродатчиков проявляется в том, что они могут устанавливаться не в самом, зачастую тщательно охраняемом помещении, а в соседних, на которые службы безопасности обращают гораздо меньше внимания.

Таким образом, вибрационные колебания ограждающих конструкций, инженерных коммуникаций под воздействием звуковых волн сегодня образуют один из наиболее опасных виброакустических каналов утечки информации.

Современные строительные материалы и конструкции (монолитный железобетон, сборные железобетонные конструкции, кирпичная кладка) обладают весьма низкими показателями затухания механических колебаний в области звуковых частот. За счет этого обеспечивается возможность распространения колебаний на значительные расстояния и создает потенциальный канал утечки информации, регистрируя колебания значительно удаленных элементов здания. В зависимости от конструкций здания и качества выполнения стыков меду его элементами, затухание на стыках варьируется в пределах от 1–3 дБ до 10–15 дБ. отсюда следует важная тактическая особенность и повышенная опасность виброакустического канала утечки информации – перехват информации возможен не только из смежных помещений, но и из помещений, значительно удаленных от источника информации.

Некоторые элементы строительных конструкций, как и в случае рассмотрения акустического канала, представляют собой волноводы вибрационных колебаний. К ним относятся трубы различных инженерных коммуникаций (отопления, водоснабжения, электропитания, системы кондиционирования и т.д.). Как и в случае воздушных волноводов, значительная разница в величинах акустического сопротивления материала труб и окружающей среды составляет $(\rho C)_{ст}/(\rho C)_{бет} \approx 4 \ldots 8$.

Создаются условия волноводного распространения сигналов на значительные расстояния. Данный канал становится особенно опасным, если трубопровод соединен с какой-то жесткой и развитой поверхностью, которая играет роль согласующего элемента при передаче энергии из воздуха в трубопровод. Таким согласующим элементом, например, являются современные легкие радиаторы отопления.

Необходимость и важность проведения мероприятий по защите помещений от утечки речевой информации по виброакустическим каналам чрезвычайно актуальна не только при выполнении регламентированных требований по защите помещений, в которых обрабатывается информация, содержащая государственные секреты, но и для любых организаций и учреждений, в которых ведутся конфиденциальные переговоры. В зависимости от режима обеспечения границы контролируемой зоны защита акустических и виброакустических каналов утечки имеет специфические особенности и ограничения, усложняющие реализацию эффективной защиты. В большинстве ситуаций применение активных мер защиты каналов утечки приводит к появлению мешающих акустических шумов, существенно снижающих комфортность работы в защищаемом и смежных помещениях. В большинстве случаев применение только пассивных мер защиты не может полностью решить задачу при условии расчета показателя защищенности, ориентированного на предельные акустические помехи. Очевидно, что только комплексное применение активных и пассивных методов и средств может обеспечить защиту оптимальным образом, выполняя требования по защите информации и одновременно обеспечивая минимальный уровень мешающих акустических шумов в помещениях.

Литература

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам / Учеб. пособие. М., 2005. С. 37–38.

РАЗБОРЧИВОСТЬ РЕЧИ В КАНАЛЕ УТЕЧКИ ИНФОРМАЦИИ

О.Ю. КОНДРАХИН

Разборчивость речи основана на оценке биологического сигнала, генерируемого человеком и воспринимаемого органами слуха. Важными факторами ее оценки являются условия, в которых воспроизводится и воспринимается речь. Наиболее объективной оценкой разборчивости речи является метрологическая. При метрологической оценке разборчивости речи возникают дополнительные факторы, которые необходимо учитывать. Важнейшими факторами, влияющими на точность оценки разборчивости речи, являются искусственные помехи. Присущие же акустическому речевому сигналу реверберационные помехи обусловлены переотражениями речевого сигнала в замкнутом объеме. Кроме того, акустический речевой сигнал искажается резонансными явлениями внутри замкнутого пространства. С учетом влияющих факторов должно быть установлено соответствие между величиной, характеризующей качество восприятия речевого сигнала, и полученным результатом ее измерения. Речевой сигнал сложен по своему звуковому составу, т.к. включает гармонические и шумовые составляющие. Для метрологической оценки разборчивости речи важно обосновать выбор измерительного сигнала. Измерительный сигнал формируют и генерируют, используя элементы речевого сигнала (слова, слоги). Из слов или слогов формируются артикуляционные таблицы (таблицы разборчивости речи).

В аппаратуре связи для контроля качества передачи речевого сигнала используют гармонический сигнал. Белый шум в полосе речевого сигнала для оценки качества передачи речевого сигнала используют при разбиении его на октавные либо третьоктавные полосы частот. Обосновано и рекомендовано использование гармонического сигнала в качестве измерительного. Предложены параметры и характеристики, необходимые для расчета разборчивости речи:

– уровень спектральной плотности речевого сигнала, дБ;

– уровень спектральной плотности фонового шума в речевом диапазоне частот, дБ.

Учитывая, что спектральная характеристика речевого сигнала частотозависима, кривая чувствительности уха неравномерна в полосе речевого сигнала, спектральная плотность фонового шумового сигнала экспоненциально спадает от нижних частот, распространение речевого сигнала зависит от затухания среды распространения. Среда распространения включает прохождение речевого сигнала через элементы ограждающих конструкций помещения (окна, двери), инженерные элементы (системы кондиционирования, системы отопления, газоводоснабжения и др.). Полосу речевого сигнала разбивают на n полос равной разборчивости. В каждой n-й полосе излучается от 1 до m полос. Этим компенсируется погрешность, обусловленная неравномерностью АЧХ канала утечки информации. Шумовые сигналы в полосе речевого сигнала в октавных (третьоктавных) полосах измеряются шумомером. Шумомеры, предназначенные для оценки характеристики шума, градуируются гармоническими сигналами. В отличие от гармонического измерительного сигнала, речевой сигнал, а также искусственные помехи, являются нестационарными. Использование шумового сигнала в октавных полосах не исключает влияния на результаты измерений нестационарных искусственных помех окружающего пространства. Информативность канала утечки информации необходимо оценивать по единому критерию. Таким критерием является порог минимальной разборчивости речи. В этой связи измерительным сигналом должен использоваться гармонический сигнал, который легко выделять из шумов.

Основной формой автоматизации процессов измерения является разработка специального программного обеспечения, аппаратного анализа случайных процессов. Акустические и вибрационные поля, ослабленные средой распространения, распространяются за пределы контролируемой зоны и могут быть перехвачены акустическим приемником. Те же поля одновременно могут воздействовать на электрические цепи и из -за параметрической модуляции наводят информационные токи (напряжения), образуя, таким образом, электроакустический канал утечки информации. Кроме того, поля, воздействуя на ВЧ-генераторы сложной системы, параметрически модулируют ВЧ-колебания, которые образуют электромагнитные ВЧ-поля. Предметом теории разборчивости речи является раздел теории информации, представленный в форме научных знаний, дающий целостное представление о свойственных данному языку закономерностях истолкования речевых сообщений и существующих связей речевой информации при ее передаче с окружающей средой.

Принцип защиты информации заключается в снижении разборчивости речи в канале утечки информации ослаблением уровня излучаемого сигнала, увеличении затухания среды распространения, увеличении уровня маскирующих шумов, скрытности функционирования информационной системы. Для речевых сигналов критерием защищенности учитывают установленную величину разборчивости речи на выходе канала утечки информации.

Литература

1. Железняк В.К. Защита информации от утечки по техническим каналам / Учеб. пособие. СПб., 2006. С. 69–109.

ПОМЕХИ ЕСТЕСТВЕННОГО ПРОИСХОЖДЕНИЯ В СИСТЕМАХ АКУСТИЧЕСКОЙ РАЗВЕДКИ И МОНИТОРИНГА МЕСТНОСТИ

А.М. Гладышев

Ведение акустической разведки и мониторинга местности затрудняется наличием интенсивных помех естественного происхождения. Осуществление эффективной фильтрации помех требует знания их спектральных характеристик.

К наиболее существенным помехам естественного происхождения следует отнести шум ветра (в листве, траве, ветвях деревьев и т.д.), шумы гидродинамического происхождения (шум рек, дождя), пение птиц, звуки грома. Наибольшей вероятностью появления обладают шумы ветра и шумы гидродинамического появления. Формы кривых спектральной плотности мощности для шума ветра в лиственном лесу и шума дождя схожи. Обе кривые начинаются с области низких частот, затем на отрезке от 500 Гц до 1 кГц имеется сильный подъем кривой с максимумом около 1 кГц, а затем наблюдается плавный спад. При увеличении скорости ветра, а также при увеличении интенсивности дробления капель воды спектр становиться более равномерным, повышается интенсивность высокочастотных составляющих, а максимум спектра становится более расплывчатым в области 1–2 кГц, при этом верхняя граница спектра может достигать 6–8 кГц.

Звук грома наибольшую энергию имеет в инфразвуковом диапазоне частот в области 0,25–2 Гц, а также имеется и второй, меньший максимум в звуковом диапазоне частот 125–250 Гц. Пение птиц имеет периодическую структуру и дискретный спектр, максимумы которого сильно варьируются и зависят от конкретного вида птиц.

Для успешного подавления помех естественного происхождения целесообразно применять высокочастотную фильтрацию ($f_в$=0,5–1 кГц) и специальные меры по защите микрофонов от ветра, а также желательно иметь априорные данные о временной структуре принимаемого сигнала для осуществления его дополнительной селекции.

ФОРМИРОВАНИЕ АКУСТИЧЕСКОЙ ВОЛНЫ ВОЗДУШНЫМ ВИНТОМ САМОЛЕТА

А.М. Джеки, С.Р. Гейстер

Обнаружение легкомоторных летательных аппаратов (вертолетов и легкомоторных самолетов) на малых и предельно малых высотах является важной задачей. В приграничной зоне мониторинг малых высот осуществляется с целью пресечения ввоза наркотиков и контрабандных товаров, вывоза ценностей, а также исключения незаконного пересечения границы воздушным путем. Решение задачи мониторинга на малых и предельно малых высотах с использованием радиолокационных средств затруднено негативным влиянием земной поверхности на распространение радиоволн, низкой радиолокационной заметностью и малыми скоростями движения легкомоторных летательных аппаратов (ЛА). Это обусловливает необходимость разработки и создания новых эффективных средств обнаружения, в которых используются естественные физические явления, возникающих при полете легкомоторных ЛА на малых и предельно малых высотах. Одним из таких явлений является звук, порождаемый работой воздушных винтов.

Рассматриваются физические основы формирования акустической волны воздушным дозвуковым винтом легкомоторного самолета. Описывается математическая модель давления вдоль вращающейся лопасти винта в зонах повышенного и пониженного давления.

Представляется оригинальная методика определения и математическая модель временной структуры акустического сигнала, формируемого идеальной лопастью.

ДЕТЕКТИРОВАНИЕ РЕЧИ

О.Б. Зельманский

Одной из самых естественных форм взаимодействия для человека является речь. Поэтому в современных компьютерных системах приветствуется, а в некоторых случаях и является крайне необходимым, использование средств речевого взаимодействия с пользователем. Начальным блоком систем распознавания речи является детектор речевого сигнала, целью которого является определение наличия речи в поступающем на его вход сигнале на фоне изменяющейся акустической обстановки.

Для детектирования речи могут применяться следующие методы:

Расчет классификационных параметров сигнала и сравнение их значений с пороговыми значениями. В качестве классификационных параметров могут выступать такие признаки, как: амплитуда сигнала, энергия сигнала, число переходов сигнала через нулевой уровень, коэффициент отношения сигнал/шум в частотном и временном диапазонах и др. При этом для определения порога часто используется метод, называемый минимум статистики, который основан на отслеживании минимума классификационного параметра [1]. К достоинствам данного метода можно отнести сравнительную простоту реализации.

Метод линейного предсказания [2]. Основной принцип которого состоит в том, что текущий отсчет речевого сигнала можно аппроксимировать линейной комбинацией предшествующих отсчетов. Коэффициенты предсказания, а именно весовые коэффициенты, используемые в линейной комбинации, при этом определяются однозначно минимизацией среднего квадрата разности между отсчетами речевого сигнала и их предсказанными значениями. Однако недостатком метода линейного предсказания является большой объем вычислений, необходимый для получения высоких результатов.

В последнее время алгоритмы анализа речевого сигнала, основанные на свойствах человеческого уха, получили широкое распространение, в связи с чем были разработаны методы детектирования речи, заключающиеся в разработке искусственных нейронных систем, физическая архитектура и принципы конструирования которых взяты у биологических прототипов [3]. Этот метод обеспечивает высокую достоверность, но сложен для реализации.

Детектор речи является важной частью современных приложений по обработке речи. Детектирование речи используется в компьютерных системах с голосовым управлением, в системах с биометрическим контролем доступа, в системах кодирования и распознавания речи, в системах повышения качества речи, в системах передачи речевых сигналов, в системах прослушивания. Положительные эффекты от использования в перечисленных выше системах качественных детекторов речи заключаются в уменьшении числа арифметических операций при обработке сигналов, понижении энергопотребления устройств, снижении загруженности информационных каналов, экономии затрат на передачу речевых сигналов.

Таким образом, в виду того, что характеристики детектора речи во многом определяют качество работы всей системы в целом, алгоритмы детектирования часто являются наиболее критической частью таких систем и одновременно с улучшением их качества, увеличивается качество и всей системы.

Литература

1. Петровский А.А. и др. Речевые интерфейсы ЭВС / Учеб.-метод. пособ. Минск, 2004.
2. Рабинер Л.Р. Шафер Р.В. Цифровая обработка речевых сигналов / Справочник М., 1981.
3. Лобанов Б.М., Елисеева О.Е. Речевой интерфейс интеллектуальных систем / Учеб. пособ. Минск, 2006.

СИСТЕМА ЛАЗЕРНОГО НАБЛЮДЕНИЯ НА БАЗЕ СИСТЕМЫ ПЕРЕМЕЩЕНИЯ "ТРИПЛАНАР"

В.В. Поляковский, В.П. Колтунов

В последние годы наблюдается активное развитие систем лазерного наблюдения, принцип действия которых основан на постоянном сканировании защищаемого пространства лазерами невысокой мощности. Гибкость таких систем определяется возможностью премещения лазероного луча по заданной траектории обхода охраняемых ценностей с высокими скоростью и точностью, что накладывает достаточно жесткие требования на системы перемещения лазеров. Одним из возможных способов реализации системы перемещения лазера является использование параллельных манипуляционных систем (ПМС), которые характеризуются высокой структурной жесткостью, повышенными кинематическими и динамическими свойствами, хорошими массогабаритными показателями. К такому классу механизмов относится рассматриваемый в работе "Трипланар", созданный совместными усилиями технического университета г. Ильменау (Германия), БГУИР (Минск) и СП "Рухсервомотор" (Минск).

"Трипланар" представляет собой ПМС в виде раскрывающегося тетраэдра, верхние ребра которого определяют подвижный треугольник (исполнительный элемент), с которым жестко связывается рабочая платформа с лазером. Верхние ребра представляют собой шарнирные соединения, нижние выполнены таким образом, что нижние вершины боковых треугольников могут быть связаны с тремя планарными приводами посредством сферических шарниров. Рабочая платформа механизма обладает шестью степенями свободы за счет независимого плоскопараллельного перемещения трех планарных приводов. В качестве датчиков обратной связи в планарных приводах ПМС "Трипланар" используются датчики на основе эффекта Холла.

В работе показано, что важнейшей задачей при постронеиии системы перемещения "ТриПланар" является задача обеспечения совместной бесколлизионной работы трех позиционеров на одном статоре. Для решения этой задачи авторами предлагается использовать алгоритмы предотвращения коллизий, полученный методами аналитической геометрии, в сочетании с заложенной системой приоритетов.

ОЦЕНКА УРОВНЯ ИСТОЧНИКОВ ШУМА В ИКШ ТРЕХМИЛЛИМЕТРОВОГО ДИАПАЗОНА

А.Я. Бельский, А.В. Гусинский, А.Ю. Ярмолич

В трехмиллиметровом диапазоне длин волн существенную роль при проведении точных измерений играют собственные шумы измерителя. Балансный смеситель является его важнейшим узлом. Он выполняется обычно на диодах с барьером Шоттки. Приводится эквивалентная шумовая схема, учитывающая тепловой, дробовой и избыточный шумы. Выясняются причины аномального поведения избыточного шума при изменении величины тока, протекающего через диод. Анализируются причины, приводящие к увеличению уровня избыточных шумов, связанные с состоянием поверхности полупроводникового материала и рассматриваются способы их уменьшения. Приводятся экспериментальные результаты исследования уровня избыточных и "белых" шумов в области низких и высоких частот. При расчете тепловых шумов рассматривается учет квантовой поправки, которая играет более существенную роль в высокочастотной области миллиметрового диапазона длин волн. Отмечается, что определенный вклад вносят также тепловые шумы за счет диссипативных потерь в стенках волноводной линии передачи и магнитные шумы невзаимных ферритовых изделий.

Формулируются требования, предъявляемые к гетеродину трехмиллиметрового диапазона волн по уровню его фазовых и амплитудных шумов. Рассматриваются различные варианты использования имеющихся гетеродинов, их шумовые характеристики и другие наиболее важные эксплуатационные характеристики и параметры.

ЗВУКОПОГЛОЩАЮЩИЕ КОНСТРУКЦИИ ДЛЯ СОЗДАНИЯ ОПТИЧЕСКИ ПРОЗРАЧНЫХ МОДУЛЬНЫХ ПЕРЕГОВОРНЫХ КАБИН

С.Н. ПЕТРОВ

Переговорные кабины, сконструированные из оптически прозрачных звукоизолирующих материалов, эффективно обеспечивают конфиденциальность речевой информации, позволяя при этом пользователю визуально обнаруживать закладные устройства. Материалом для создания такого рода кабин являются прозрачные пластики. Также конструкции переговорных кабин должны исполняться в сборном виде из модульных блоков, чтобы обеспечить легкость и удобство сборки. Создание унифицированных модульных блоков для переговорных кабин позволит собирать конструкции с различными габаритными размерами.

Недостатком такой кабины является низкий коэффициент звукопоглощения пластика, в результате чего, время реверберации внутри кабины превышает оптимальное. Использование мягких пористых материалов для уменьшения переотражений приведет к потере оптической прозрачности кабины. Рассматривается возможность уменьшения переотражений звуковых волн за счет использования объемных звукопоглотителей из прозрачных упругих пленок (ПВХ, резина).

СЕКЦИЯ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

АРХИТЕКТУРА ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ ГРИД-СИСТЕМЫ

В.В. Анищенко, А.В. Глевич

В данном докладе предлагается архитектура инфраструктуры открытых ключей (ИОК) грид-системы для аутентификации и защиты процесса обмена данными пользователей в грид-системе. Основная цель ИОК грид-системы — обеспечение, путем применения цифровых сертификатов, надежной связи открытых ключей с объектами, что позволяет другим объектам проверить эту связь и получить необходимые услуги для осуществления управления ключами в распределенной среде. ИОК интегрирует цифровые сертификаты, криптографию с открытыми ключами и органы сертификации в единую архитектуру безопасности грид-среды.

Сертификаты ключей используются для аутентификации пользователей, аутентификации шлюзов, аутентификации диспетчера сетевых заданий, подписи заданий, подписи программного обеспечения. В иерархии ИОК грид-системы предлагается использовать два уровня: корневой сертификационный центр (СЦ) и СЦ грид-системы. Корневой СЦ используется для подписи СЦ грид-системы и гарантирует его целостность. Сертификат СЦ грид-системы подписывается корневым СЦ и получает необходимые права для подписания пользовательских и серверных сертификатов с меньшим объемом прав. СЦ грид-системы использует собственный список отозванных сертификатов для отзыва вышедших из употребления сертификатов и сертификатов с нарушенной подписью, т.е. сертификатов, личные ключи которых похищены или потеряны. Сертификаты и списки отозванных сертификатов как корневого СЦ, так и СЦ грид-системы доступны для всех клиентов, так как они могут быть использованы при проверке цепочки сертификатов. Сертификат нижнего уровня действителен только тогда, когда действительны все вышестоящие сертификаты.

Особенно важным условием функционирования ИОК грид-системы является обеспечение комплексной безопасности — использование организационно-технических мер и программно-технических средств защиты.

ОРИЕНТИРОВАННАЯ НА ПОЛЬЗОВАТЕЛЯ МОДЕЛЬ ОДНОКРАТНОГО ВХОДА В ГРИД-СИСТЕМУ

А.В. Глевич, Ю.В. Земцов

Обеспечение однократного входа в грид-систему является важной, но сложной в реализации задачей. В настоящий момент предложено множество подходов, призванных решить данную задачу. Тем не менее, реализованные подходы не в полной мере отвечают современным требованиям безопасности и удобства в использовании. В данном докладе представлена схема аутентификации клиента в грид-системе и его последующей авторизации. В докладе также описаны наиболее популярные в современных грид-системах подходы к аутентификации, приведены их недостатки и предложены способы их устранения. Предлагаемая модель представляет собой вариант инфраструктуры открытых ключей, обеспечивающей выполнение пользователем основных действий в грид-системе, например, безопасного запуска задания, делегирования полномочий и управления учетной записью. Указываются основные

преимущества предлагаемого подхода в области удобства в использовании, защиты данных пользователя и информационной безопасности в целом. Описываемая модель в полном мере ориентирована на пользователя в том смысле, что пользователь действует как свой собственный удостоверяющий центр, самостоятельно принимающий решение о передачи данных в грид-среду.

Наиболее существенные преимущества предлагаемой модели:

– реализация однократного входа в грид-среду;

– защита от фишинга;

– более высокая эффективность за счет отсутствия необходимости в выполнении запросов к провайдеру удостоверения личности грид-системы;

– данные пользователя хранятся в грид-среде в зашифрованном виде и находятся под управлением пользователя;

– нет риска компроментации злоумышленником провайдера удостоверения личности грид-системы, что позволило бы злоумышленнику выдать себя за легального пользователя либо похитить базу данных пользователей.

Достижение всех указанных преимуществ требует внесения изменений как в клиентское так и в серверное программное обеспечение, однако данная модель допускает поэтапное внедрение.

ДИНАМИЧЕСКАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В РЕАЛЬНОМ МАСШТАБЕ ВРЕМЕНИ

В.В. Анищенко, Ю.В. Земцов

Увеличение сложности корпоративных информационных систем приводит к росту степени риска нарушения информационной безопасности при их эксплуатации. Поэтому актуальной становится проблема разработки специализированных систем поддержки принятия решений (СППР), осуществляющих текущий мониторинг состояния контролируемых аппаратно-программных комплексов, и обеспечение лица, принимающего решения, необходимой информацией для предотвращения аварийных с точки зрения информационной безопасности ситуаций или минимизации наносимого ими ущерба.

Наиболее перспективен для этих целей класс динамических СППР, функционирующих в реальном масштабе времени. Основным отличием от традиционных статических экспертных и интеллектуальных систем является наличие динамической базы знаний, модифицируемой и корректируемой на основе внешних информационных потоков от системы датчиков, контролирующих основные параметры объекта. Динамические СППР на базе однопроцессорных платформ хорошо зарекомендовали себя лишь для решения узкоспециализированных задач безопасности в достаточно простых корпоративных информационных системах; это связано как с организацией последовательного логического вывода, так и с проблемой одновременного усвоения информации от большого числа датчиков. Потому применение параллельных суперкомпьютерных платформ для комплексных СППР сложных корпоративных информационных систем приобретает первоочередное значение.

Использование суперкомпьютеров кластерной архитектуры позволяет обеспечить многоуровневую параллелизацию процесса усвоения данных (как по отдельным каналам, так и по группам каналов, характеризующих подобные процессы). В докладе показано, что производительность как отдельных алгоритмов усвоения данных, так и СППР в целом на базе кластерных платформ по сравнению с их традиционными аналогами существенно выше.

ВЕРОЯТНОСТНАЯ МОДЕЛЬ ПЕРЕДАЧИ КЛЮЧЕВОЙ ИНФОРМАЦИИ В СИСТЕМЕ СО СЛУЧАЙНЫМ ПЕРЕКЛЮЧЕНИЕМ ПРИЕМО-ПЕРЕДАЮЩИХ БАЗИСОВ

В.Ф. Голиков, С.Г. Скобля

Одним из перспективных способов распределения криптографических ключей для симметричных криптосистем считается квантовая передача. Эффективность передачи криптографических ключей с помощью квантов света в настоящее время существенно зависит качества систем генерации, передачи и приема фотонов. Однако существенные резервы имеются и за счет оптимизации процедур формирования "сырого ключа" (ключа, содержащего ошибки) и устранения этих ошибок.

В докладе рассматривается гипотетическая модель передачи ключевой информации в системе со случайным переключением приемо-передающих базисов. Такая модель имитирует статистические процессы и является полезной для оценки эффективности передачи ключа. Постановка задачи следующая. Пусть имеется объект A которому необходимо передать некую двоичную последовательность K_j, где $j=\overline{1,n}$, n — длина последовательности, например, ключевую информацию, по открытому каналу связи объекту B. Злоумышленник C имеет возможность подключиться к этому каналу и перехватывать передаваемую информацию, анализировать ее и возвращать либо в неизменном виде, либо в искаженном обратно в канал связи. Будем считать, что передатчик объекта A генерирует физические сигналы, параметры которых зависят от того в каком состоянии (режиме) находится передатчик. Для управления состояниями передатчика A вырабатывается случайная последовательность чисел R_i, где i=1, 2. Пусть распределение вероятностей R_i — равномерное, т.е. каждый режим равновероятен P_i=0,5. Физический сигнал, сформированный в i-м режиме модулируется битами двоичной случайной последовательности (той последовательности, которую A должен передать B). По аналогии с квантовой технологией в i-й режим работы передатчика, в котором сформирован физический сигнал, переносящий "1" или "0", будем называть i-м базисом. Если базисы передатчика A и приемника B при передаче j-го бита совпадают, то он принимается правильно, если базисы противоположны, то независимо от передаваемого бита принимается либо "1", либо "0" с одинаковыми вероятностями. Будем считать, что злоумышленник C обладает техническими возможностями перехватывать передаваемые сигналы при этом, если базис C совпадает с базисом передатчика A, то передаваемый бит принимается C правильно, если базисы A и C противоположны, принятый бит равновероятно может оказаться равным "1" или "0". Принятый C бит (правильный или неправильный) возвращается в канал связи и достигает приемника B, который принимает его по описанному ранее алгоритму. При этом C может передавать возвращаемый бит в том же базисе, в котором он был принят им от A или в противоположном.

Для сформулированных исходных данных построен граф передачи K_j и получено выражение для вероятности правильной передачи K_j.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

С.Г. Скобля, В.Ф. Голиков

Существенными недостатками современных симметричных и асимметричных криптографических систем являются: 1) возможность ретроспективного взлома; 2) отличная от нуля вероятность обнаружения алгоритмов быстрого вычисления односторонних функций, используемых в асимметричных системах; 3) незащищенность

перед алгоритмами взлома, разработанными для квантовых компьютеров. И если алгоритмы Гровера (для взлома DES) и Шора (для факторизации), разработанные для несуществующих пока квантовых компьютеров, никак не сказываются на степени взломостойкости информации, защищенной с помощью упомянутых систем, то два первых недостатка заставляют работать над поиском альтернативных решений уже сегодня.

Одной из перспективных альтернатив является квантовая криптография, а более конкретно — квантовое распределение ключей. В этом направлении сейчас ведутся интенсивные исследования, уже получены практические результаты, разработаны первые промышленные установки. Однако, имея очевидные преимущества перед конкурентами, системы квантового распределения ключей на современном этапе развития имеют и существенные недостатки, важнейший из которых — низкая эффективность распределения ключевой информации, которая выражается, главным образом, в низкой скорости генерации ключа и относительно небольших максимальных расстояниях передачи.

Изучение существующих протоколов квантового распределения ключей и принципов функционирования установок, в которых они реализованы, анализ причин, ограничивающих эффективность передачи ключевой информации, позволяет сделать вывод о том, что повышение эффективности подобных систем возможно. Основными перспективными направлениями исследований в этой области видятся: 1) улучшение аппаратной части, включающее усовершенствование оборудования и материалов, используемых в установках, в особенности — источников и приемников фотонов, оптоволокна; 2) разработка новых более эффективных протоколов передачи и совершенствование существующих протоколов (и, в частности, методов формирования окончательного ключа из "сырого"). В докладе рассматриваются возможности второго направления.

СУЩНОСТЬ, ПРЕДМЕТ И КЛАССИФИКАЦИЯ ОБЪЕКТОВ СУДЕБНОЙ АППАРАТНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

И.В. Русаков, С.И. Цыбовский

При расследовании уголовных дел, связанных с мошенничеством и хищениями нередко возникает потребность в проведении криминалистических экспертиз на предмет внесения изменений в аппаратную часть компьютеризированных систем технического контроля и наблюдения, фискальных систем, систем автоматизированного управления. Для решения подобных задач в отношении аппаратной части компьютерных и компьютеризированных систем в процессуальной форме создан новый вид судебных экспертиз — судебная аппаратно-техническая экспертиза (далее САТЭ), относящаяся к судебной компьютерно-технической экспертизе.

Сущность судебной аппаратно-технической экспертизы заключается в проведении диагностического исследования технических (аппаратных) средств компьютерной системы, определении функциональных возможностей, фактического и начального состояния, технологии изготовления, эксплуатационных режимов и т.п. Предметом САТЭ являются имеющие отношение к правонарушению факты и обстоятельства, устанавливаемые на основе исследования закономерностей разработки, производства, функционирования, эксплуатации и ремонта аппаратно-технических средств компьютерных и компьютеризированных систем, а также их комплектующих, реализованных на основе микропроцессорного управления.

Систему объектов САТЭ составляют: класс аппаратных объектов, класс программных объектов и класс информационных объектов (данных). Объекты САТЭ (аппаратно-технические средства) включают следующие классы:

– персональные компьютеры;

– мобильные компьютеры (ноутбуки, карманные персональные компьютеры);

– устройства ввода-вывода и обмена информации (периферийные устройства и сетевые аппаратные средства);

– интегрированные системы (органайзеры, мобильные телефоны, GPS-системы контроля, навигации и позиционирования, ID-карты, смарт-карты, SIM-карты, банкоматы и т.п.);

– встроенные системы на основе микропроцессоров (микроконтроллеров) (иммобилайзеры, транспондеры, круиз-контроллеры и т.п.);

– бытовая техника и промышленное оборудование, управление которыми реализовано на основе микропроцессоров (микроконтроллеров);

– комплектующие всех указанных компонент (аппаратные блоки, датчики, платы расширения, микросхемы и т.п.).

ИНФОРМАЦИОННО-КОМПЬЮТЕРНАЯ ЭКСПЕРТИЗА (ДАННЫХ), НАПРАВЛЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Д.В. Липень, Д.В. Михейчик

Информационно-компьютерная экспертиза (данных) является ключевым видом судебной компьютерно-технической экспертизы, так как позволяет создать доказательственную базу путем решения диагностических и идентификационных задач, связанных с компьютерной информацией. Целью этого вида СКТЭ является поиск, обнаружение, восстановление, анализ и оценка информации на машинных носителях, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе. Исключительно на выводах подобной экспертизы стоится доказательная база при обвинении в совершении преступлений в области информационной безопасности.

Основными машинными носителями на сегодняшний день являются накопители на жестких магнитных дисках (винчестеры) или НЖМД. Поэтому в лаборатории судебных компьютерно-технических исследований НИИ КиСЭ Министерства юстиции Республики Беларусь ведется разработка методических рекомендаций по проведению криминалистического исследования НЖМД, разработка научно обоснованных подходов для криминалистического исследования имеющейся на них информации (в том числе и удаленной), разработка подходов к считыванию информации с технически неисправных НЖМД, разработка общей схемы проведения подобных исследований неповреждающими методами. Отдельное внимание уделяется формам представления информации и способам ее сокрытия.

Проведен анализ алгоритмов работы специализированных программ поиска информации "Encase Forensic Edition", "ILOOK Investigator", "Vogon International". Наиболее перспективным признан "Encase Forensic Edition", поскольку реализованная в нем хэш-функция "криминалистического образа" позволяет полностью исключить изменения данных недобросовестным следователем или экспертом. Более того, "Encase Forensic Edition" представляет собой "концепцию программной среды, адаптированной к продвинутому поиску информации" и позволяет "подключать" шаблоны и модули иных разработчиков ПО.

КОМПЛЕКСНАЯ ЭКСПЕРТИЗА ДОКУМЕНТОВ, НАПРАВЛЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Д.В. Липень

Информатизация государства и общества в области оптимизации документооборота является современным, адекватным к всевозрастающим

требованиям инструментом управления оборотом информации. Традиционный (бумажный) документооборот, не смотря на значительную модернизацию в последние годы, уже на сегодняшний день не справляется с возложенной на него задачей, особенно в сферах, требовательных к качеству информационного взаимодействия в режиме реального времени, таких как военное и банковское дело, торговля, логистика, работа исполнительных, силовых и контролирующих органов власти.

Поэтому в связи с подготовкой к переходу на электронный документооборот появилась потребность в более широкой трактовке понятия "документ" именно как "зафиксированная юридически значимая информатизация". В настоящее время нерукописные реквизиты документов на бумажных носителях на 90–95% нанесены с помощью знакопечатающих устройств (далее ЗПУ). Современные способы создания полиграфических и удостоверительных печатных форм также ориентированы на применение компьютерных технологий. Традиционные подходы и методы экспертизы документов оказались не применимы в современных условиях.

Лабораториями СТИД и СКТИ Института в 2003–2007 гг. разработаны и успешно внедрены в экспертную практику методики исследования цифровых панхроматических моделей (ЦПМ) документов и их реквизитов, полученных с помощью сканера. Как было доказано, подобные модели с высокой точностью сохраняют геометрические и цветовые характеристики исследуемых документов, обладая рядом полезных с криминалистической точки зрения свойств. При проведении исследований ЦПМ производится их обработка в растровом графическом редакторе "Adobe Photoshop", а математический анализ колористической информации осуществляется с помощью пакета системного анализа "MathLab".

На сегодняшний день ЦПМ применяются при решении идентификационных и диагностических задач при исследовании удостоверительных печатных форм и штампов, при диагностике допечаток текста, при диагностике компьютерных монтажей, при решении задачи пересекающихся штрихов, при установлении релевантности изображений.

Следует отметить, что на сегодняшний день криминалистические исследования документов с использованием ЦМП проводятся только в НИИ КиСЭ Министерства юстиции Республики Беларусь (ведется подготовка к обучению экспертов Украины и Литвы).

СПОСОБЫ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ КАРТ

М.Л. Данилкович

Интеллектуальные карты (смарт-карты) являются самым молодым и перспективным представителем многочисленного семейства идентификационных карт, широко используемых в разнообразных прикладных информационных системах. В связи с широким внедрением технологий с использованием смарт-карт актуальным становится вопрос устойчивости интеллектуальных карт к атакам на их информационную безопасность.

Различают два вида атак на интеллектуальные карты: пассивные (passive) атаки и активные (active) атаки.

Примерами пассивных атак могут служить атака по времени выполнения (timing attack) и атака по потребляемой мощности (SPA).

В качестве защиты от атак по времени выполнения можно использовать следующие методы: обеспечить выполнение модулем шифрования операций строго за одно и то же количество тактов процессора независимо от значений операндов и маскировать время выполнения операций. В качестве противодействия SPA предлагаются различные методы зашумления — аналогично атакам по времени выполнения.

Активные атаки подразумевают различные специфические воздействия на смарт-карту с целью нарушения ее нормального функционирования, в результате чего она может давать сбои в процессе своей работы. Независимо от вида воздействия на модуль шифрования, подобные атаки называются атаками на основе сбоев (fault attacks).

Заставить смарт-карту работать некорректно можно множеством различных способов. Наиболее эффективными воздействиями являются: изменение напряжения питания (spike attack), изменение тактовой частоты (glitch attack), высокоточное облучение (optical & radiation attacks), высокоточное наведение электромагнитного поля или локальный нагрев определенной области смарт-карты (electromagnetic & heating attacks) и внесение изменений в конструкцию смарт-карты.

К сожалению, какого-либо универсального средства защиты от активных атак на смарт-карты не существует. Однако, существенно усложнить проведение атак на основе сбоев можно следующими способами: внедрение детекторов различных воздействий, использование различного рода пассивного экранирования и различные виды дублирования вычислений со сравнением результатов.

Подобные методы в свою очередь приводят к удорожанию устройств и/или снижению их быстродействия и должны выбираться с учетом рисков нарушения безопасности смарт-карт.

КРИПТОГРАФИЧЕСКИЕ ПРОЦЕДУРЫ СОЗДАНИЯ И ВЕРИФИКАЦИИ ИДЕНТИФИКАТОРОВ ДОКУМЕНТОВ И ТОВАРОВ

В.Ю. Липень

В докладе автор анализирует различные методы и средства защиты бумажных документов от фальсификации и системы контроля за обращением документов. Отдельно рассматриваются методы защиты бланков строгой отчетности (полиграфия, спецкраски, голограммы, муаровые изображения и др.) и методы защиты контента (специальные реквизиты, шифрование, печать защитных данных, например, электронной цифровой подписи (ЭЦП) и открытого ключа в виде двумерного штрих-кода (ШК) и др.). Анализируются патенты и публикации, обосновывающие использование графической интерпретации ЭЦП в виде двумерного ШК. Рассматривается не очень успешный опыт создания и эксплуатации Единый Государственный автоматизированный системы (ЕГАИС), которая предназначена для компьютерного контроля изготовления и обращения алкогольной продукции в России. Анализируются аналогичные подходы к защите документов, предлагаемые в рассмотренных патентах.

Одним из выявленных недостатков подхода, реализованного в ЕГАИС, является необходимость размещения на этикетке товара графического образа ЭЦП и открытого ключа в виде двумерного ШК, что предполагает необходимость печати, оптического считывания и верификации оригинальных ШК (например, PDF-417), имеющих емкость более килобайта.

Еще в 2002 г. автором предлагался альтернативный подход к защите документов и этикеток подакцизных товаров. Для индивидуальной маркировки предлагается использовать уникальный идентификатор в виде линейного ШК, воспринимаемого обычным кассовым считывателем. Разработанные алгоритмы криптографических процедур создания и верификации многокомпонентного идентификатора предусматривают возможность как автономной, так и сетевой проверки его корректности. На основе использования результатов многократных сетевых проверок подобных уникальных идентификаторов обеспечивается возможность компьютерной реконструкции маршрута движения документов и партий товаров. Рассматривается возможность использования предлагаемого подхода для борьбы с неучитываемым

производством контрафактной продукции и преступлениями, совершаемыми с использованием фальсифицированных документов.

ИССЛЕДОВАНИЕ ГЕНЕРАЦИИ ПОМЕХ ЗАЩИТНЫМИ ПОКРЫТИЯМИ ПРИ МЕХАНИЧЕСКИХ ВОЗДЕЙСТВИЯХ

Г.В. Давыдов, В.Ю. Серенков

В настоящее время механизм генерации зарядов защитными покрытиями при их механическом нагружении мало изучен. Отсутствует связь между уровнями помех, габаритными параметрами изделий и температурой.

Для выяснения указанных зависимостей и связей, а также для определения уровня помех, генерируемых боле широким классом диэлектрических материалов были проведены экспериментальные исследования, цель которых заключалась в следующем:

– выявить механизм генерации зарядов защитными покрытиями при их механическом нагружении;

– определить факторы существенно влияющие на уровень генерируемых помех;

– определить уровни помех, генерируемых защитными покрытиями и несущими конструкциями РЭС.

Для экспериментальных исследований и выявления механизма генерации зарядов защитными покрытиями были изготовлены образцы из стеклотекстолита, гетинакса и ситалла.

Образцы крепились консольно на столе вибростенда. Токопроводящие участки подключались ко входу измерительного усилителя с высоким входным сопротивлением. Путем изменения частоты колебаний вибростенда производилась настройка на частоту резонансных изгибных колебаний образцы. Исследования проводились в широком диапазоне температур, который обеспечивался камерой тепла и холода.

В результате экспериментальных исследований уровней помех генерируемых несущими элементами конструкций РЭС установлено, что уровни помех не имеют существенной зависимости от расстояния между токопроводящими элементами. Уменьшение длины токопроводящих участков приводит к уменьшению уровня помех от 0,8 мВ до 0,1 мВ.

Исследования показывают, что материал образца, его структура, влажность и температура оказывают существенное влияние на уровень генерируемых помех.

Покрытия образцов защитными покрытиями на основе эпоксидных смол приводит к увеличению уровня помех на 25–30 %.

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ ДЛИТЕЛЬНОСТЕЙ СИНТАГМ В РЕЧЕВЫХ СИГНАЛАХ АРАБСКОГО ЯЗЫКА

Аль-Хатми Мохаммед Омар

Предложен алгоритм синтеза речеподобных сигналов (РПС) применительно к арабскому языку [1]. Эти сигналы целесообразно использовать в качестве специально организуемых акустических помех для защиты речевых сигналов (РС) от несанкционированного прослушивания и для тестирования речевых каналов связи.

Исходными данными для указанного алгоритма на сигнальном уровне являются статистические характеристики, в частности, — длительностей пауз между энергетически значимыми элементами РС, а также длительностей синтагм, фраз и фоноабзацев.

Проведенная экспериментальная оценка распределения вероятностей длительностей пауз в РС арабского языка показала, что это распределение имеет выраженный двухмодовый характер, со значениями мод близкими 0,5 с и 1 с.

Цифровые записи РС производились в специально оборудованном лабораторном помещении БГУИР, имеющем защиту от акустических шумов и шумов вибраций с остаточным их уровнем менее 40 дБ. Регистрация и анализ и обработка РС осуществлялись с помощью персонального компьютера. Для ввода РС в компьютер использовались микрофон типа М-101 и 16-разрядная звуковая плата. Частота дискретизации составляла 22 050 Гц.

Эти же записи использованы для анализа плотности распределения вероятностей длительностей синтагм. По результатам анализа, проведенного на ПЭВМ с помощью специально разработанной для этого рабочей программы, построена гистограмма этой плотности.

Статистические характеристики распределения длительностей синтагм имеют следующие значения: математическое ожидание 2,3 с; среднеквадратическое отклонение 1,46 с; коэффициент асимметрии 6,2; коэффициент эксцесса 28,2; медианное значение 1,8 с.

Полученные данные целесообразно использовать при решении задачи формирования РПС речи на арабском языке.

Литература

1. Аль-Хатми Мохаммед Омар, Воробьев В.И., Давыдов А.Г. Синтез речеподобных сигналов арабского языка // Докл. БГУИР. №6. 2007. С. 16–19.

2. Аль-Хатми Мохаммед Омар. Экспериментальная оценка распределения вероятностей длительностей пауз в речевых сигналах арабского языка // VI Междунар. науч.-практ. конф. "Управление информационными ресурсами", 24 апреля 2008 г., г. Минск (в печати).

АЛГОРИТМ ПРЕДВАРИТЕЛЬНОЙ ЦИФРОВОЙ ОБРАБОТКИ ПРИ ПЕРЕДАЧЕ ТЕЛЕВИЗИОННЫХ ИЗОБРАЖЕНИЙ

АРЕБИ МАЖЕД АЛИ

В работе рассматривается базовый алгоритм для аппаратуры цифровой обработки кодированных данных. Такая аппаратура входит в состав системы передачи телевизионных изображений, широко используемых в различных системах связи. Построение и принципы действия таких устройств должны быть согласованы с характером решаемых задач. К этим задачам на этапе предварительной обработки относятся: обнаружение объектов при наличии фона или шумов; преобразование изображений обнаруженных объектов с целью выделения наиболее существенных информативных признаков и подавления малоинформативных; кодирование результатов обработки и преобразования изображения.

В докладе представлен алгоритм цифровой обработки при передаче изображений, основанный на преобразованиях контурных данных, получаемых с помощью телевизионных камер. При этом наблюдаемый контур некоторого объекта рассматривается в виде цифрового массива, представляющего линию контура в параметрической форме. Массивы данных обрабатываются комплексным преобразованием Фурье. В результате на основании предложенной математической модели разработана программа в среде MathCAD, которая позволяет проводить моделирование цифровой обработки контуров объектов, обнаруженных с помощью цифровой камеры, а также осуществлять подавление фона с оптимизацией по критерию оценки контурности изображении.

Разработанный алгоритм проиллюстрирован двумя примерами его реализации в среде MathCAD. В первом примере контур был представлен массивом данных включающих M отсчетов по горизонтальной и вертикальной координатам, формирующим прямоугольный контур при различном его расположении, а также

при наличии шумов. Во втором примере рассматривается моделирование цифровой обработки сложного контура в виде силуэта корабля.

Проведенное моделирование показало высокую эффективность алгоритма по выделения контурных изображения для использования в устройствах предварительной обработки данных РПУ и РПрУ систем.

ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ОТ ВНУТРЕННИХ И ВНЕШНИХ ПОСЯГАТЕЛЬСТВ НА ИНФОРМАЦИЮ И РЕСУРСЫ

С.Э. АФАНАСЕНКО, С.Н. КАСАНИН

Технология построения виртуальных защищенных сетей, включающих в свой состав отдельные компьютеры (рабочие станции и сервера), находящиеся в локальной сети или удаленно подключаемые, фрагменты локальных сетей, локальные сети в целом. Путем построения распределенной системы персональных и межсетевых экранов, обеспечивающих также шифрование трафика в сети, автоматически для любых информационных систем и приложений обеспечивается конфиденциальность и достоверность информации, защита от сетевых атак, как из глобальных, так и из локальных сетей. Технология основана на использовании программных модулей, применяется на существующих сетях и не требует специального оборудования. Одновременно обеспечивается поддержка инфрастуктуры для использования электронной цифровой подписи, организация виртуальных каналов для безопасного подключения отдельных станций локальной сети к открытым ресурсам Интернет, защита конфиденциальных данных на дисках при таких подключениях.

ПРОГРАММНЫЙ МОДУЛЬ АНАЛИЗА ФАЗОВЫХ СООТНОШЕНИЙ

Ф.В. БОНДАРЕНКО

Программный модуль (ПМ) для анализа фазовых соотношений между основным тоном и обертонами гласных звуков речи актуален для более глубокого проникновения в повседневную жизнь и миниатюризации цифровых систем. Данный ПМ призван увеличить точность распознавания различных дикторов.

Новый ПМ рассчитан на разработчиков цифровых устройств и программных пакетов, дает возможность выделять дополнительные информационные признаки в человеческой речи.

Процесс разработки ПМ предусматривает проведение всех стадий проектирования (техническое задание, эскизный проект, технический проект, рабочий проект, внедрение) и относится к 3-й группе сложности. По степени новизны ПМ относится к группе "В " с коэффициентом 0,7.

Разработан и создан эффективный ПМ для анализа фазовых соотношений между основным тоном и обертонами гласных звуков речи. Модуль ориентирован на повышение результатов распознавания человеческой речи.

ВОЗМОЖНОСТИ РАБОТЫ С DICOM ФАЙЛАМИ В СРЕДЕ МАТРИЧНОГО МОДЕЛИРОВАНИЯ MATLAB

А.В. Смирнов, В.М. Бондарик

DICOM — формат хранения и передачи медицинской графической информации. В формате DICOM 3.0 могут храниться данные, полученные в основном на томографах и рентгеновских аппаратах. Изображение в данном формате, обычно сжимается JPEG, Huffman JPEG или JPEG-LS схемами сжатия. Наряду с изображением в состав файла входит служебная информация: имя пациента, дата проведения исследования, вид исследования, вид оборудования и т.д.

MATLAB (Image Processing Toolbox — IPT) содержит 6 команд для работы с DICOM файлами. Наиболее важные команды с практической точки зрения: чтение и запись DICOM изображений — dicomread и dicomwrite соответственно, чтение метаданных из файла — dicominfo.

Команда dicomread считывает видеоинформацию из DICOM-файла — массив полутонового изображения X с размерностью M×N или массив цветного изображения X с размерностью M×N×Z, где параметр Z описывает градацию цвета. Многомерные изображения компьютерных томаграмм могут представляться четырехмерным массивом.

Измененные данные можно записать с помощью функции dicomwrite, которая производит запись бинарного полутонового или цветного изображения X в файл формата DICOM. С помощью параметров param записываются различные атрибуты и опции DICOM–файла.

Для просмотра служебной информации предназначена функция dicominfo, которая формирует метаданные, полученные из DICOM-файла.

MATLAB обладает широким инструментарием позволяющим применять цифровую фильтрацию к изображению сохраненному в формате DICOM, что упрощает описание изображения медицинским работникам, позволяет детализировать малозаметные патологии.

СЕТЕВОЕ МОШЕННИЧЕСТВО: СОЗДАНИЕ КОПИЙ ИНТЕРНЕТ-МАГАЗИНОВ

Д.В. Буко

Мошенничество — получение денег путем обмана. Под сетевым мошенничеством будем понимать мошенничество с использованием электронных систем и сетей. Также введем понятия "кардинга" — мошенничества с использованием кредитных карт и "фрауда" — незаконной операции с использованием чужой кредитной карты. В качестве электронной системы будем рассматривать интернет-магазин, в качестве сети — интернет.

Расчет с покупателем интернет-магазина по кредитной карте удаленно требует от покупателя следующую информацию — номер карты, срок ее годности, имя и контактную информацию владельца, а также специальный код (либо коды) CVV, CVV2, CVN.

Цель мошенника, таким образом, получить эту информацию. Он может использовать различные методы — взломы интернет-систем и получения доступа к базам данных магазинов или банков, обман, создание несуществующих сетевых сервисов или копирование существующих и т.д. Далее более подробно рассматривается последний метод.

Мошенник выбирает интернет-магазин, копирует его дизайн, регистрирует похожий адрес и, по возможности его рекламирует. Пользователь, попадает на такой сайт, выбирает существующий товар и производит его заказ, указывая при этом всю

необходимую для удаленной оплаты информацию. Копия магазина, созданная мошенником, отправляет эту информацию в реальный магазин, а копию этой информации — мошеннику. Так, покупатель получит товар от реального магазина, а мошенник — всю требуемую ему информацию о покупателе.

ВСТРОЕННЫЕ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ДЕЛОПРОИЗВОДСТВА И ДОКУМЕНТООБОРОТА

В.Л. Бусько, А.Л. Гончаревич

В докладе рассмотрены задачи решаемые встроенными подсистемами безопасности различных информационных автоматизированных систем делопроизводства и документооборота (ЕВФРАТ, ДЕЛО, LanDocs, Гран-Док, БОСС-Референт, ДЕЛОПРОИЗВОДСТВО и др.), механизмы реализации задач и взаимодействие подсистемы безопасности с другими подсистемами делопроизводства и документооборота.

Проведен обзор преступлений за 2006–2007 гг. в информационных процессах организаций и мер по их предотвращению, приведены тенденции и прогнозы на 2008 г.

Предлагается функциональное расширение подсистемы безопасности в части разграничения полномочий доступа к рабочей информации по вертикали и горизонтали структуры организации в системах делопроизводства и документооборота. Данное функциональное решение позволит сократить вероятность утечки конфиденциальной информации не только в случае действий инсайдеров, но и в случае утечки информации связанной с беспечностью персонала, а значит повысить общий уровень безопасности системы делопроизводства и документооборота в целом.

ЗАЩИТА ОТ ИСКАЖЕНИЙ СОПРЯЖЕННОЙ СОСТАВЛЯЮЩЕЙ АНАЛИТИЧЕСКОГО СИГНАЛА

В.В. Величковский, Е.Н. Шнейдеров

Сопряженная составляющая $\hat{x}(t)$ аналитического сигнала $z(t) = x(t) + j\,\hat{x}(t)$ является интегральным преобразованием Гильберта функции $x(t)$. В реальных условиях функция $x(t)$ задается на конечном промежутке длиною T в N дискретных точках оси времени. Оба названных фактора приводят к искажению сопряженной составляющей.

Влияние дискретного задания функции $x(t)$ в виде $x(n)$ можно минимизировать, сузив класс рассматриваемых функций до полигармонических. Тогда замена непрерывной функции дискретной по теореме Котельникова может быть произведена без потери информации. Вычисление сопряженной составляющей $\hat{x}(n)$ на концах отрезка $[0,T]$ выполняется с большой ошибкой из-за недостатка информации о функции $x(n)$ вблизи $t = 0$ и $t = T$. Повысить точность вычисления можно путем экстраполяции $x(n)$ влево и вправо от точек $t = 0$ и $t = T$ соответственно. Рассмотрены два метода экстраполяции функции $x(n)$ влево (экстраполяция вправо от $t = T$ осуществляется аналогично). Первый базируется на представлении $x(n)$ по формуле Тейлора в окрестности точки $t = 0$. Производные заменяются конечными разностями соответствующих порядков. В основу второго метода положен ряд Котельникова, дающий возможность получить значение функции $x(t)$ в любой момент времени t по его дискретным значениям. Для реализации этого метода число дискретных значений на отрезке должно существенно превосходить минимально необходимое по теореме

Котельникова, и за счет этого возможна экстраполяция $x(n)$ влево. Проведенное моделирование на ЭВМ показало, что оба метода существенно снижают искажения сопряженного сигнала $\hat{x}(t)$ на концах интервала $[0,T]$.

АНАЛИЗ ЗАЩИЩЕННОСТИ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ ПО ТЕХНОЛОГИИ xDSL ОТ ПЕРЕХОДНЫХ ВЛИЯНИЙ

М.В. ВЛАСЕНКО, В.И. КИРИЛЛОВ

На современном этапе цифровизации систем передачи большую роль играет семейство технологий xDSL, которые применяются для решения проблемы "последней мили". При этом кроме проблемы "последней мили" данные технологии могут решить целый ряд других задач, связанных с модернизацией первичных сетей связи в Республике Беларусь, в частности, повысить качество связи и эффективность систем передачи.

В докладе проведен анализ вариантов построения цифровых систем передачи (ЦСП) по технологии xDSL. Показано, что проблема увеличения длины регенерационного участка ЦСП является актуальной для всех рассмотренных вариантов систем передачи. Раскрыты основные недостатки ЦСП старого парка (типа ИКМ-30), показана целесообразность и эффективность замены их на ЦСП по технологии xDSL. Однако в современной научно-технической литературе отсутствуют универсальные методики расчета основных параметров ЦСП по технологии xDSL.

Авторами предложена методика анализа защищенности ЦСП по технологии xDSL от переходных влияний. Приведены основные результаты анализа по этому критерию различных вариантов построения ЦСП.

АНАЛИЗ ЭФФЕКТИВНОСТИ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ, ИСПОЛЬЗУЮЩИХ РАЗЛИЧНЫЕ ВИДЫ МОДУЛЯЦИИ ЛИНЕЙНЫХ СИГНАЛОВ

М.В. ВЛАСЕНКО, В.И. КИРИЛЛОВ

Наряду с однотипной модуляцией линейного сигнала в пределах одной цифровой системы передачи (ЦСП) возможно применение различных видов модуляции. Это может существенно снизить затраты на основное оборудование ЦСП, поскольку известно, что использование многоуровневой АИМ-модуляции линейного сигнала на "низкочастотном" направлении в сравнении с CAP(QAM)-модуляцией уменьшает стоимость ЦСП в целом с сохранением достоинств технологии xDSL. Однако в литературе отсутствует методика анализа эффективности таких ЦСП.

Авторами предложена методика оценки эффективности ЦСП с различными видами модуляции линейного сигнала. В докладе приведены результаты математического моделирования прохождения сигнала и помех в тракте ЦСП, использующей многоуровневые АИМ и CAP(QAM) линейные сигналы. Обоснован критерий оценки эффективности таких ЦСП – обеспечением максимальной длины регенерационного участка при заданной достоверности передачи информации. С использованием данного критерия произведен анализ эффективности ЦСП. При анализе учитывались: защищенность ЦСП от собственных шумов, защищенность от переходных влияний на ближнем конце, защищенность от переходных влияний на дальнем конце. При этом принималось, что существует несколько вариантов построения таких ЦСП с различными видами модуляции.

ПРОБЛЕМЫ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ ОТ ПОМЕХ НЕЛИНЕЙНОГО ПРОИСХОЖДЕНИЯ

К.В. Дука, В.И. Кириллов, А.А. Пилюшко

На фоне решения глобальных вопросов модернизации сетей связи, может создаться впечатление, что цифровизация снимает целый ряд проблем, связанных с повышением качества связи и эффективности систем передачи. Однако, даже при построении цифровых систем объективно сохраняется необходимость борьбы с помехами нелинейного происхождения.

В докладе проведен подробный анализ различных типов современных цифровых систем передачи (волоконно-оптических, радио и радиорелейных, в том числе спутниковых) на предмет их защищенности от помех нелинейного происхождения. Показано, что проблема линеаризации трактов прохождения сигналов является актуальной для всех рассмотренных типов систем передачи. При этом особо отмечено, что нелинейности, с которыми приходится иметь дело, носят весьма сложный (например, кусочно-нели-нейный) характер. Это обстоятельство сильно затрудняет анализ помех нелинейного происхождения и далеко не всегда позволяет воспользоваться на практике известными (традиционными) методами их расчета.

Авторами предложен комплексный метод спектрального анализа нелинейных преобразователей с произвольной мгновенной динамической характеристикой, который позволяет с высокой степенью точности определить спектральный состав сигнала на выходе преобразователя даже при условии подачи на его вход полигармонического воздействия, в том числе и модулированных колебаний.

МНОГОСЛОЙНЫЕ ПОГЛОТИТЕЛИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ ДЛЯ СНИЖЕНИЯ ЗАМЕТНОСТИ НАЗЕМНЫХ ОБЪЕКТОВ

Т.В. Борботько

В настоящее время широкое развитие получили средства дистанционного зондирования Земли, которые в виду их технических характеристик позволяют с высокой разрешающей способностью вести наблюдение земной поверхности с воздушных и космических носителей. Особое внимание в мире уделяется их применению в вооруженных силах, что позволят обеспечить процесс наблюдения за наземными объектами, расположенными на значительных расстояниях от центров сбора такой информации.

Противодействие данным средствам может быть реализовано путем скрытия наземных объектов с использованием маскировочных комплектов и покрытий. Эффективность скрытия в данном случае будет определяться в первую очередь, техническими характеристиками материалов, входящих в состав маскировочных комплектов и покрытий.

Современные средства дистанционного зондирования широко используют частотный и спектральный ресурс, и работают в видимом, ближнем, среднем и дальнем инфракрасном, а также в радиочастотном диапазонах. В связи с чем, основное требование к современным маскировочным материалам — широкодиапазонность. Существующие методы создания поглотителей электромагнитного излучения в настоящее время не позволяют синтезировать однослойные материалы, эффективно поглощающие электромагнитную энергию в указанных диапазонах длин волн. В связи, с чем возникает необходимость разработки поглотителей электромагнитного излучения многослойной конструкции.

Использование многослойных конструкций поглотителей электромагнитного излучения позволяет не только расширить их рабочий диапазон длин волн, но и обеспечить создание маскировочных материалов с управляемыми свойствами за счет варьирования физических параметров каждого слоя конструкции в отдельности.

ПОВЫШЕНИЕ РАЗВЕДЗАЩИЩЕННОСТИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ

Е.В. МАШКИН, Д.В. ЗАНЕВСКИЙ

Скрытность радиоэлектронных средств (РЭС) определяется энергетической, пространственной, частотно-временной доступностью средствам разведки.

В связи с этим, методы повышения разведзащищенности РЭС разделяется на: энергетические, временные, пространственные и сигнальные. Эффективность применения данных методов зависит от особенностей построения радиолиний, диапазонов рабочих волн и т.д.

Снижение энергетической и временной доступности РЭС достигается использованием режима пакетной передачи информации в радиолиниях КВ, УКВ диапазона и сетях спутниковой связи со случайным множественным доступом с временным и кодовым разделением сигналов.

В докладе рассматривается метод повышения разведзащищенности радиолиний КВ-УКВ диапазонов при использовании метода накопления информации и пакетной ее передачи в режимах быстродействия и сверхбыстродействия.

На основе предложенного метода рассматриваются варианты повышения временной защищенности РЭС. В частности показано, что временная защищенность РЭС за счет использования режима пакетной передачи информации с одновременным изменением параметров используемых радиосигналов по псевдослучайному закону со скоростью на порядок превышающей скорость их оценки исключает возможность обработки сигналов РЭС средствами радиоразведки.

PROTECTING TECHNIQUES AGAINST CROSS-SITE SCRIPTING ATTACKS

D. VOLODKO

Nowadays, many web sites make extensive use of client side scripts to enhance user experience. Unfortunately, this trend has also increased the popularity and frequency of cross-site scripting (CSS for short, but more often abbreviated as XSS) attacks. Cross-site scripting is an attack against web application in which scripting code is injected in to the output of an application, sent to a user browser, executed with the browser permissions and used to transfer sensitive data to a third party (i.e the attacker).

XSS protecting techniques could be divided in to client side or server side by deployment methods and dynamic or static by the type of analysis used. Dynamic server side protection example is Perl's taint mode when the flow of tainted values is tracked within the Perl interpreter [1]. Static analysis proposes to use flow-sensitive, inter-procedural and context-sensitive dataflow analysis to discover vulnerable points in a program. In addition, alias and literal analysis were employed to improve the correctness and precision of the results [2].

Client-side protection introduces an application level firewall that analyzes browsed HTML pages for hyperlinks that might lead to the leakage of sensitive data. Suspicious requests are blocked based on the analysis and generated on-the-fly rules [3]. Client-side methods of performing an in-depth and precise analysis of how sensitive values are propagated inside the user's browser. Using a combination of dynamic and static analyses, they can efficiently identify implicit information flows that purely dynamic approaches cannot identify.

XSS vulnerabilities are being discovered and disclosed at an alarming rate. XSS attacks are generally simple, but difficult to prevent because of the high flexibility that HTML encoding schemes provide to the attacker to pass through server-side/client-side input filters and there is a growing need for automated vulnerability detection in Web application development.

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

О.А. Вольская

На современном этапе на компьютерах, оснащенных новейшим программным обеспечением, процесс аутентификации сложен и используются длинные, путаные пароли и за системами следят самые квалифицированные администраторы — все равно остаются уязвимые места, т. к. человек, как правило, самое слабое звено в системе защиты.

Возможно, именно поэтому достаточно часто злоумышленники используют метод социального инжиниринга, основанный на использовании слабостей человеческого фактора. Целью этого метода является кража информации.

Таким образом, злоумышленник должен неплохо разбираться в психологии.

Выделяют три стадии подготовки такого рода атаки:

1. Определение точной цели, определение местоположения конечной цели. На данном этапе злоумышленник сначала пытается четко определить, за какого рода информацией он охотится, ведь если это ясно, то операция производится быстро: путем введения в заблуждение жертвы получается root и копируется необходимая информация;

2. Сбор информации об объекте обработки - это наиболее важный этап, во время которого похититель информации собирает сведения о характере жертвы, ее предпочтениях, привычках и уязвимых местах, чтобы свести время для получения информации к минимуму;

3. Разработка плана действий, моральная подготовка/тренировка. На данной ступени проводится просто колоссальная работа в области психологии: буквально каждое слово сопоставляется с психологической моделью изученной жертвы, необходимо просчитывать каждое слово, в зависимости от объекта, ведь люди разные и реакция на одно и то же слово у каждого разная.

Таким образом, следует обратить серьезное внимание на сложившуюся ситуацию и вести разработку систем защиты с учетом всего вышеперечисленного, а также следует соблюдать элементарные правила безопасности. Ведь, как известно, любую проблему легче предотвратить, чем потом бороться с нежелательными последствиями.

ИССЛЕДОВАНИЕ ТАНГЕНСА УГЛА ДИЭЛЕКТРИЧЕСКИХ ПОТЕРЬ В ПОЛИМЕРНЫХ ПОКРЫТИЯХ

Г.В. Давыдов, В.Ю. Серенков

Известно, что тангенс диэлектрических потерь с увеличением содержания влаги в полимерном покрытии в большинстве случаев увеличивается почти пропорционально количеству поглощенной влаги, что объясняется в основном ростом тока проводимости в увлажненном покрытии. Для каждого материала при увлажнении рост тока проводимости происходит по -разному, поэтому значения тангенса угла диэлектрических потерь для разных покрытий даже при одинаковом водо- и влагопоглощении будут разными.

При экспериментальном определении значений тангенса угла диэлектрических потерь для полимерных покрытий измерения проводились на частоте 1000 Гц, при этом измерялся тангенс угла диэлектрических потерь не отдельной пленки лака, а полимерного покрытия, нанесенного на стеклотекстолитовую плату толщиной 1,5 мм с обеих сторон в один или несколько слоев.

Насыщение влагой полимерных покрытий производилось при влажности воздуха 98 % и температуре 40 С. Результаты измерений отражены в таблице.

Зависимость тангенса угла диэлектрических потерь полимерных покрытий от увлажнения

Полимерное покрытие	Тангенс угла диэлектрических потерь до увлажнения	Тангенс угла диэлектрических потерь после увлажнения	Длительность увлажнения, ч	Количество слоев покрытия с одной стороны
Лак УР-231	0,0015	0,0080	75	1
Лак ЭП-730	0,0010	0,0020	75	1
Лак ЭП-9114	0,0020	0,0040	75	1
Лак УР-231	0,0030	0,0020	300	3
Лак ЭП-730	0,0015	0,0100	300	3

МЕТОД ОЦЕНКИ ФОРМАНТНОЙ РАЗБОРЧИВОСТИ РЕЧИ ПРИ ИСПОЛЬЗОВАНИИ ЗАЩИТНОГО ЗАШУМЛЕНИЯ

Г.В. Давыдов, Ю.В. Шамгин

Объективная количественная оценка разборчивости речи (РР) является необходимым условием для обеспечения защиты речевой информации (РИ), передаваемой речевыми сигналами (РС).

Существующие инструментальные и расчетные методы оценки РР в основном ориентированы для восприятия речи "на слух", когда требуется обеспечить высокий уровень РР. Для случая, когда необходимо обеспечить защиту РИ, оценка РР "на слух" становится недостоверной, или попросту невозможной. В этом случае единственно возможными становятся инструментальные методы РР, учитывающие динамический диапазон РС и уровень спектра помех, оставшийся после проведения операции шумоочистки речи. Последние методы в настоящее время не узаконены и требуют экспериментального обоснования для своего надежного использования.

В качестве инструментального нами использовался формантный метод РР. Под формантами понимаются максимумы спектра РС. Разборчивость формант определяется законами распределения формант по частотному и динамическому диапазонам речи.

Для определения динамического диапазона РС мы определяли среднеквадратическое отклонение (СКО) этого сигнала и СКО сопутствующего шума, измеренного между произносимыми словами. Далее определяя ширину частотного диапазона речи, ограниченного шумами, оценивали величину формантной разборчивости РС.

Таким образом, величина формантной разборчивости в условиях защитного зашумления с достаточной для практики степенью точности определялась произведением ширины частотного диапазона (в герцах) и средней величины эффективного динамического диапазона сигналов речи (в децибелах). При необходимости величина формантной РР могла быть представлена величиной словесной РР.

Рассмотренный метод позволял проводить повторяемые оценки РР величиной в единицы процентов, что недостижимо для других методов.

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ЭНЕРГЕТИЧЕСКОЙ И СТРУКТУРНОЙ СКРЫТНОСТИ

Н.А. Деев

Рассматриваются методы защиты информации, основанные на сокрытии самого факта существования секретной информации, а также средства реализации этих методов в виде системы передачи двоичных сообщений с фазовой манипуляцией сигнала и псевдослучайной перестройкой рабочей частоты. В качестве контейнерной составляющей в данном случае служат узкополосные сигналы, а скрываемые данные передаются на фоне сигнала распределенные по диапазону, модулированные с помощью межсимвольной ППРЧ. Для передачи данных предлагается использовать фазовую манипуляцию, что затрудняет процесс перехвата за счет расширения полосы частот сигнала, более чем это необходимо для передачи реальной информации и повышает помехоустойчивость приема на 3 дБ по сравнению с частотной манипуляцией. При точном воспроизведении псевдослучайной импульсной последовательности в наибольшей степени удается осуществить подавление контейнерной составляющей. В случае, когда действует сумма сигналов контейнерной составляющей и скрываемых данных с различными спектрами, необходимо выделять из смеси каждую из них, оценивать, а затем вычитать из действующей смеси. Линейные фильтры для выделения сигналов контейнерной составляющей и скрываемых данных являются неэффективными для построения компенсаторов, поскольку при подавлении контейнерной составляющей подавляется и часть спектральных составляющих широкополосного сигнала скрываемых данных. Поэтому предлагается использовать нелинейные методы выделения и оценивания (фильтрации) параметров сигнала контейнерной составляющей основанные на сочетании без инерционного нелинейного преобразования с линейной фильтрацией. Коммутация адаптивных компенсаторов контейнерных составляющих в каналах приема осуществляется в соответствии с синхронизированной ПСП и за счет этого обеспечивается обнаружение и эффективная оценка параметров узкополосных сигналов контейнерной составляющей с последующей компенсацией.

ТРАНСИВЕР ДЛЯ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ ПО НИЗКОВОЛЬТНЫМ СЕТЯМ ПЕРЕМЕННОГО ТОКА

И.Ю. Малевич, Н.А. Деев, М.А. Катков

Промышленная сеть представляет очевидную альтернативу различным проводным и беспроводным низкоинформационным каналам передачи данных в системах телеметрии, удаленного управления, оповещения и т.п. Однако высокий уровень помех в линиях электропитания существенно ограничивает применение их в качестве трансляционных систем. Поэтому использование промышленной сети переменного тока 230 В в качестве информационного канала требует разработки устройств с повышенной защищенностью передаваемой информации.

Функциональная схема трансивера состоит из модулей приемника и передатчика, соединенных посредством канала передачи данных на основе промышленной сети электропитания 230 В.

Приемный тракт трансивера выполнен по классической схеме супергетеродинного РПУ с низкой промежуточной частотой и цифровым демодулятором, реализующим неко-герентную обработку сигнала. Принцип работы демодулятора основан на корреляцион-ной обработке принятого сигнала и его образа, задержанного на половину периода. Это обеспечивает эффективное выделение фазоманипулированного сигнала на фоне интенсивных сетевых помех. Передающий

тракт трансивера использует ключевой выходной каскад, управляемый от микроконтроллера.

В реализованной конструкции в качестве устройства цифровой обработки сигнала использован компьютер со звуковой картой. Программное обеспечение выполнено в среде Delphi 7.

Натурные испытания трансивера в сетях переменного тока показали высокую защищенность передаваемой информации от интенсивных мультипликативных помех.

КЛАССИФИКАЦИЯ УЯЗВИМОСТЕЙ СЦЕНАРИЕВ НА ЯЗЫКЕ PHP

Д.А. Дука, А.Н. Мацкевич

Современные версии PHP позволяет создавать изображения, PDF-файлы, флэш-ролики, в него включена поддержка большого числа современных баз данных, встроены функции для работы с текстовыми данными любых форматов, включая XML, и функции для работы с файловой системой. Он поддерживает взаимодействие с различными сервисами посредством соответствующих протоколов, таких как протокол управления доступом к директориям LDAP, протокол работы с сетевым оборудованием SNMP, протоколы передачи сообщений IMAP, NNTP и POP3, протокол передачи гипертекста HTTP и т.д. Так же включена поддержка объектов Java и возможность их использования в качестве объектов PHP.

Языки описания сценариев, такие как Perl, Python, Rexx, Tcl, PHP, ASP и языки оболочек UNIX, предполагают стиль программирования, весьма отличный от характерного для языков системного уровня. Они предназначаются не для написания приложения с нуля, а для комбинирования компонентов, набор которых создается заранее при помощи других языков. С появлением этих языков программирования возникли и новые возможности по взлому систем, в которых они используются.

Предлагается следующая классификация уязвимостей сценариев на языке PHP:

– неправильная установка интерпретатора PHP;

– неправильная настройка интерпретатора PHP (опции Register_globals, Magic Quotes и т.д.);

– некорректное использование конструкций языка PHP (Fopen, Include, Require и т.д);

– переполнение памяти в следствии отсутствия деструкторов в классах;

– неправильная работа с сессиями и COOKIE;

– вывод критичных (с точки зрения безопасности) сообщений об ошибках;

– компрометация исходного кода при выходе из строя WEB сервера;

– выполнение системных вызовов из PHP сценариев;

– использования сценариев на PHP в качестве прокси-сервера;

– некачественная фильтрация входных данных пришедших от пользователей;

– загрузка вредоносного кода под видом картинок и другой информации.

Большинство успешных атак основывается на коде, написанном без учета соответствующих требований безопасности. В частности открытые проекты постоянно сообщают о найденных новых ошибках в их коде.

Поэтому необходимо учитывать особенности языков программирования с точки зрения классификации уязвимостей и мер защиты информации.

Литература

1. Котеров Д.В., Костарев А.Ф. PHP 5. Наиболее полное руководство. 2007.
2. Фленов М.Е. PHP глазами хакера. СПб., 2005.

УНИВЕРСАЛЬНЫЕ ОТЛАДЧИКИ ЯЗЫКА PHP

Д.А. Дука

Отла□дка — этап разработки компьютерной программы, на котором обнаруживают, локализуют и устраняют ошибки. Есть различные подходы и средства отладки; в качестве основного средства используются отладчики.

Отладчики для интерпретируемых языков, таких как PHP, могут использоваться с целью сохранения и отображения значения глобальных переменных, используемых в сценариях, отображения истории подключаемых файлов, систематизации сообщений об ошибках выполнения сценария, подсчета времени выполнения запросов к базам данных и определенных участков кода.

В отличие от системных языков программирования отладка сценариев на языке PHP не является тривиальной задачей, которой она может показаться на первый взгляд. Важность наличия при разборе чужого кода такого отладчика трудно переоценить. Объектный стиль программирования внес свои коррективы в процесс программирования и времена, когда сценарии сайтов состояли из нескольких файлов уже далеко в прошлом. Для сценариев не подходят отладчики, написанные для продуктов на языках системного уровня, поэтому необходимо создавать специальные продукты для этих целей.

Основные требования к отладчикам сценариев, написанных на PHP, следует выделить следующие:

– удобный пользовательский интерфейс;

– настройка отладчика и возможность интеграции с проверяемыми сценариями;

– удобное отображение отладочной информации и ее классификация по категориям;

– возможность правильного отображения типов переменных, классов и их методов;

– возможность отображать исходный код сценариев.

Такие отладчики могут использоваться при проверке сценариев на недекларированные возможности в специализированных лабораториях.

Пример такого отладчика, созданного на кафедре защиты информации, доступен для скачивания на сайте www.sec-it.ru.

Литература

1. Котеров Д.В., Костарев А.Ф. PHP 5. Наиболее полное руководство. 2007.
2. Фленов М.Е. PHP глазами хакера. СПб., 2005.

ЗАЩИТА КОНТРОЛЛЕРА СИСТЕМЫ ПЕРЕМЕЩЕНИЙ НА ЛШД ОТ ВЫПОЛНЕНИЯ НЕКОРРЕКТНЫХ КОМАНД ПРИ ДИСТАНЦИОННОМ УПРАВЛЕНИИ

Е.А. Жучков, И.В. Дайняк

Объектом исследования является аппаратно-программный комплекс, позволяющий через локальную компьютерную сеть дистанционно задавать перемещения и программировать траектории движения системы перемещений на базе ЛШД. Комплекс был разработан в учебно-научной лаборатории "Математическое моделирование технических систем и информационные технологии" (ММТСиИТ) БГУИР и включает: прецизионную систему перемещений, контроллер управления, ЭВМ локального управления и ЭВМ дистанционного управления.

Основными проблемами технической защиты аппаратно-программного комплекса являются следующие:

– предотвращение выполнения некорректных команд, которые могут привести к выходу из строя контроллера управления;

– ограничение рабочего поля перемещений, при выходе за пределы которого могут быть повреждены исполнительные элементы системы перемещений;

– обеспечение дистанционного управления только одним удаленным оператором в многопользовательском режиме.

Для решения вышеперечисленных задач в разработанном программном обеспечении комплекса в составе программы локального управления и программы дистанционного управления предусмотрено следующее:

– для программирования перемещений используется промежуточный набор команд на языке высокого уровня, который минимально достаточен, чтобы задавать позицию, скорость и ускорение перемещений;

– ограничена функциональность программы дистанционного управления в пользу удобства программирования траектории, которое осуществляется визуально. После визуального задания траектории осуществляется синтез программы движения на промежуточном языке;

– обязательная проверка выхода исполнительного элемента за пределы рабочего поля, которое определяется параметрами системы перемещений, подключенной к ЭВМ локального управления;

– трансляция программы движения на промежуточном языке осуществляется программой локального управления в программу на языке активного контроллера с автоматической проверкой синтаксиса и передаваемых данных.

Таким образом, разработанное программное обеспечение аппаратно-программного комплекса для дистанционного управления системой перемещений на базе ЛШД позволяет предупредить ошибочные действия оператора и выход оборудования из строя.

СТЕГАНОГРАФИЯ КАК ОДИН ИЗ МЕТОДОВ ЗАЩИТЫ АВТОРСКИХ ПРАВ И ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ ЦИФРОВОЙ ИНФОРМАЦИИ

Е.О. Конопельченко

Сегодня информация стала основным производственным ресурсом и основным товаром в современном обществе. Следствием развития информационных сетей стала доступность информации, ее избирательность, вследствие этого возникла острая необходимость защиты информации.

Первоочередной задачей защиты является обеспечение конфиденциальности информации при ее передачи в компьютерных сетях, в том числе по каналам передачи данных общего пользования. Современным решением этой задачи является применение стеганографической защиты информации.

Методы стеганографии позволяют не только скрытно передавать данные, но и решать задачи помехоустойчивой аутентификации, защиты информации от несанкционированного копирования, отслеживания распространения информации по сетям связи, поиска информации в мультимедийных базах данных. Одним из направлений цифровой стеганографии является встраивание цифровых водяных знаков (ЦВЗ) (watermarking).

Наиболее действенным способом является простановка авторского копирайта непосредственно на изображении. Задачу встраивания и выделения сообщений из другой информации выполняет стегосистема.

Данные, содержащие скрытое сообщение, могут подвергаться преднамеренным атакам или случайным помехам. В стегосистеме происходит объединение двух типов информации так, чтобы они могли быть различимы двумя принципиально разными детекторами. В качестве одного из детекторов выступает система выделенияцифрового водяного знака, в качестве другого — человек.

В большинстве стегосистем для внедрения и выделения цифровых водяных знаков используется ключ. Ключ может быть предназначен для узкого круга лиц или же быть общедоступным.

МЕТОДИКА ВЫЯВЛЕНИЯ ПРИЗНАКОВ ВРЕДОНОСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ПОМОЩЬЮ ВИРТУАЛЬНОЙ МАШИНЫ

А.Э. Ивашков

Технология виртуальных машин позволяет запускать на одном компьютере несколько различных операционных систем одновременно. При работе с дополнительной, "гостевей" операционной системой исследователь не испытывает никаких затруднений в использовании ее возможностей, то есть происходит полная иллюзия функционирования реальной системы.

Предложенная методика исследования включает: установку и конфигурирование необходимой для исследования операционной системы с помощью виртуальной машины; запуск исследуемой программы на виртуальной машине; поиск внесенных изменений в элементы автозагрузки; поиск внесенных изменений в "Диспетчере задач"; поиск внесенных изменений в файлы на носителях информации (появление новых файлов, удаление старых файлов, изменение атрибутов файлов, таких как размер, дата создания, имя владельца, права доступа к файлу, метод доступа к файлу); поиск внесенных изменений в реестр; исследование сетевой активности (если необходимо); в зависимости от результатов поиска, запуск стандартных программ операционной системы; перезагрузку операционной системы; повторение пунктов 3–8; оформление отчета с выводами о проделанной работе.

Представлен пример использования данной методики. Для исследования используется вирус Virus.Win32.Neshta.b (согласно номенклатуре "Антивируса Касперского).

Описаны преимущества и недостатки использования виртуальной машины по сравнению с другими исследованиями программно-компьютерной системы.

ЭКСПЕРТНОЕ ИССЛЕДОВАНИЕ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ В ПРОЦЕССЕ ПРОВЕДЕНИЯ СУДЕБНОЙ ПРОГРАММНО-КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ

А.Э. Ивашков

Предметом данного исследования является закономерности разработки и применения программного обеспечения компьютерной системы, представленной на исследование в целях установления истины по уголовному или гражданскому делу.

Целью судебной программно-компьютерной экспертизы является изучение функционального предназначения, характеристик и реализуемых требований, алгоритма и структурных особенностей, текущего состояния представленного на исследование программного обеспечения компьютерной системы.

Предложено частноэкспертные методы исследования разделить на три группы:

– методы исследования исходных текстов;

– методы изучения алгоритмов программ;

– методы исследования загрузочных модулей (исполняемых кодов).

При этом экспертиза загрузочных программных модулей может использовать такие основные методы: дисассемблирование программ, отладка программ,

мониторинг, при котором отслеживаются все прерывания, вызываемые исследуемой программой.

Каждый из названных методов представляется группой методов частно-прикладного характера, свойственных именно типу решаемых экспертных задач.

Рассмотрены методы экспертного исследования криминалистически значимой информации, которые реализованные в большинстве стандартных утилит и сервисных программ. По алгоритмам доступа и анализа информации эти методы классифицированы следующим образом:

– методы поиска и доступа к данным;

– методы манипуляции с данными (копирование, перемещение, редактирование);

– методы восстановления данных (в т.ч. удаленной информации);

– методы архивации, парольной защиты и пр.

ДЕКОДИРОВАНИЕ ФУНКЦИОНАЛЬНОСТИ МЫСЛИТЕЛЬНЫХ ПРОЦЕССОВ МОЗГОВОЙ АКТИВНОСТИ ДЛЯ УПРАВЛЕНИЯ ОБЪЕКТОМ

В.М. Колешко, Е.А. Воробей

Развитие нейрокомпьютерных систем управления объектами, способных распознавать мыслительные функциональные состояния человека по данным мозговой активности, приобретает все большее значение в научных исследованиях. При этом основная цель в возможности получения данных заключается как в разработки новых методов извлечения информативных признаков функциональности мозга, так и алгоритмов их классификации. Кроме того, проблема извлечения свойств из данных мозговой активности касается главным образом линейности, гауссовости и не принятия во внимания фазовых характеристик биоэлектрического сигнала, что объясняет трудности с нормальным распределением, статическими характеристиками и некоррелированностью частотных свойств активности мыслительных процессов. Несмотря на то, что в нейрокомпьютерных системах управления широкое распространение находит авторегрессионный, вейвлет, фрактальный анализы, в последние годы интенсивно развивается анализ независимых компонент, который, однако, рассматривает частотные характеристики и не учитывает фазовые свойства сигнала. Все эти методы позволяют достичь точности порядка 80% при декодировании двух функциональных состояний.

Наиболее эффективным методом в преодолении проблемы распознавания функциональности работы мозга обладает используемый нами биспектральный анализ, включающий статистику высшего порядка, являющийся перспективным направлением извлечения информативных признаков функциональности работы мозга человека. В то время как традиционные свойства как, например, спектр мощности или автокорреляционная функция с критериями второго порядка не предоставляют такую возможность. К тому же спектральный анализ теряет свои качества, если сигнал нестационарный, отношение сигнала к шуму является низким или спектральный диапазон сигнала перекрывается с частотами других сигналов. В таком случае, если сигнал является случайным гауссовским процессом, кумулянт и, следовательно, биспектр равны нулю, а биспектр негауссовского сигнала легко вычисляется с подавлением цветных и белых шумов. Использование отработанных эффективных механизмов классификации данных, к которым относятся линейный дискриминантный анализ, метод опорных векторов или обычные нейронные сети, совместно с биспектральными характеристиками (биспектр, бикогерентность) позволяет достигнуть высокой степени точности до 90% в распознавании двух мозговых команд, поэтому оптимизационные процессы обработки станут важнейшим направлением в развитии нейрокомпьютерных систем. Однако следует отметить,

что на сегодняшний день нет высокоточных математических методов декодирования функциональных мыслительных процессов, что является нашей дальнейшей задачей в развитии интеллекта и познании тайн головного мозга человека, информатики биосистем, а в конечном итоге проектировании умных машин.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ЭКСПРЕСС-ДИАГНОСТИКИ КРОВИ И ЗАЩИТА ИНФОРМАЦИИ

В.М. Колешко, Е.А. Воробей

Многолетние исследования показали, что оптимизационные кластерные методы анализа позволяют решать сложные интеллектуальные задачи в различных научных направлениях. При этом наиболее яркий практический успех методов анализа в многомерном пространстве признаков в настоящее время достигнут при распознавании неявных патологических процессов в организме человека, когда единственным источником информации являются биологические составляющие отдельной личности, которые могут включать биохимические данные о составе слюны, мочи и в частности анализа крови. Кластерные методы анализа прекрасно справляются с решением сложных задач диагностики, и, в частности, они определяют зависимость между общими параметрами крови и наличием определенной патологии у человека, поскольку любое заболевание приводит к изменению биофизиологических процессов в организме. На основании этих предположений была разработана интеллектуальная программа экспресс-диагностики крови "Био-ЭДК", которая осуществляет распознавание состояния человека с вероятностной моделью обнаружения или отсутствия скрытых форм протекания заболеваний на этапе их возникновения. Отличительной особенностью программы является высокая чувствительность и достоверность к протекающим изменениям в организме за счет использования большой базы показателей анализов крови и патологий, характеристик симптомов заболеваний, оптимизационных кластерных методов обработки, а также адаптивность для анализа других биологических компонент.

Для предотвращения случаев намеренного или случайного ввода неверных значений показателей в программе предусмотрена оценка значения показателя в определенных допустимых диапазонах его изменения, которая рассчитывалась на основе нормальных численных представлений. При этом для обеспечения наглядности и защиты введенной информации о значениях показателей крови, а также выбранных явных симптомов заболевания, которые наблюдаются у больного, предусмотрено окно вывода данных, в котором заносятся все изменения при работе с программой. Результаты прогнозирования также отображаются в представленной области программы, что позволяет в реальном времени осуществлять передачу информации о внесенных данных анализа крови и результатов распознавания патологии медицинскому персоналу. В случае необходимости возможно также скрытие окна вывода для обеспечения конфиденциальности передаваемой информации с последующей гарантией просмотра любой проведенной экспресс-диагностики состояния человека по крови. Кроме того, нужно, чтобы основная база со всеми исходными данными оставалась защищенной от несанкционированного взлома, с ограничением функций для ее заполнения. Поэтому программа "Био-ЭДК" позволяет не только распознавать болезнь, но и препятствовать процессам неправомерных изменений базы данных, неправильной постановки диагноза, а также получения информацией об анализах диагностируемой личности.

СИСТЕМА ЦЕНТРАЛИЗОВАННОГО МОНИТОРИНГА И КОНТРОЛЯ СОСТОЯНИЯ УЗЛОВ КОМПЬЮТЕРНОЙ СЕТИ

Ю.М. Кротюк, Я.И. Кирилов

Система централизованного мониторинга и контроля состояния узлов компьютерной сети "Монитор" представляет собой многокомпонентную распределенную систему реального времени и призвана обеспечить интеграцию различных программных, аппаратных и аппаратно-программных средств и сервисов обеспечения безопасности корпоративной сети в единую информационную среду, реализующую унифицированные механизмы сбора, хранения и обработки оперативной информации о возникающих в процессе эксплуатации компьютерной сети событиях, например, таких как неудачная попытка аутентификации, ошибка репликации Active Directory, обнаружение вирусного заражения, отказ порта коммутатора и т.п. Вся информация о подобного рода событиях принимается соответствующим компонентом системы, аккумулируется в центральной базе данных, а затем выводится на консоль автоматизированного рабочего места администратора корпоративной информационной сети. Вывод информации сопровождается световой сигнализацией и звуковым оповещением.

"Монитор" способен взаимодействовать с электронной моделью корпоративной информационной сети, представляющей собой совокупность сведений о физической топологии сети, имеющихся узлах, каналах связи и их характеристиках. Электронная модель визуально представлена на плоскости в виде диаграммы размещения, например оформленной в соответствии с получившей широкое распространение графической нотацией, утвержденной стандартом унифицированного языка моделирования UML [1].

Все события, инициированные поставщиками, попадают в базу данных только после прохождения фильтра событий. Любое событие, хранящееся в базе данных, может находиться в одном из двух состояний — обработано администратором (не активно) или не обработано администратором (активно). Узел сети, для которого в базе данных зафиксировано хотя бы одно активное событие считается активным, иначе — не активным. Отображение активных узлов на диаграмме размещения сопровождается световой сигнализацией. Система обеспечивает возможность фильтрации событий в соответствии с устанавливаемыми правилами.

Литература

1. Леоненков А. Объектно-ориентированный анализ и проектирование с использованием UML и IBM Rational Rose. Москва, 2006.

ТЕКСТОЗАВИСИМЫЙ ВЕРИФИКАТОР РЕЧИ В СИСТЕМЕ КОНТРОЛЯ ДОСТУПА

Т.В. Левковская

Большинство верификаторов речи являются зависимыми от текста. Верификация диктора осуществляется по фиксированной парольной фразе, которая может быть изменена по определенным словам, порядок произношения которых определяется самой системой случайным образом. В последнем случае снижается возможность фальсификации голосового пароля.

Предложена системы автоматической верификации диктора по голосу. В качестве информативных признаков используются мел-кепстральные коэффициенты дискретно-косинусного преобразования и их дельта-параметры. Сравнение тестового и эталонного высказываний осуществляется с помощью нескольких классификаторов. В одном из них распознавание осуществляется модифицированным методом динамического программирования, который позволяет определить вероятность

присутствия распознаваемых слов в непрерывном речевом потоке и оценить их временное местоположение в реальных условиях наличия разного рода акустических помех при неизвестных начале и конце слова. Используются также классификаторы на основе моделей гауссовых смесей. Принятие решения осуществляется путем анализа и объединения вероятностных оценок используемых классификаторов. В докладе приведены результаты исследования надежности верификации диктора на примере распознавания изолированно произносимых названий цифр. Для тестирования была создана экспериментальная речевая база данных, включающая образцы голосов 36 взрослых дикторов (14 женщин, 22 мужчин). Запись производилась с периодичностью 14 дней в офисных условиях. Каждый диктор произносил цифры от 0 до 9 по 2 раза. Речевые сигналы записывались в моно-режиме с частотой дискретизации 11 025 Гц, 16 бит на отсчет.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В БАНКОВСКИХ СИСТЕМАХ

А.Е. Лещев

В этом докладе рассматривается общая картина безопасности информации в банке, возможные угрозы и уязвимости, а также способы отражения их.

Под понятием "защищаемая банковская информация" будем понимать конфиденциальную финансовую информацию, информационные ресурсы с ограниченным доступом, составляющие служебную и коммерческую тайну, а также иные конфиденциальные данные на бумажной, магнитной, оптической основе и информацию, защищенную технико-инженерными конструкциями, информационные массивы и базы данных.

Защита банковской информации является комплексным процессом. Комплексность обеспечивается рядом мер, направленных на сохранение безопасности на всех этапах "жизни" данных: получение, хранение, передача и использование. Процесс же означает непрерывность действий направленных на безопасность информации.

Для представления общей картины необходимо выделить основные звенья в цепи защиты банковской информации. В работе рассматриваются четыре таких звена: передача информации по сети; техническая защита (в первую очередь, подразумеваются аппаратные средства "сопротивления вторжению"); надежность программного обеспечения; защита от "человеческого фактора".

Рассмотрены некоторые угрозы и уязвимости защиты конфиденциальной банковской информации, а также методы противодействия им: физический доступ к местам хранения и обработки информации; создание, хранение и использование резервных копий баз данных; несанкционированный доступ к информации сотрудниками банка.

На мой взгляд, только детальное представление и понимание возможных угроз и методов защиты от них для каждого звена цепи позволяют вырабатывать комплекс мероприятий, обеспечивающих безопасность системы в целом.

МАСКИРОВАНИЕ СООБЩЕНИЯ СИГНАЛОМ ИЗОБРАЖЕНИЯ

А.И. Митюхин, А.А. Карчевский

Рассматривается метод передачи дополнительной (скрываемой) информации с использованием эффективного кодирования изображения и дисперсионной фильтрации коэффициентов дискретного преобразования Хартли (ДПХ).

Предполагается, что канал передачи изображения является широковещательным. Свойства канала и источника информации считаются

фиксированными. Задача состоит в надежной передаче сообщения, например, низкоскоростных двоичных данных, или отсчетов речевого сигнала при условии, что неопределенность подслушивателя (перехватчика информации) за время наблюдения (анализа) сигналов не меньше, чем наперед заданная величина. Обеспечение скрытности факта наличия в сигнале изображения дополнительной информации достигается за счет различия основных характеристик используемых в системе сигналов. Полоса частот маскирующего сигнала должна быть много шире полосы информационного. Период передачи одного информационного символа соизмерим с размерностью блока пикселов кодируемого фрагмента изображения. Отношение средней мощности информационного сигнала к средней мощности маскирующего сигнала много меньше единицы.

В качестве фрагментов маскирующих изображений использовались матрицы отсчетов размером 8×8. Результатом эффективного кодирования является матрица коэффициентов преобразования Хартли. В преобразованном векторном пространстве сравнительно небольшое число координат представляют с минимальной среднеквадратической ошибкой большую часть статистической информации о кодируемых элементах изображения. Это свойство позволяет осуществить зональную фильтрацию тех коэффициентов преобразования (трансформант), которые несущественны в энергетическом отношении. Если руководствоваться дисперсионным критерием [1] отбора трансформант, вычисляется двухмерная функция распределения дисперсий трансформант. С ее помощью определяется пространственная зона в которую внедряется дополнительная информация. Декодирование информации реализуется на основе алгоритма обратного линейного двухмерного ДПХ и операции сравнения с исходным маскирующим фрагментом.

Литература

1. Митюхин А.И., Карчевский А.А. // Сб. матер. междунар. науч.-практ. конф. "Современная радиоэлектроника: научные исследования и подготовка кадров", Ч. 2. Минск, 2008. С. 47–48.

ЗАЩИТА ИНФОРМАЦИИ В ПАССИВНОЙ СИСТЕМЕ КОНТРОЛЯ ДОСТУПА

Н.И. Мурашко

Пассивная система контроля доступа предназначена для скрытого наблюдения за территорией и выдачи сигнала тревоги при возникновении нештатной ситуации. Система включает видеокамеры, сейсмические, акустические и магнитометрические интеллектуальные сенсоры, информация от которых передается по каналам связи в удаленный компьютер пункта управления. В процессе эксплуатации системы возникают проблемы скрытности передачи и обработки информации. Ложные срабатывания интеллектуальных сенсоров приводят к передаче данных, которые могут быть перехвачены техническими средствами потенциального нарушителя. Необходимо учитывать, что система контроля доступа должна функционировать в условиях возможного радиоэлектронного противодействия.

Повысить степень защиты информации предлагается за счет снижения частоты ложных срабатываний интеллектуальных сенсоров и применения современных средств радиосвязи, обладающих высокой помехозащищенностью, которая включает в себя скрытность системы радиосвязи и ее помехоустойчивость. Снизить до минимума частоту ложных срабатываний, а следовательно и выход в эфир, можно за счет многоэтапной предварительной обработки информации интеллектуальных сенсоров. По мере приближения человека к запретной зоне последовательно срабатывают детекторы движения телевизионной камеры и сейсмического датчика, а информация о движении передается в пункт управления при наличии сигналов от двух детекторов движения. Если нарушитель перемещается на транспортном средстве, то его обнаруживают также акустический и магнитометрический интеллектуальные сенсоры.

Принимая во внимание незначительный объем передаваемой информации о нарушителе, у противодействующей стороны практически не остается времени на обнаружение и измерение основных параметров радиосигналов и создания мощной помехи.

ЗАЩИТА НАВИГАЦИОННЫХ ДАННЫХ В СИСТЕМЕ ВЫСОКОТОЧНОГО МОНИТОРИНГА

А.Н. Мурашко

В системе высокоточного мониторинга координаты места нахождения подвижного объекта могут измеряться до 50 см с дальнейшей передачей по радиоканалу в пункт управления. В качестве подвижного объекта могут выступать колесное или гусеничное механизированное средство, воздушный летательный аппарат и человек. Подвижный объект должен быть оснащен навигационным приемником, миникомпьютером (бортовым компьютером) и аппаратурой радиосвязи, в качестве которой может быть использован GPRS модем. Высокая точность отображения координат места положения объекта достигается за счет информации о дифференциальных поправках географических координат.

В пункте управления производится кодирование передаваемой информации о дифференциальных поправках с учетом географических координат места нахождения объекта, точность которых не превышает 70 м. При этом объекту передаются данные в местной системе координат, которые отображаются на изображении местности высокого пространственного разрешения или топографическом плане крупного масштаба. Таким образом, мобильный объект не располагает ключом (конвертором) преобразования географической системы в местную высокоточную систему координат. При отсутствии на изображении местности известных опорных точек объект осуществляет их поиск, производит измерение географических координат с точностью до 0,5 м и передает в пункт управления. При этом географические координаты опорных точек, количество которых не превышает пяти, кодируются с помощью произвольного цветного изображения формата JPEG 1280×1024 пикселей и передаются в пункт управления, где устанавливается связь между географической и местной системами координат.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ РЕЖИМОВ БЛОЧНЫХ ШИФРОВ ДЛЯ "ПРОЗРАЧНОГО" ШИФРОВАНИЯ ФАЙЛОВЫХ СИСТЕМ

А.В. Недилько

"Прозрачное" шифрование файловой системы является одним из наиболее распространенных и надежных средств защиты информации в настоящее время. Суть метода состоит в том, что создается единый зашифрованный файл на физическом носителе информации (так называемый контейнер), в пределах которого (как обычного дискового раздела) стандартными средствами ОС создается и используется файловая система. Таким образом, для пользователя работа с зашифрованными данными не отличается от работы с обычными данными.

Большинство современных файловых систем делят хранимую информацию на секторы, и выполняют все операции посекторно. Это означает, что драйвер виртуального устройства, который осуществляет шифрование / дешифрование, должен шифровать каждый сектор независимо от других. Сектор обычно больше блока шифра, поэтому сектор шифруется как последовательность блоков; при этом применяется определенный режим шифрования.

Необходимость шифровать каждый сектор независимо, а также особенности организации файловых систем создают следующие специфические условия, значительно расширяющие возможности для успешной атаки:

– файловая система всегда содержит служебные данные, формат, расположение, и часто сами значения которых могут быть предугаданы;

– теоретически возможно попадание в руки "взломщиков" нескольких копий одного и того же сектора, зашифрованного одним ключом, но с различным инициализационным вектором;

– создавать случайные инициализационные векторы для каждого сектора нецелесообразно; вместо этого они вычисляются, а значит, могут быть вычислены и при взломе.

В этих условиях стандартные режимы шифрования (ECB, CBC, CFB, OFB, CTR) не обеспечивают достаточный уровень надежности.

Для обеспечения надежности защиты данных при шифровании файловых систем были разработаны специальные режимы шифрования: ESSIV, LRW, XEX, XTS. На сегодняшний день наиболее безопасным является режим XTS, который был сертифицирован IEEE в декабре 2007. Режим XTS уже используется в специализированном ПО для "прозрачного" шифрования файловой системы.

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ ЛВС В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ НА ОСНОВЕ КЛАВИАТУРНОГО ПОЧЕРКА

В.О. Пантелеев

Среди развиваемых в настоящее время биометрических идентификационных технологий особое место занимает технология идентификации и аутентификации пользователей компьютерных средств, основанная на анализе почерка работы на клавиатуре.

Работа биометрической системы описывается техническими и ценовыми параметрами. Оценка эффективности биометрических технологий, помимо стоимостных показателей и удобства использования, основывается на использовании двух вероятностных параметров — ошибки первого и второго рода.

Имеющаяся в открытой печати информация о характеристиках систем и реализованных в них алгоритмах позволяет сделать вывод о том, что подобные системы не обеспечивают требуемый уровень надежности, так как имеют не достаточно низкую вероятность ошибки ложного отказа и ошибки ложного пропуска.

Анализ практики применения таких систем показал, что существующие в настоящее время системы не в полной мере отвечают требованиям скрытности идентификации, ограничения на вычислительные ресурсы при реализации алгоритма и удовлетворительной достоверности идентификации при ограниченном времени решения задачи, которое определяется не только временем обработки, но и временем накопления статистических данных. Таким образом, при реализации проекта были решены задачи разработки эффективных методов обработки экспериментальных данных и задачи по реализации программного комплекса, обеспечивающего оперативную обработку информации в режиме реального времени и ее защищенность.

В рамках решения первой задачи были исследованы методы идентификации пользователя, суть которых состоит в том, чтобы из имеющегося статистического материала вычислять характеристику, учитывающую не одну, а несколько особенностей клавиатурного почерка. Сравнительный анализ показал, что реализация предлагаемых методов позволяет по сравнению с известными уменьшить вероятности ошибок при одинаковом объеме статистического материала.

Программный комплекс был реализован в виде набора следующих модулей:

– модуль накопления статистических данных (реализовано в виде клиент-серверного приложения);

– модуль обработки информации (на данном этапе происходит сравнение накопленных данных о пользователе с его эталоном);

– модуль управления программным комплексом (позволяет просматривать результаты обработки информации и управлять текущим состоянием подключенных клиентов и системой в целом).

Данное архитектурное решение позволяет разместить серверное приложение и модуль обработки информации на отдельных рабочих станциях, что позволяет существенно увеличить производительность системы.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОНЕЧНЫХ БАНКОВСКИХ ТЕРМИНАЛОВ

А.Н. ПАРХИМОВИЧ

Предложение банковских продуктов через сеть терминалов самообслуживания становится массовым явлением. Как показывает мировая практика 90% банковских услуг, оказываемых в рамках традиционных отделений банка, может быть не только автоматизировано, но и переведено в сферу самообслуживания с помощью современных терминальных устройств.

Данный процесс требует к себе особого внимания как со стороны правового обеспечения его функционирования, так и со стороны обеспечения безопасности при работе и эксплуатации терминалов.

Существующая в Республике Беларусь система безналичных расчетов по розничным платежам на основе применения электронных платежных инструментов представлена в основном системами расчетов с использованием банковских пластиковых карточек и электронных денег.

Правовую основу функционирования системы составляют Банковский кодекс Республики Беларусь, нормативные правовые акты Национального банка, а также разработанные в соответствии с ними локальные нормативные правовые акты и договоры банков и иных участников систем расчетов с использованием электронных платежных инструментов.

Системы расчетов с использованием электронных денег поддерживаются соответствующими техническими, организационными и процедурными мерами защиты для предотвращения, сдерживания и обнаружения угроз безопасности системы, в том числе и злоумышленных действий.

Программные и технические средства, применяемые в системах расчетов с использованием электронных денег, подлежат сертификации органом по сертификации программно-технических средств в области банковских услуг и технологий в порядке, установленном законодательством Республики Беларусь.

В целях обеспечения безопасной и надежной деятельности при осуществлении операций с электронными деньгами банки должны соблюдать нормативы безопасного функционирования и выполнять резервные требования, установленные Национальным банком.

Техническая, организационная и информационная поддержка развития функционирующих в Республике Беларусь систем расчетов с использованием банковских пластиковых карточек осуществляется ОАО "Национальный процессинговый центр", ЗАО "Платежная система "БелКарт".

Под безопасностью системы банковских терминалов понимают их свойство, выражающееся в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных возмущающих (умышленных и неумышленных) воздействиях на нее. Иными словами под безопасностью системы понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Следует отметить, что природа

воздействия может быть самой различной, а следовательно и поле для угроз безопасности достаточно обширное.

Для многих банков характерно то, что нарушение безопасности информации в их конечных банковских терминалах может нанести огромный материальный ущерб как самим банкам, так и их клиентам. Поэтому эти организации вынуждены особое внимание уделять гарантиям безопасности, что ведет к необходимости реализации комплексной защиты.

Комплексный подход к обеспечению безопасности, а так же постоянный мониторинг и поиск новых угроз являются ключевым моментом обеспечения безопасного функционирования конечных банковских терминалов.

На сегодняшний день существует достаточно широкий спектр возможных злонамеренных действий, детектируемый на различных уровнях классификации угроз информационной безопасности и с каждым годом он расширяется.

Физическое воздействие на конечный банковский терминал - один из первоочередных вопросов. Защита от вандализма, погодных условий, попытки физического взлома — решаются путем совершенствования конструкции терминалов: установкой сейфов с различными видами замков (с двойной комбинацией, с двойной комбинацией и дистанционным доступом и др.); доработкой кассет и контейнеров загрузки, хранения банкнот, исключающих доступ к денежным средствам; установкой различного рода тревожных датчиков (датчики тревожной сигнализации, сейсмические датчики, датчик температуры и др.); установкой источника бесперебойного электропитания; установкой встроенной камеры видео наблюдения, а так же тщательным исследованием места установки терминала с точки зрения безопасности его использования.

Внешний вид терминала, а так же расположение его основных функциональных частей является не только отличительными признаками того или иного производителя устройства, но и тщательно продуманной стратегией безопасности.

Скимминг — вид мошенничества, при котором используют специальные виды электронных устройств, устанавливаемые на лицевой части терминала, для считывания информации о платежной карточке (номер карточки, пин-код), так считывающее устройство накладывается поверх гнезда для ввода карточки (закамуфлированные сканеры) и клавиатуры (накладные клавиатуры).

В сфере мошенничества электронных платежей при обращении с кредитными картами, невозможно выделить единичную причину позволяющую совершать преступление. Так угрозы в виде "кардинга", "фишинга", пользования украденной (утерянной) картой, заявление от чужого имени и др. содержат в себе как социальные аспекты, так и уязвимости программного обеспечения и самого устройства терминала.

Эффективной мерой противодействия, в данном случае, является обучение клиентов банковских терминалов правилам пользования терминалов и мерам безопасности при обращении с картами электронных платежей, а так же своевременное их уведомление о выявленных опасностях.

Сети современных крупных банков уже нельзя назвать локальными в традиционном значении этого слова. Они состоят из множества подсетей и сегментов, распределенных территориально и объединяемых самыми различными каналами связи – от оптических до коммутируемых. Переходя с использования в своих банкоматах OS/2 на применение Windows и IP-сети, банки соответственно в корне меняют и систему подключения к своим информационным сетям. Во многих случаях это означает, что банкоматы и обычные офисные компьютеры банков оказываются подключенными к одним и тем же вычислительным сетям. Как следствие, сети банкоматов, инфокиосков, обменных пунктов и др. могут быть подвержены всем существующим видам угроз — вирусным атакам (в 2003 г. вирус Slammer заставил прекратить работу сразу 13 000 банкоматов Bank of America, Imperial Bank of Commerce), злонамеренным действиям персонала, ошибкам администраторов, проникновениям изнутри и т.д.

Пути решения проблемы лежат в четком планировании и проектировании строящейся сети терминалов с учетом современных тенденций развития телекоммуникационных сетей, а так же использовании передовых технологий защиты информации:

– межсетевого экранирования;

– шифрации трафика;

– организации системы антивирусной безопасности и установки обновлений операционной системы;

– разработке политики безопасности функционирования системы;

– грамотном делегировании полномочий администраторов и обслуживающего персонала и др.

Следует так же учитывать тенденцию унификации электронных платежных сообщений и объединение в одну платежную систему ранее разрозненных организаций, что с упрощением взаимодействия между финансовыми учреждениями, в то же время, создает предпосылки для новых угроз безопасности.

РАЗРАБОТКА ЗАЩИЩЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Н.Г. Пришивалко

Современное программное обеспечение (ПО) как средство защиты информации в компьютерных и телекоммуникационных сетях должно удовлетворять следующим требованиям безопасного программирования:

1) при создании в ПО должен быть реализован объектно-ориентированный (ОО) подход, включающий в себя ОО анализ, ОО проектирование и ОО программирование.

2) исходные тексты программ должны быть оформлены в соответствии с требованиями венгерской нотации (Hungarian Notation), включающей:

– мнемоническое значение: идентификатор должен легко запоминаться;

– смысловое значение: роль идентификатора должна быть ясна из его названия;

– преемственность: похожие объекты должны иметь похожие идентификаторы;

– скорость решения: создание, ввод и редактирование идентификатора не должны занимать слишком много времени, идентификатор не должен быть слишком длинным;

– каждая строка в программе должна иметь смысловой комментарий.

В программных процессах (особенно, выполняющихся в ОС типа Windows) должна присутствовать обработка исключений, реализующаяся через специальные конструкции применяемого ОО языка программирования (например, для C++ это операторы — try, catch, throw).

Для защиты от несанкционированного доступа в программном продукте должны быть реализованы следующие функции:

– защита от дизассемблирования и трассировки;

– генерация серийного номера и настройка на параметры компьютера, на котором выполняется генерация и дальнейшая эксплуатация;

– каждый объект в ПО должен позволять свою отладку независимо от других;

– описание ПО должно быть представлено раздельно в виде алгоритмов и объектов (в руководстве программиста);

– в ПО должна присутствовать и отображаться по запросу пользователя статистика работы всех процессов (в том числе информация о сбоях);

– работа в защищенном режиме микропроцессора (защита от взлома должна выполняться на уровне команд микропроцессора, начиная с команд микропроцессора Intel386);

– должна выполняться периодическая проверка производительности отдельных подсистем компьютера.

ИСПОЛЬЗОВАНИЕ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ ПРИ РАБОТЕ ГОСУДАРСТВЕННЫХ ОРГАНОВ ПО ПРИНЦИПУ "ОДНО ОКНО"

Н.В. Ручанова

При реализации административных процедур госорганами возникает потребность в надежной и быстрой передаче данных между различными ведомствами. При передаче информации в электронном виде должны быть обеспечены конфиденциальность, контроль целостности, контроль подлинности запрашиваемых госорганом данных.

Целостность и подлинность обеспечивается использованием средств ЭЦП электронного документа, хеширования или имитозащиты. Неотказуемость от приема (передачи) электронного документа обеспечивается использованием средств ЭЦП (подпись документа отправителем), квитированием приема документа (подпись квитанции получателем) и хранением документа с ЭЦП в течении установленного срока отправляющей (принимающей) стороной. Конфиденциальность может быть обеспечена посредством криптографических методов защиты информации.

Таким образом современные средства ЭЦП и существующие асимметричные криптоалгоритмы позволяют успешно решить сформулированные выше задачи.

На начальном этапе построения системы "Одно окно" данные требования могут быть удовлетворены путем использования системы защищенной электронной почты для государственных органов, включающей в себя инфраструктуру открытых ключей и шифрование передаваемого трафика.

Однако в дальнейшем необходимо создание полнофункциональной системы защиты информации с использованием сертифицированных ГЦБИ средств ЭЦП и защиты информации и полной экспертизой системы на соответствие требованиям действующего законодательства. Внедрение данной системы позволит организовать нормативно значимый межведомственный документооборот госорганам, работающим по принципу "Одно окно", ускорить выполнение административных процедур, улучшить механизмы отчетности по выполненным процедурам и выборки данных.

СИСТЕМЫ МАСКИРОВАНИЯ ГОЛОСА ГОВОРЯЩЕГО

А.С. Рылов, Ю.А. Вежик, А.С. Вискуп, Д.В. Мотуз

Исследования в области разработки систем маскирования (изменения) голоса (СМГ) говорящего представляют сегодня целое направление в речевой информатике. Все СМГ можно разделить на две разновидности.

К первой разновидности относятся СМГ для изменения качества голоса и могут использоваться для защиты прав свидетеля на суде или для удовлетворения требования человека быть неузнанным при публичном раскрытии какой-либо информации. Проведенный анализ показал, что эти системы реализуются, как правило, на основе вокодерных систем, работающих как в частотной, так и во временной областях. Также установлено:

1) системы, работающие в частотной области, позволяют гибко регулировать акустические параметры как тоновые, так и форматные, но имеют недостаток, связанный с возникновением фазовых искажений при больших значениях коэффициента модификации параметров. Это ощущается в виде реверберационных эффектов воспринимаемых на слух. Кроме того, реализация этих систем более сложная, чем систем, работающих во временной области;

2) системы, работающие во временной области, позволяют легко нелинейно изменять частоту основного тона без изменения формантной структуры. Модификация формантной структуры затруднена, однако применение систем анализа-синтеза речи

на основе метода линейного предсказания с выделением линейных спектральных пар и с последующим их преобразованием с помощью билинейного Z-преобразования позволяет преодолеть этот недостаток.

Ко второй разновидности СМГ относятся системы, которые позволяют трансформировать голос истинного диктора в голос определенного диктора (диктора-"мишени"). При этом осуществляется адаптация параметров речи истинного диктора к параметрам речи диктора-"мишени" для определенного речевого фрагмента (предложения, фразы), которые были произнесены обоими дикторами. К наиболее сложным морфологическим системам относятся системы с распознаванием речи произвольного диктора. В этом случае речевой морфинг осуществляется без предварительной фазы адаптации к параметрам определенного диктора-"мишени", но принадлежащими определенной речевой единице. Предварительной фазой в таких системах является распознавание речи от произвольного диктора, а затем выделение параметров у истинного диктора для распознанного речевого фрагмента от диктора-"мишени", и только после этого осуществляется адаптация параметров обоих дикторов и синтез речи похожий на голос диктора-"мишени". В системах этого типа при синтезе речи целесообразно применять трехмерную анимацию лица диктора-"мишени" с целью повышения правдоподобности речевого морфинга.

Системы, относящиеся ко второй разновидности СМГ, как правило, используются для создания систем синтеза речи по тексту, которые могут говорить голосом любого диктора. Кроме того, они могут использоваться в качестве специальных систем.

РАЗДЕЛЕНИЕ КЛЮЧЕВОГО ПРОСТРАНСТВА СИММЕТРИЧНЫХ ШИФРОВ НА ОСНОВЕ УСЕЧЕННОЙ ИНТЕРПОЛЯЦИОННОЙ ОЦЕНКИ ТЕСТОВОЙ ХАРАКТЕРИСТИКИ

С.Б. САЛОМАТИН, Д.М. БИЛЬДЮК

Надежность симметричных алгоритмов шифрования характеризуется безопасным временем, которое определяет устойчивость криптоалгоритма к использованию метода прямого перебора для отыскания ключа. Если длина ключа составляет n бит, то метод прямого перебора требует проведения порядка 2^n операций криптоанализа. Существуют методы дифференциального и линейного криптоанализа, позволяющие исключить из рассмотрения значительную часть вариантов ключа, что приводит к уменьшению вычислительной сложности криптоанализа по сравнению с прямым перебором. Однако данные методы не эффективны при анализе шифров типа AES.

Один из путей ускорения криптоанализа состоит в разделении множества ключевых комбинаций на классы по форме кривой усеченной интерполяционной оценки тестовой характеристики симметричного шифра.

Тестовая характеристика шифра представляла собой отклик шифра на воздействие импульсных информационных кодов, при заданной форме ключа.

Усеченная интерполяционная оценка выполнялась по методу Бен–Ор–Тивари с использованием алгоритма Берлекампа–Месси и исключением последнего этапа решения системы уравнений. Результат интерполяционных преобразований отображался в виде кривой визуализации.

Результаты моделирования. Исследовались шифры AES и ГОСТ 28147. Моделирование алгоритмов показало, что ключевое пространство криптосистем можно разделить на классы по следующим признакам: кривые визуализации параболического типа разного масштаба и отсутствие решения алгоритма Берлекампа–Месси.

Полученный результат позволяет использовать разделение ключевого пространства для ускорения процесса криптоанализа.

КРИПТОГРАФИЧЕСКАЯ СИСТЕМА НА ОСНОВЕ ХАРАКТЕРИСТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ТРЕТЬЕГО ПОРЯДКА

С.Б. САЛОМАТИН, А.А. ОХРИМЕНКО, А.М. МАКАРЕВИЧ

Криптографические системы на основе характеристических последовательностей третьего порядка являются технической альтернативой систем RSA и систем на эллиптических кривых. Характеристические последовательности формируются на основе кубического уравнения, с помощью регистра сдвига с обратными связями.

Техника характеристических последовательностей позволяет реализовать быстрые системы шифрования, аутентификации с открытым ключом, а также распределения и формирования ключей.

Система распределения с открытым ключом. Имеет два состояния: формирования ключей и установления общего ключа пользователей. В первом состоянии формируется двухуровневое ключевое пространство пользователей на основе кубического неприводимого полинома над полем $GF(p)$ периода $P=(p^2+p+1)$. Первый уровень содержит секретные ключи пользователей, второй уровень — открытые ключи системного взаимодействия. Ключи первого уровня представляют собой случайные числа, взаимно простые с числом P. Ключи второго уровня представляют собой пару элементов (s_k, s_{-k}) двух взаимных характеристических последовательностей, формируемых кубическим полиномом. Пространство ключей представляют собой множества, состоящие из всех лидеров смежных классов модуля p^2+p+1 и всех неприводимых полиномов над полем $GF(p)$ степени 3 с периодом p^2+p+1.

Во втором состоянии формируется общий ключ пользователей на основе свойства характеристических последовательностей: $s_k(s_e(a, b), s_{-e}(a, b))=s_{ke}(a, b)$, где k и e — положительные целые числа. Алгоритмы системы реализуются с использованием техники быстрых вычислений.

Оценка уровня защитных свойств. Защитные свойства характеристических последовательностей и криптосистем на их основе базируются на трудности решения задачи дискретного логарифма в конечном поле $GF(p^3)$, где p — простое число.

Оценка вычислительной сложности. Вычислительная сложность быстрого алгоритма криптосистемы может быть приблизительно оценена зависимостью $L \log n$ модулярных операций умножений.

УПРАВЛЕНИЕ ГРАФИКОМ ПЕРЕДАЧИ ПАКЕТОВ В ШИРОКОВЕЩАТЕЛЬНЫХ СИСТЕМАХ В УСЛОВИЯХ DOS-АТАК

С.Б. САЛОМАТИН, И.В. БОБРОВ, П.А. ПРОХОРОВ

Рассматривается широковещательная система, использующая пакетную форму информационного взаимодействия. Предполагается, что каждый пакет соотнесен с текущим состоянием источника информации, содержит k информационных символов и требует для их передачи одну условную единицу времени.

Модель графика передачи пакетов. График передачи пакетов определяется как последовательность величин $S=\{r_1, r_2, \ldots\}$, $r_j \geq 1$, где r_j — количество времени, требуемое для передачи j-го сообщения. Длина сообщения равна $r_j k$.

Последовательности S ставится в соответствие временная последовательность стартовых позиций $\{t_1, t_2, \ldots\}$, где t_j — время начала передачи сообщения j.

В модели используются также оценки времени ожидания, вероятного времени ожидания, старения данных.

Модель DoS-помехи. Предполагается, что помеха представляет собой последовательность $\{h_1, l_1, h_2, l_2, \ldots\}$, где h_1 — момент передачи первого импульса; h_j —

длина интервала времени между (j–1)-м и j-м импульсами сигнала помехи; l_j — длина j-го импульса помехи.

Взаимное влияние графиков помехи и системы передачи данных оценивается с помощью методов оптимизации с ограничениями и решения диофантовых уравнений теории чисел.

Определяется оптимальная DoS-помеха для регулярных графиков пакетного взаимодействия. Предлагается структура анти-DoS графика, использующего дополнительные защитные блоки временных интервалов.

СИСТЕМЫ С СИНХРОННЫМ ХАОТИЧЕСКИМ ОТКЛИКОМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

А.В. СИДОРЕНКО

Многообразие потенциальных угроз информации в телекоммуникационных системах, их структурно-функциональная сложность, участие человека в технологическом процессе обработки информации обуславливают необходимость комплексного подхода для реализации целей безопасности путем анализа, разработки и создания средств защиты информации.

Средства зашиты на уровне аппаратного и программного обеспечения позволяют осуществить разграниченный доступ к информации; защиту информации в каналах передачи; защиту от воздействия программ-вирусов; защиту от утечки информации по акустическим и электромагнитным излучениям.

Один из подходов обеспечения защиты информации в каналах передачи в сфере управления доступом, криптографической защиты и целостности, основан на теории нелинейных динамических систем, использующих детерминированный хаос.

Практически защита информации при ее передаче осуществляется в системах с синхронным хаотическим откликом.

В работе рассмотрены различные схемы передачи информации на основе синхронного хаотического отклика. Представлены особенности каждой их схем, описаны принцип действия, методы построения структурных схем систем информации. Приводится сравнительный анализ различных схем построения по критериям конфиденциальности и качества передачи информации.

ПРОЕКТИРОВАНИЕ АППАРАТНОЙ АРХИТЕКТУРЫ РАСПРЕДЕЛЕННЫХ ИНТЕРНЕТ-ПРИЛОЖЕНИЙ С УЧЕТОМ ТРЕБОВАНИЙ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.О. СИЛЬВАНОВИЧ

В текущее время наблюдается бурное развитие массовых интернет-сервисов. Это социальные сети, офисные приложения, онлайн-игры и прочее.

Популярность такого рода сервисов очень высока, следовательно, их программному обеспечению приходится постоянно испытывать большую нагрузку. Поэтому абсолютное большинство таких приложений имеет распределенную архитектуру. Но с ростом количества компьютеров обслуживающих приложение возрастает и уязвимость самого приложения — вероятность потери информации или несанкционированного доступа к данным.

Предлагаемый подход сводится к использованию так называемых уровней защиты, доступ к каждому из которых строго регламентируется. "Первый" уровень — это серверы хранилища данных, включающие в себя всю пользовательскую информацию, как в виде файлов, так и в виде содержимого базы данных. "Второй" уровень включает в себя непосредственно прикладную логику приложения в виде

исполняемых файлов. "Третий" уровень — это программное обеспечение распределяющее пользовательские запросы, то есть прокси-серверы и балансировщики нагрузки. "Четвертый" уровень представляет собой серверы авторизации и управления доступом, хранения и обработки пользовательских сессий. Также на этом уровне может выполнятся шифрование данных. Каждый уровень представляет собой отдельную подсеть, к которой имеют доступ только серверы следующего уровня. Только к последнему уровню есть возможность доступа извне. Физический доступ к серверам первого и второго уровня не должны иметь даже работники датацентров, а только специально акредитованный персонал. Второй и последующие уровни должны быть разделены между собой аппаратными файрволами.

Достоинства такого построения приложения очевидны. Каждый уровень можно обслуживать отдельно, использую разных сотрудников и разные дата-центры. Упрощается масштабирование. Но самое главное — безопасность пользовательских данных, что отражается на репутации и материальном состоянии компании владельца.

Область применения данного подхода — крупные интернет-сервисы, либо распределенные приложения, требующие повышенных мер безопасности.

ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ ДАННЫХ ДЛЯ МНОГОРЕЖИМНЫХ ДАТЧИКОВ В БЕСПРОВОДНОЙ СЕТИ

С.И. Сиротко, С.В. Юзефович

По мере распространения беспроводных технологий для все более широкого круга применений становится актуальной разработка оконечных устройств различного назначения — сравнительно простых и недорогих, но достаточно функциональных и эффективных. В частности, требования к беспроводным датчикам нередко могут быть противоречивы: поддержка различных типов чувствительных элементов и режимов работы, при этом унификация управления и экономичность. Это предполагает наличие достаточно емкой памяти данных и параметров, а также использование специального протокола обмена, причем устройство подвержено сбоям из -за внешних факторов, а канал связи — помехам и искажениям. Следовательно, необходимо обеспечивать надежность и безошибочность хранимых и передаваемых данных, включая и их восстановление.

Методы, использующие контрольные суммы и помехозащищенные коды, обеспечивают достаточную надежность и безусловно целесообразны, но они реализуются на нижних уровнях иерархии программных средств и не распространяется на логическую корректность данных. Целостность и одновременно правильность обработки могут быть достигнуты объединением данных с описанием их формата и структуры; примером может служить XML. Однако работа с такими форматами достаточно затратна.

Для простых устройств с ограниченными ресурсами эффективно самодокументирование данных в более простой форме: представление их структурами, состоящими из обязательного дескриптора и некоторого (возможно, нулевого) количества однотипных элементов данных, причем дескриптор несет исчерпывающие сведения о всей структуре. Такая форма универсальна, сочетаема с объектными моделями и позволяет корректно интерпретировать каждую отдельно взятую структуру. Ошибки элементов данных ограничиваются пределами структуры, а ошибка в дескрипторе или неверная выборка дескриптора приводят к нарушению связности списка структур и тоже могут быть локализованы (восстановление списка будет требовать дополнительных внешних средств).

Защита передаваемой информации от несанкционированного перехвата и/или искажения рассматривается как задача следующего этапа разработки.

ПРОГРАММА ДЛЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ ПО ЛВС

О.Г. Дубова, А.А. Обухович, Т.Г. Таболич, И.С. Терех

Обеспечение информационной безопасности программного обеспечения (ПО) локальных вычислительных сетей (ЛВС) включает в себя [1] как один из компонентов проверку целостности информации, под которой понимается обеспечение точности, полноты информации и методов ее обработки. Имеется большое число программ, позволяющих проводить проверку целостности ПО ЛВС, однако их использование не всегда может являться оптимальным решением проблемы. Действительно, не всегда существует уверенность в отсутствии путей для входа в систему и, к тому же, необходимо, чтобы хэш-функция удовлетворяла ряду условий: необратимости, чувствительности к изменениям в тексте (вставки, исключения, перестановки), пренебрежимо малой вероятности совпадения значения хэш-функций двух различных документов (вне зависимости от их длин). В докладе контроль целостности ПО АРМ и серверов ЛВС обеспечивается специально разработанной прикладной программой. В настоящее время, эта программа прошла комплексную отладку и успешно используется для контроля целостности ПО в системе комплексной защиты ЛВС предприятия. Использование программы позволило значительно повысить уровень надежности ЛВС и уменьшить число сбоев. С учетом того, что повышение надежности работы ЛВС предохраняет как от прямых материальных потерь, так и от косвенного, "морального", ущерба, можно утверждать, что разработанная программа является экономически эффективной и окупаемой.

Литература

1. СТБ П ИСО/МЭК 17799-2004. Предварительный государственный стандарт Республики Беларусь. Информационные технологии и безопасность. Правила управления информационной безопасностью. – Мн., 2004.

МЕХАНИЗМЫ ЗАЩИТЫ В ВОЛОКОННО-ОПТИЧЕСКИХ СЕТЯХ

Н.В. Тарченко

Рассматривается проблема надежности передачи информации в транспортных сетях телекоммуникаций, которая связана с частотой сбоев в оборудовании, используемом при сквозном режиме обслуживания. В волоконно-оптических сетях, использующих оборудование систем передачи, работающих по технологиям транспортных сетей (SDH, DWDM), используются различные методы повышения надежности (механизмы защиты), которые можно разделить на следующие группы: защита сети или подсети; защита тракта; защита оборудования; защита трафика; защита от несанкционированного доступа.

Защита сети либо подсети используется для увеличения доступности режима сквозного обслуживания и подразумевает использование непересекающейся маршрутизации линий и узлов связи. Это гарантирует работу сети даже при сбоях в узлах или линиях связи. Защита сети или подсети основана на механизмах защиты мультиплексорных секций в топологиях цепь и кольцо 1+1 и 1:1 (MSP, MS-SPRing).

При использовании механизмов защиты тракта, сигнал передачи данных передается по двум различным трактам, которые начинаются и заканчиваются в одних и тех же оконечных точках. Защита тракта в сети может выполняться по следующим правилам: разделение узлов (рабочий и защитный тракты не используют совместно какие-либо промежуточные узлы) и разделение линий связи (рабочий и защитный тракты не имеют общих линий связи).

Защита оборудования обеспечивает защиту сигналов, проходящих через то или иное оборудование, при сбое в интерфейсной или центральной плате. Защита

оборудования реализуется на основе механизма автоматического защитного переключения в форматах 1+1 и 1:n.

Механизм защиты трафика предполагает разделение нагрузки: трафик между двумя узлами сети передается по двум отдельным трактам.

Механизмы защиты от несанкционированного доступа в волоконно-оптических сетях используют как электронные (различные методы модуляции оптической несущей), так и механические средства, не позволяющие снимать информацию неразрушающим способом.

В сложных по топологии сетях используется механизм восстановления. Восстановление не является одним из методов защиты, а использует перенаправление трафика по другим маршрутам сети под действием системы управления сетью в случае каких-либо сбоев. Сеть, в которой применяется восстановление, должна обладать достаточным количеством свободных ресурсов для поиска альтернативных маршрутов (до 30%).

Разработаны методики расчета надежностных параметров сети при использовании различных механизмов защиты и восстановления в транспортных сетях.

ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ ДИФФЕРЕНЦИАЛЬНОЙ ФАЗОВОЙ МОДУЛЯЦИИ (DPSK) В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ ПЕРЕДАЧИ

В.Н. Урядов, Я.В. Рощупкин

DPSK-модуляция для волоконно-оптических систем передачи впервые привлекла внимание в начале 1990-х годов. С появлением и развертыванием оптических усилителей, интерес к DPSK-модуляции заметно снизился, особенно после того, как выяснилось, что нелинейный фазовый джиттер ограничивает длину регенерационного участка. Однако, существенное увеличение скорости канала, спектральной эффективности системы, и длины регенерационного участка значительно изменили сравнительные показатели производительности и между DPSK и модуляцией по интенсивности.

Показано, что, в системах с использованием оптических усилителей, чувствительность приемника при DPSK-модуляции превосходит чувствительность приемника при модуляции по интенсивности примерно на 3 дБ. При вычислении чувствительности применялась схема прямого фотодетектирования с использованием интерферометра Маха-Цендера с задержкой на бит в одном плече. Интерферометр конвертирует приходящий DPSK сигнал в сигналы с модуляцией по интенсивности на его двух выходных портах. Эти сигналы дифференциально детектируются балансным приемником. Выигрыш в чувствительности можно объяснить тем, что расстояние между сигналами "0" и "1" при использовании DPSK в два раза больше, чем при использовании модуляции по интенсивности.

Кроме того, DPSK системы не только лучше по чувствительности приемника, но и более терпимы к нелинейности волокна, особенно в системах со спектральной эффективностью равной 0,4 и выше. Представлен метод компенсация нелинейного фазового джиттера, позволяющие еще более улучшить характеристик DPSK в магистральных системах передачи.

ПРИМЕНЕНИЕ НОВЫХ ФОРМАТОВ МОДУЛЯЦИИ В ВОСП ДЛЯ ПОВЫШЕНИЯ СКРЫТНОСТИ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

В.Н. Урядов, Я.В. Рощупкин

Известно, что снятие информации с волоконного световода достаточно трудоемкая задача, особенно при передаче информации на высокой скорости. Дальнейшее увеличение степени защиты передаваемой информации возможно при использовании других волоконно-оптических технологий: волнового уплотнения, кодирования, пространственного разнесения и т.д. В докладе обсуждается возможность повышения защиты информации при использовании новых видов модуляции в оптических системах передачи.

В настоящее время, в волоконно-оптических системах передачи, стандартом является двоичная модуляция по интенсивности. Однако все интенсивнее ведутся исследования по разработке новых форматов, основанных на модуляции оптической несущей по фазе и частоте. С помощью этих форматов предполагается можно определить две главные задачи: во -первых, обеспечить более эффективное использование спектральных каналов в системах плотного волнового мультиплексирования и, во -вторых, снизить чувствительность информационных сигналов к искажениям из -за дисперсии или нелинейности. Показано, что эти форматы позволяют повысить скрытность передачи информации по оптическому волокну. Действительно, при их использовании отсутствует изменение интенсивности излучения, передаваемого по каналу. В связи с этим, помимо традиционных трудностей снятия информации с волоконного световода возникает дополнительная сложность определения скорости передачи информации, вызванная отсутствием амплитудной модуляции, т.е. уровень интенсивности излучения всегда остается постоянным. На основе фазовой и частотной модуляции оптической несущей, может быть построено множество различных форматов (дифференциальная фазовая модуляция, двойной фазомодулированный бинарный формат, частотная модуляция с различным числом несущих частот и т.д.), каждый из которых может быть применен для обеспечения дополнительной скрытности. В этом случае возникает еще одна степень защиты, связанная с необходимостью распознавания используемого формата модуляции.

БЕЗОПАСНОСТЬ ПЕРЕДАЧИ ИНФОРМАЦИИ В ВОЛОКОННЫХ СИСТЕМАХ С ВОЛНОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

М.А. Вилькоцкий, Ю.Б. Стункус

Сегодня ключевым моментом деятельности традиционных операторов является ранее недооцененная технология пассивных оптических сетей (Passive Optical Networking, PON), которая является практическим воплощением концепции FTTH (Fiber To The Home).

Одним из недостатков сетей PON является общая среда передачи сигналов. Это уменьшает стоимость, но означает не только то, что пользователи должны делить между собой пропускную способность, в частности поток данных по направлению к головному узлу, но и то, что от головной станции данные для абонентов попадают на все абонентские узлы. По заголовкам пакетов абонентский узел находит информацию, предназначенную для него, но с точки зрения безопасности информации этот подход содержит ряд недостатков. Во-первых, потенциальный злоумышленник может получить доступ к конфиденциальной информации абонентов. Во-вторых, создается прецедент, когда недобросовестные абоненты смогут пользоваться услугами, за которые не платили, перехватывая информацию, предназначенную для других абонентов — новости, вещательное видео и т.д. Для решения этих проблем

спецификации FSAN предусматривают встроенное шифрование, компании Quantum Bridge, Terawave и Lucent предлагают добавить к стандартному шифрованию FSAN механизм защиты с помощью паролей по методу churning keys.

Однако последние тенденции в развитии пассивных оптических сетей, указывают на то что большинство производителей оборудования PON (особенно из числа недавно появившихся) отстаивают реализацию BP (волнового разделения) поверх PON для обеспечения почти "неограниченной" пропускной способности. Технология волнового разделения способна предоставить каждому конечному пользователю его собственную длину волны и таким образом обеспечить поддержку множества пользователей. Такой подход в построении сети PON снимает вопрос вышеописанных проблем безопасности, однако ставит другие вопросы. PON с волновым разделением будут строится на основе оптических мультиплексоров, которые, с учетом требования об относительно невысокой стоимости для таких систем, имеют довольно низкое переходное затухание — порядка 15–30 дБ. При таком низком переходном затухании без труда можно выделить полезный сигнал соседних (и не только) каналов. Вопрос повышения безопасности в этом случае стоит в параметрах оптического мультиплексора.

Литература

1. Daniel Pastor, Pascual Munoz, Jose Capmany Modeling and Design of ArrayedWaveguide Gratings. JOURNAL OF LIGHTWAVE TECHNOLOGY, vol. 20, №. 4, april 2002.
2. P. Munoz, D. Pastor, J. Capmany, “Analysis and design of arrayed waveguide gratings with MMI couplers,” Opt. Express 9, 328-338 (2001).

КОРРЕКЦИЯ КЛАССИФИЦИРОВАННЫХ ЗАВИСИМЫХ ОШИБОК ЦИКЛИЧЕСКИМИ БЧХ-КОДАМИ

А.В. Шкилёнок

В работе [1] была проведена классификация случайных ошибок для циклических БЧХ-кодов. Было выявлено, что для уменьшения сложности селектора при построении декодера все многократные случайные ошибки в соответствии с их диаметрами следует разделить на типичные и нетипичные и осуществлять их раздельное декодирование. Если провести аналогичную классификацию для однократных зависимых (модульных и пакетных) ошибок, то, очевидно, что все они являются типичными. Следовательно, исправлять их можно аналогично типичным случайным ошибкам. Коррекцию ошибок можно осуществлять как декодером с модификацией синдромов, так и без нее. Более того, построение декодера однократных зависимых ошибок будет существенно проще, поскольку не требуются селекция и исправление нетипичных ошибок.

Известно, что для коррекции одиночных пакетных ошибок широкое применение на практике нашли коды Файра, которые являются лучшими из известных высокоскоростных циклических кодов, исправляющих одиночные пакеты ошибок. Они задаются полиномами вида $g(x)=(x^{2t-1}-1)\cdot p(x)$, где $p(x)$ — примитивный многочлен над $GF(q)$, t — кратность корректируемых ошибок. Достоинством декодера кодов Файра для коррекции одиночных пакетов ошибок является простота его реализации [2]. Основными недостатками кодов Файра являются достаточно большая длина кодов и как следствие значительные временные затраты при их декодировании. Длина кодов Файра строго определяется длиной исправляемого пакета ошибок p и порождающим полиномом $g(x)$. Если при решении прикладных задач требуется укоротить код, то применяют укороченные коды Файра с модификацией схемы декодера [3], что приводит к значительному повышению аппаратных затрат на реализацию устройств декодирования данных кодов.

Для исправления одиночных зависимых ошибок предлагается использовать декодер БЧХ-кодов без модификации синдромов, который при обнаружении селектором корректируемой ошибки, будет посимвольно выводить синдром ошибки

на корректирующий сумматор по модулю два аналогично декодеру кодов Файра. Следует отметить, что делитель предлагаемого декодера будет проще, поскольку БЧХ-коды обладают меньшей длиной (проверочный полином короче — поэтому для построения требуется меньше элементов). БЧХ-коды обладают сопоставимыми с кодами Файра избыточностью и возможностями по коррекции зависимых ошибок.

Литература

1. Шкиленок А.В. Конопелько В.К. // Докл. БГУИР. 2007. №2. С. 12–18.
2. Огнев И.В., Сарычев К.Ф. Надежность запоминающих устройств. М., 1988.
3. Вернер М. Основы теории кодирования. М., 2006.

СПОСОБ ЭФФЕКТИВНОЙ ЗАЩИТЫ ЦИФРОВОЙ АУДИОИНФОРМАЦИИ

И.И. Чёрная, А.Н. Коляда

Современный этап развития техники передачи информации характеризуется использованием цифровых методов передачи буквально для всех видов информации, в том числе для звуковой информации. Одной из основных проблем в этой области явилась проблема записи звука в цифровой форме. Эта проблема была обусловлена несовершенством аналоговых методов записи, заключающемся в малом динамическом диапазоне записываемых сигналов, неточной передаче частотной характеристики звука, большом уровне нелинейных искажений и собственных шумов. Однако переход к современным цифровым методам передачи и записи звука сталкивается с существенными сложностями в реализации, так как влечет за собой необходимость замены аппаратуры в связи с изменением частоты дискретизации, разрядности, схем коррекции ошибок и т.д.

В докладе рассматривается новый способ записи передачи и защиты звуковой информации, базирующийся на однобитной технологии в отличие от имеющихся в настоящее время многоразрядных цифровых систем передачи.

Однобитная технология предполагает использование дискретизации аналогового сигнала с частотной, многократно превышающей верхнюю граничную частоту сигнала (так называемая "передискретизация"). "Передискретизация" позволяет существенно снизить шумы квантования. Кроме того упрощается аппаратная реализация аналого-цифровых и цифро-аналоговых преобразователей, устройств коммутации и синхронизации.

Важным преимуществом рассматриваемой технологии является устойчивость к ошибкам, так как эффект от каждой ошибки обратно пропорционален коэффициенту передискретизации. Значительно уменьшаются также нелинейные искажения и улучшаются фазовые и частотные характеристики сигнала.

ЗАЩИТА FLASH-НАКОПИТЕЛЕЙ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Э.Э. Шевцов

В настоящее время вирусы и другие виды вредоносного программного обеспечения представляют серьезную угрозу информационной безопасности. Как правило, используя в своей системе только один антивирус невозможно добиться высокой степени защищенности. В связи с этим ведутся разработки различного программного обеспечения для реализации комплексной безопасности.

При рассмотрении способов распространения вредоносного программного обеспечения доказано, что вирусы могут проникнуть из одной закрытой системы в другую только в случае переноса на каком-либо носителе. Ярким примером являются flash-накопители. В связи с этим возникает необходимость при помощи специального

программного обеспечения исключить возможность распространения вредоносных программ таким способом.

Решением данной проблемы может послужить блокировщик записи. Основной целью данной программы является блокировка записи какой-либо информации сторонними процессами операционной системы на flash-накопитель.

Реализация основной функции программы заключается в заполнении всего свободного объема памяти файлом, напоминающим по своей структуре образ. Таким образом, на flash-накопителе в корневом каталоге будут находиться только сам файл-образ и программа, осуществляющая запись.

Главной особенностью всего содержимого является невозможность их модификации либо удаления с этого носителя стандартными способами операционной системы.

В результате всех манипуляций на накопитель попадает только то, что пользователь собирался туда поместить. Интерфейс программы планируется максимально интегрировать с операционной системой, что на данный момент является основным приоритетом при разработке. Таким образом, мы имеем потенциально непреодолимую преграду против распространения вредоносного программного обеспечения.

СКРЫТНАЯ ПЕРЕДАЧА ИНФОРМАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ РАВНОМЕРНЫХ СВЕРТОЧНЫХ КОДОВ

АЛЬ-АЛЕМ АХМЕД САИД, А.И. КОРОЛЁВ

Сверточные коды с алгоритмом порогового декодирования обеспечивают реализацию ряда дополнительных функций при передаче информации по каналу связи без снижения корректирующей способности кода. Максимальную кратность (длину) корректируемых пакетных ошибок обеспечивают равномерные сверточные коды.

Данное свойство равномерных сверточных кодов положено в основу обеспечения скрытной передачи информации. Сущность метода скрытной передачи информации состоит в исскуственном введении при передаче символов кодовой последовательности пакетов ошибок, корректируемых выбранным равномерным сверточным кодом.

В процессе кодирования "особо важной информации" равномерным сверточным кодом в канал связи передаются только проверочные символы, а информационные символы "особо важной информации" заменяются нулевыми символами кратностью, равной длине корректируемого пакета ошибок равномерного сверточного кода.

На приемной стороне переданная нулевая последовательность будет восприниматься канальным декодером как пакет ошибок, который будет исправлен и тем самым будет восстановлена исключенная при передаче "особо важная информация ".

Для повышения скрытности передачи информации, а также исключения на приемной стороне некорректируемых пакетных ошибок, сформированные кодовые символы подвергаются псевдослучайному перемежению.

ВОПРОСЫ СОЗДАНИЯ И ПРИМЕНЕНИЯ ЦВЕТНЫХ ТЕМАТИЧЕСКИХ ФОТОКАРТ

А.А. Кравцов, А.Н. Крючков, В.Ю. Липень, А.В. Тузиков

Объединенный институт проблем информатики НАН Беларуси, г. Минск, Республика Беларусь

В докладе описана технология формирования изображений тематических цветных фотокарт, являющихся новым видом картографической продукции, создаваемой на основе данных аэрокосмической съемки с использованием методов и средств компьютерной графики. Рассматриваются особенности объектового состава и правил оформления фотокарт, ориентированных на различные сферы применения. Анализируются проблемы предоставления картографических информационных услуг, включающих в себя формирование на основании заказа актуальных цифровых описаний фотокарт на заданные заказчиком участки местности и передачу продукции в виде электронных документов и полиграфических тиражей на бумажном носителе.

Введение

Прошедший год для участников Союзной программы "Космос-СГ" был знаменателен тем, что он был годом ее завершения и подготовки к выполнению следующей программы "Космос-НТ". Вторым важным событием явилось проведение "Третьего белорусского космического конгресса", на котором совместно с российскими коллегами был рассмотрен широкий круг проблем по космической тематике и подведены итоги научно-исследовательских работ и внедрений их результатов в рамках "Космос-СГ". На Конгрессе нами был представлен доклад, посвященный проблемам создания и применения фотокарт, как нового вида картографической продукции [1]. Следует отметить, что на стадии развертывания этих работ авторы предоставляли доклад на ТИБО–2006, опубликованный в [2].

Опыт нескольких десятилетий работы специалистов института в области цифровой картографии показывает, что формализация процесса создания традиционной топографической карты является достаточно сложной и трудоемкой задачей. Даже при использовании современных геоинформационных систем (ГИС) доля работ, возлагаемых на профессионального картографа в автоматизированном картоиздательском процессе, остается значительной, что делает выпуск тиражей актуальных топографических карт довольно длительным и дорогостоящим.

Действительно, правила составления и оформления карт, как объекта материальной культуры человечества, формировались на протяжение веков и ориентировались исключительно на данные ручных топографических съемок на местности. Качество карт в значительной мере определялось опытом и искусством картографа. Даже создание электронных карт, сохраняющих частично внешний вид и правила построения традиционных топографических карт, представляет собой достаточно трудоемкий процесс.

Наличие в руках современных специалистов аэрокосмических снимков высокого разрешения и средств определения точных координат объектов местности позволяет с одной стороны создавать массивы цифровых данных, используемых непосредственно для компьютерной навигации или точного наведения подвижных объектов. С другой стороны, современный уровень развития методов и средств компьютерной графики позволяет по новому решать задачу обеспечения пользователей актуальными картографическими материалами, содержащими необходимую им информацию

В работе [3], показано, что создание кадастровых карт по традиционной технологии на основе топографических карт приводит к потере качества из -за того, что находящиеся в обращении топографические карты обновляются крайне редко. Из этого автор делает вывод о целесообразности использования актуальных трансформированных космических снимков в качестве топографической основы кадастровой карты. Еще в большей мере эти выводы справедливы для картографических материалов, используемых при решении задач на местности

подразделениями МЧС и МО, службами экологии, лесного и сельского хозяйства, а также при прокладке маршрутов и управлении летательными аппаратами, включая беспилотные.

Действительно, с использованием методов и средств компьютерной графики можно на основе фотоплана и вспомогательных данных об объектах содержания создавать картографическую продукцию нового вида — цветные фотокарты. В результате выполнения ряда процедур компьютерного синтеза может быть создано цветное изображение фотокарты, на котором принадлежность объектов к конкретным типам элементов содержания передается с помощью цветового тонирования полутоновых площадных участков исходного фотоснимка и воспроизведения в цветах синтезированных изображений линейных объектов, условных знаков и подписей. Подобные фотокарты имеют ряд преимуществ как перед полутоновыми фотопланами, так и перед традиционными топографическими картами.

Следует отметить, что и обработанные средствами ГИС аэрокосмические снимки, и цифровые карты местности, и упомянутые фотокарты могут поставляться потребителям как в цифровом виде, так и на носителях. С другой стороны, эти и иные картографические материалы в различных деловых ситуациях могут являться объектами авторского права, коммерческим продуктом, юридически значимым документом. В связи с этим представляется обоснованным использование современных информационных технологий для того, чтобы разработчик картографического информационного продукта мог удостоверить свое право распоряжения и ответственность за его качество, а заказчик мог подтвердить целостность переданного ему цифрового описания материала. Для этого требуется разработка специальных криптографических процедур, обеспечивающих возможность создания полноценных электронных документов, на которые распространялось бы действие положений Закона Республики Беларусь "Об электронном документе".

Формирование фотопланов на основе аэрокосмических снимков

Одним из важнейших этапов создания фотокарты является формирование фотоплана заданного участка местности, имеющего в общем случае масштаб и плановое положение стандартного листа топографической карты. В обобщенном виде технологию создания фотоплана можно представить в виде последовательности следующих укрупненных процедур: компоновка фотоплана участка из аэрокосмических снимков (трасс съемки), приведение к масштабу и плановому положению листа топографической карты или заданного участка, устранение линейных, угловых и градационных искажений, нанесение сетки, дешифрирование изображения участка с использованием спектрозональных снимков и цифровой карты участка в соответствии с требованиями к фотокарте, регистрация результатов дешифрирования на фотоплане и/или формуляре.

Из указанных видов работ наибольший интерес и сложность представляют задачи дешифрирования. При решении задач оперативного дешифрирования аэрокосмических снимков и генерации картографических изображений используются элементы теории экспертных систем. Разрабатываемые технологии представляют собой совокупность картографических, математических и других правил, обеспечивающих автоматизированное выделение объектов на изображении и их классификации.

Технология синтеза изображения фотокарты с использованием средств компьютерной графики

Последовательность процедур, выполняемых при создании на базе фотоплана цифрового описания цветной фотокарты можно представить следующим образом: нормализация базового полутонового изображения (снимка); нанесение координатной сетки, тонирование площадных объектов; формирование в требуемых цветах линейных объектов; выделение цветом (знаками) локальных объектов; наложение на фотоплан участка картины распределения характеристик местности для создания тематической карты; формирование подписей; формирование зарамочного оформления.

Апробация различных режимов раскраски площадных объектов показала, что по сравнению с вариантом однотонной либо текстурированной заливки площадных объектов, например, леса или населенного пункта, более информативным и наглядным представляется способ тонирования, соответственно зеленым, бежевым или оранжевым цветом полутоновых изображений этих участков. При таком тонировании на крупномасштабном фотоплане остаются визуально различимыми участки густого леса, редколесье, кустарники и луга. В пределах населенных пунктов на крупномасштабных планах представлены отдельные строения, земельные участки, что особенно важно для выполнения работ по оформлению документов о владении (распоряжении) землей либо при составлении тематических туристических карт с социально-культурными объектами.

Были приняты следующие правила раскраски площадных объектов:

– участки местности, покрытые лесом, тонируются зеленым цветом (C80, M0, Y100, K0), с использованием режима наложения слоя "Наложение/Overlay", с помощью инструмента "Заливка/Fill" с разбросом границы 40;

– открытые участки местности, включая поля, тонируются бежевым цветом (C0, M15, Y50, K0), с режимом наложения слоя "Наложение/Overlay" (тонируется все изображение, для единообразия оттенков накладывается поверх остальной тонировки);.

– водная поверхность — синим цветом (C90, M70, Y0, K0), с режимом наложения слоя "Наложение/Overlay", с помощью инструмента "Заливка/Fill" разброс границы 40;

– заболоченная местность — голубым цветом (C90, M70, Y0, K0), с режимом наложения слоя "Наложение/Overlay", с помощью инструмента "Заливка/Fill" с разбросом границы 40;

– населенные пункты — коричневым цветом (C30, M70, Y100, K0), с режимом наложения слоя "Наложение/Overlay", с помощью инструмента "Заливка/Fill" с разбросом границы 40.

При раскраске линейных объектов используются следующие правила тонирования:

– дороги (шоссе) — желтым цветом (C0, M0, Y100, K0) с режимом наложения слоя "Нормальный/Normal" и последующим заданием обводной линии толщиной два-пять пикселей черного цвета с помощью инструмента "Обводная линия/Outline". Необходимая толщина достигается также с помощью инструмента "Обводная линия/Outline" базовым желтым цветом;

– грунтовые дороги — красным цветом (C0, M100, Y100, K0) с режимом наложения слоя "Нормальный/Normal" и последующим заданием обводной линии толщиной два-пять пикселей черного цвета с помощью инструмента "Обводная линия/Outline". Необходимая толщина достигается также с помощью инструмента "Обводная линия/Outline" базовым желтым цветом. Желательно, чтобы толщина линии грунтовых дорог была меньше толщины линии шоссе;

– объекты гидрографии (только реки и ручьи) — синим цветом (C100, M100, Y0, K0) с режимом наложения слоя "Нормальный/Normal". Необходимая толщина достигается с помощью инструмента "Обводная линия/Outline" с использованием базового синего цвета.

Для выделения цветом и/или знаками локальных объектов по выбору заказчика создается библиотека графических примитивов. Возможно применение стандартных топографических обозначений. При наложении на фотоплан участка картины распределения характеристик местности для создания тематической карты по выбору заказчика создается набор градиентов, текстур, штриховок. Желательно формирование контрастных разделительных границ с помощью обводных линий насыщенных оттенков тонирования. При формировании подписей и зарамочного оформления по выбору заказчика возможно применение стандартных топографических систем координат, шрифтов, заголовков и легенд.

Таким образом, выбранные разработчиками состав технологических процедур и требования к составу и качеству изображения тематической фотокарты определяют

возможные варианты организации передачи картматериалов из подсистем, реализующих обработку данных ДЗЗ и формирование цифровых карт местности.

Для представления цифрового описания исходного фотоплана, подлежащего раскрашиванию и нанесению подписей, может использоваться один из растровых форматов типа BMP, TIFF или PCX. Данные форматы воспринимаются в качестве обменных на входе растровой графической системы ADOBE PHOTOSHOP CS2, используемой в процедурах дизайна фотокарты.

Вспомогательные картматериалы, характеризующие принадлежность имеющихся на фотоплане объектов к тому или иному классу элементов содержания, могут быть представлены на входе подсистемы в виде расчлененных по элементам содержания бумажных или электронных копий, а также в виде текстового формуляра (легенды). Более подробно технология изложена в работе [4].

Представление снимков и карт в виде электронных документов

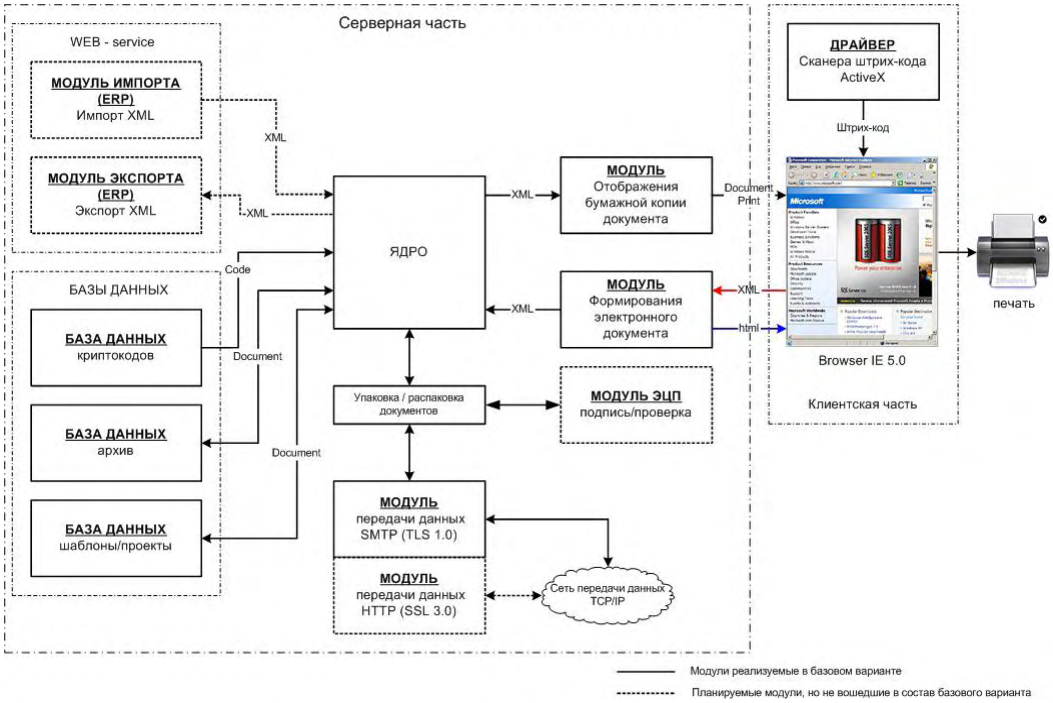
Технология создания и контроля за обращением электронных и бумажных документов разрабатывается в лаборатории компьютерной графики на протяжении ряда лет. Создаваемая в настоящее время версия технологии "Контроль обращения документов (КОД)" планируется, как универсальное средство обработки документов. Однако, попытка распространения подходов, разработанных в первую очередь для текстовых документов, на объемные, сложноструктурированные описания картографических материалов и аэрокосмические снимки сопряжена с необходимостью проведения ряда доработок, направленных на адаптацию универсального комплекса к задачам картографии.

Программно-технический комплекс "КОД" предназначен для создания документов и для контроля их движения в комбинированной среде обращения, в которой осуществляется обмен как бумажными, так и электронными документами.

Подтверждение достоверности электронной версии снимка или карты с помощью электронной цифровой подписи (ЭЦП), а соответствующей бумажной версии — с помощью традиционных реквизитов зарамочного оформления и единого для обеих версий уникального идентификатора, наносимого на бумажную копию в виде штрих-кода, делает обе формы представления документа юридически правомочными и создает условия для их обращения в комбинированной среде.

Структура разрабатываемого комплекса представлена на рисунке. Она является расширенной версией базового варианта, предназначенного для текстовых документов, и состоит из двух частей — серверной и клиентской. Клиентская часть представляет собой браузер IE 5.0 или выше с установленным ActiveX компонентом для работы со сканером штрих-кода. Клиентская часть основана на технологии "тонкий клиент" и требует постоянного подключения к серверу. Клиентская часть позволяет: создавать новые документы, просматривать документы, создавать бумажную копию электронного документа, осуществлять поиск необходимого документа по штрих-коду или реквизитам.

Серверная часть реализует следующие функции: ведение базы данных криптокодов, что позволяет контролировать процесс выдачи уникальных номеров документов и вести их учет; ведение "архива", что позволяет хранить все исходящие и входящие документы, а также осуществлять быстрый поиск документа по его реквизитам или уникальному номеру; создание базы шаблонов и проектов, что позволяет подключать новые типы документов и сохранять промежуточные результаты заполнения форм ввода; передача данных, что позволяет передавать электронные документы через защищенные каналы передачи данных, обеспечивая секретность передаваемой информации; удостоверение электронного документа с помощью ЭЦП, верификация ЭЦП, шифрование/дешифрование электронных документов; формирование формы ввода данных на основе зарегистрированных шаблонов документов и отправка их в web browser; печать бумажной копии документа на основе его XMl-описания. Предлагаемый подход был представлен специалистам по защите информации в докладе [5] и был оценен ими положительно.



Структурная схема сетевого варианта птк "штрих-код"

Заключение

Изложенные результаты исследований позволяют кратко сформулировать предложения авторов относительно путей использования фотокарт, как нового вида картографических материалов и новых информационных технологий, как средства контроля обращения электронных и бумажных документов, в качестве которых аэрокосмические снимки и карты различных типов.

Фотокарты (тематические карты) должны создаваться на основании отдельных заявок профильных пользователей, определяющих плановое положение, масштаб, тираж и другие реквизиты заказа, в соответствии с согласованными требованиями по объектовому составу и правилам оформления. Актуальные фотокарты могут поставляться заказчику в в виде небольших тиражей бумажных копий, изготовленных с помощью цифровых печатающих машин формата А3+ и более или цветного лазерного принтера формата А3.

В случае использования фотокарт в качестве актуальной топографической основы для создания заказчиком собственных тематических карт путем нанесения обстановки, объектов собственности, подписей и т.п., цифровое описание может поставляться в электронном виде. Во всех случаях передачи потребителям информационного продукта в виде обработанных снимков, цифровых карт местности и иных материалов представляется полезным наделение продукции статусом электронного документа, а бумажных копий- статусом внешней формы его представления.

Образцы цветных фотокарт, изготовленные с использованием рассмотренных технологий, представляются докладчиком в виде бумажных копий и компьютерных слайдов. Более полная информация имеется на сайте лаборатории www.uiip.bas-net.by/rus/lab214/project_10.html.

Список литературы

1. Кравцов А.А., Крючков А.Н., Липень В.Ю. и др. // Третий белорусский космический конгресс: материалы конгресса. Минск, Беларусь. 23–25 октября 2007 г. Минск, 2007. С. 230–235.

2. Кравцов А.А., Крючков А.Н., Липень В.Ю. и др. // Технологии информационного общества: Докл. XIII Белорусского конгресса по телекоммуникациям, информационным и банковским технологиям (TIBO). Минск. 4–7 апреля 2006 г. Минск, 2006. С. 148–151.
3. Шавров С.А. // Технологии информационного общества: Докл. XIII Белорусского конгресса по телекоммуникациям, информационным и банковским технологиям (TIBO). Минск. 4–7 апреля 2006 г. Минск, 2006.
4. Кравцов А.А., Крючков А.Н., Липень В.Ю. и др. // Обработка информации и управление в чрезвычайных и экстремальных ситуациях. Пятая междунар. конф. Минск. 24–26 октября 2006 г. Минск, 2006. Т. 2. С. 138–142.
5. Липень В.Ю. и др. // Технические средства защиты информации: материалы V Белорусско-рос. науч.-техн. конф. Минск-Нарочь. 28 мая–1 июня 2007 г. Минск, 2007. С. 16.

БЕЗОПАСНОСТЬ РЕШЕНИЯ КОМБИНАТОРНЫХ ЗАДАЧ НА ЛОКАЛЬНЫХ СЕТЯХ

М.П. РЕВОТЮК, П.М. БАТУРА

Объект рассмотрения — способ противодействия раскрытия смысла задач комбинаторной оптимизации, решаемых по технологии GRID на вычислительных сетях общего назначения. Невозможность на таких сетях физической и логической изоляции программных компонент проблемно-ориентированной системы агентов создает угрозу раскрытия информации о задаче легитимным пользователем рабочей станции.

Однако для многих вычислительно сложных задач комбинаторной оптимизации шаги процесса поиска решения можно естественным образом связать с требованиями основной теоремы безопасности. Для этого достаточно выбрать подходящие приемы грануляции процесса решения и запутывания представления задачи с секретом, назначаемым агентом-диспетчером на рабочей станции.

Например, решение задачи коммивояжера методом ветвей и границ процесса, как известно, наиболее эффективно проводится с ветвлением на множестве линейных задач назначения. Распараллеливание такой задачи в момент появления доступного процессора рекомендуется проводить в узле с минимальным расстоянием от корня дерева. Скрытие параметров и содержания задачи предлагается выполнять случайно генерируемой перестановкой индексов элементов матриц порождаемых подзадач. Это позволяет сохранить преимущества жадного алгоритма загрузки процессоров сети с минимизацией передачи коррелированных данных о подзадачах.

В результате новый агент получает фактически матрицу квадратичной задачи назначения. Так как последняя относится к классу обобщенных задач коммивояжера, то раскрытие описания задачи в узле порождения становится существенно более сложным.

Реализация предлагаемого подхода не исключает стандартных подходов к обеспечению безопасности работы на сетях.

КОНТРОЛЬ ПРОРЫВА АДРЕСНОГО ПРОСТРАНСТВА ПРОЦЕССОВ

М.П. РЕВОТЮК, Ю.М. РЕВОТЮК

Внедрение вредоносного кода в исполняемый процесс в среде Windows NT/2000/XP/2003/Vista базируется на прорыве адресного пространства процесса посредством подключения к процессу динамической подключаемой библиотеки (DLL). Механизм внедрения, например, посредством удаленного порождения потоков не нуждается в наличии на рабочей станции средств отладки, а возможность управляемого подключения к процессу DLL позволяет скрыть любой код.

Однако факт создания потока может быть зарегистрирован, например, на уровне драйвера или даже прикладного процесса. Выявление момента создания потока, причем непосредственно перед активизацией кода его функции, возможно посредством обработки событий DLL_THREAD_ATTACH и DLL_THREAD_DETACH, о которых уведомлена факультативная для любой DLL функция DllEntryPoint.

Используя доступность информации о файле внедряемой DLL, несложно создать для защищаемого процесса агент контроля попыток порождения нерегламентированных потоков. Такой агент, исполняемый в отдельном потоке с максимальным приоритетом и с нулевыми масками доступа, должен создавать слой проверок и установок условий безопасности процесса, а также порождать события аудита. Тело функции агента может быть представлено в отдельной DLL, играющей роль сенсора потоков.

Представленная схема защиты, тем не менее, уязвима к угрозам подключения отладчика на нулевом шаге создания процесса, а также к внедрению DLL через асинхронный вызов процедур (APC) без порождения потоков. Предлагается обнаруживать факт замораживания потоков при отладке динамической системой, образуемой, по меньшей мере, триадой однородных потоков. Любой из потоков должен перевести память процесса в состояние, не подлежащее интерпретации внешнему наблюдателю. Запуск такой системы должен выполняться с секретными параметрами пользователя синхронно с процедурами авторизации и аутентификации.

СИСТЕМА СОПРОВОЖДЕНИЯ ОПТИЧЕСКИ НАБЛЮДАЕМЫХ ОБЪЕКТОВ НА ОСНОВЕ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ

А.В. Шевяков

Современные охранные телевизионные системы представляют собой сложные технические системы, особенностью информационных потоков в которых, в силу природы их формирования, является наличие нечеткости в форме нестохастической объективной размытости. Анализ современных вероятностных методов, применяемых для решения задач привязки изображений, обнаружения и распознавания объектов, локализации мобильных объектов на видеопоследовательностях, позволил сделать вывод о квазиоптимальности любого из них. Существующие методы обладают следующими общими недостатками: относительно высокой размытостью основного корреляционного пика и наличием боковых лепестков, высокой вычислительной сложностью, высокой чувствительностью к уровню постоянной составляющей.

Существующая статистическая теория не способна в значительной степени повысить эффективность подобных систем, в тоже время ряд отечественных и зарубежных ученых исследуют применимость положений теории нечетких множеств в задачах цифровой обработки изображений.

В докладе приведены результаты исследований, направленных на теоретическое обоснование применения теории нечетких множеств при решении задач цифровой обработки изображений. Анализ принципов формирования оптического изображения позволил выявить основные причины возникновения нечеткости и формы ее представления для обработки изображений как совокупности нечетких множеств. Для повышения эффективности систем сопровождения оптически наблюдаемых объектов предложено использовать различные типы расстояний между нечеткими множествами. Для оценки эффективности модифицированной системы разработана математическая модель и программная реализация рассматриваемой системы. Приведены результаты экспериментальных исследований. Отмечено, что замена изображения совокупностью нечетких множеств и использование расстояния между нечеткими множествами позволили использовать не только поле оптического контраста для локализации движущихся объектов, но и вторичную информацию, являющуюся результатом сегментации и обнаружения объектов. В совокупности

предложенный алгоритм позволил получить прирост эффективности системы более чем на 20%, что подтверждается результатами экспериментальных исследований.

АЛГОРИТМ ХАОТИЧЕСКОГО ШИФРОВАНИЯ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СТАТИЧЕСКОГО И ДИНАМИЧЕСКОГО КЛЮЧЕЙ

А.А. Борискевич, И.А. Гордеев

Развитие телекоммуникационных и мультимедийных технологий способствует увеличению потоков информации и вызывает необходимость в создании новых алгоритмов защиты информации от несанкционированного доступа. В данной работе предлагается хаотический алгоритм для защиты мультимедийных данных, основанный на поточном их шифровании с использованием хаотических маскирующих последовательностей, обладающих высокой чувствительностью к ключевой информации (начальным значениям хаотической переменной и управляющему параметру).

Из особенностей разработанного алгоритма следует отметить:

– использование одновременно трех хаотических генераторов, работающих практически независимо друг от друга;

– инициализирующие параметры для генераторов берутся из динамического ключа, который изменяется на каждой итерации алгоритма;

– динамический ключ модифицируется зашифрованным байтом изображения, хаотическими отображениями и элементами статического ключа.

В качестве статического ключа используется md5-хеш ключевого слова, вводимого пользователем. Байты (субключи) хеша выступают в роли инициализирующих параметров динамического ключа.

Проверка качества шифрования выполнялась методом оценки межпиксельной корреляции и чувствительности к модификации одного пикселя исходного изображения. Результаты моделирования хаотического алгоритма на 13 тестовых изображений показали гарантированный уровень их защищенности. Установлено, что межпиксельная корреляция между двумя вертикально смежными пикселями, двумя горизонтально смежными пикселями и двумя по диагонали смежными пикселями зашифрованного изображения составляет порядка 10^{-3} и слабо зависит от используемого хаотического отображения.

ФРАКТАЛЬНО-МОРФОЛОГИЧЕСКИЙ АЛГОРИТМ ПОИСКА ИЗМЕНЕНИЙ НА ЦВЕТНЫХ ИЗОБРАЖЕНИЯХ

А.А. Борискевич, А.А. Односторонцев

В настоящее время данные дистанционного зондирования земной поверхности используются при решении широкого круга задач, таких как оперативный спутниковый контроль природных ресурсов, исследование динамики протекания природных процессов и явлений, анализ причин, прогнозирование возможных последствий и выбора способов предупреждения чрезвычайных ситуаций, получение оперативных разведанных, наполнение и обновление информации в геоинформационных системах. Время обработки и принятия решения возможно сократить в десятки раз, если передавать потребителю не все снимки, а только те, на которых имеются признаки изменений по сравнению с некоторым снимком, считающимся эталонным.

Целью настоящей работы является разработка фрактально-морфологического алгоритма автоматизированного поиска изменений на цветных изображениях,

инвариантного к изменениям условий съемки каждого вновь поступающего на обработку изображения по сравнению с предыдущим.

Сущность предложенного алгоритма состоит в обработки цветных изображений в два этапа: грубый предварительный поиск и уточняющий детальный поиск. На предварительном этапе используется метод анализа фрактальной размерности, позволяющий сократить временные и вычислительные затраты поиска областей изменений на изображениях. На этапе точного поиска используется метод морфологического анализа формы изображения с целью выделения обнаруженных изменений на этапе грубого поиска.

Результаты моделирования в среде программирования Matlab показали, что разработанный алгоритм обладает высокой точностью обнаружения и локализации информации о произошедших изменениях в изображении, а также инвариантностью к изменениям условий съемки.

ЗАЩИТА ИНФОРМАЦИИ КОДОВЫМИ КРИПТОСИСТЕМАМИ НА ОСНОВЕ ТЕОРИИ НОРМ СИНДРОМОВ И СВОЙСТВ ЦИКЛОТОМИЧЕСКОЙ ПЕРЕСТАНОВКИ ЧИСЕЛ

В.К. Конопелько, О.Г. Смолякова

Современные методы защиты информации включают в себя применение кодовых криптосистем с отрытым ключом, использующих порождающую матрицу кода в качестве отрытого ключа. Устойчивость ко взлому таких кодовых криптосистем определяется сложностью синдромного декодирования, то есть так называемой проблемой селектора. С увеличением длины кода и его расстояния сложность декодирования такой криптосистемы возрастает экспоненциально и уменьшить ее для санкционированного пользователя можно применяя при генерации пары "открытый-закрытый ключ" нормы синдромов векторов ошибок кода и их размещение при использовании циклотомической перестановки.

В докладе предлагается вариант кодовой криптосистемы, использующей в качестве открытого ключа специальным образом сконструированную порождающую матрицу кода, а в качестве закрытого — знание норменного циклокласса к которому могут принадлежать нормы синдромов разрешенных векторов ошибок. При кодировании с помощью порождающей матрицы кодовые слова имеют "искусственный дефект", то есть внесенные предумышленно ошибки. Норма синдрома такого кодового слова указывает на норменный циклотомический класс, с помощью которого происходит восстановление информации.

Полученные результаты позволяют конструировать кодовые криптосистемы, в основе которых лежат коды большой длины, увеличивая этим проблему селектора; знание закрытого ключа — норменного циклокласса — позволяет избежать этой проблемы санкционированному пользователю.

ЗАЩИТА СРЕДСТВ АУТЕНТИФИКАЦИИ С ЭЛЕКТРОННЫМ МОДУЛЕМ ОТ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ БОЛЬШОЙ МОЩНОСТИ

Т.В. Борботько, А.Л. Барщевский, С.С. Кузнецов

В настоящее время средства аутентификации с электронным модулем получили широкое распространение. Речь идет об электронных паспортах с использованием радиочастотных меток, различных карт доступа и т.д. Защита данных средств аутентификации от воздействия электромагнитного излучения большой мощности является серьезной проблемой. Для ее решения предлагается использовать многослойный материал, первым слоем которого является влагосодержащий

порошкообразный наполнитель, вторым — фольгированный алюминиевый металлический отражатель, третий слой выполнен из материала аналогичного первому слою. Данный материал может быть использован для создания контейнеров различной конфигурации, в которых будут размещаться средства аутентификации. Вся конструкция помещается в герметичный корпус.

Наличие порошкообразного наполнителя состоящего из влагосодержащих порошков диоксида кремния (SiO_2) и диоксида титана (TiO_2) позволяет сформировать поглощающий слой, имеющий высокие диэлектрические потери в широком диапазоне частот. Внешнее электромагнитное излучение, падающее на данный материал, поглощается за счет его высоких диэлектрических потерь. Поглощение электромагнитного излучения на частотах свыше 25 ГГц обеспечивается его рассеянием на неоднородностях поверхности материала. Процессы поглощения и рассеяния в материале сопровождаются частичным переходом электромагнитной энергии в тепловую. Наличие металлического отражателя за поглощающим слоем позволяет повысить эффективность экранирования конструкции в целом. Расположение за металлическим отражателем в качестве третьего слоя материала аналогичного первому слою позволяет подавить электромагнитную волну, проникшую внутрь контейнера, через стыки стенок конструкции контейнера.

Таким образом, применение данного материала, позволит защитить средства аутентификации с электронным модулем от электромагнитного излучения большой мощности, что определяется многослойной конструкцией и поглощающими свойствами порошкообразного наполнителя.

УСТРОЙСТВО ПОЛНОГО КОПИРОВАНИЯ ИНФОРМАЦИИ С НОСИТЕЛЯ ПРИ ОТСУТСТВИИ ЕЕ МОДИФИКАЦИЙ

С.И. Цыбовский, А.М. Прудник

Сфера высоких технологий создает новые виды преступлений, такие как несанкционированное использование компьютерной информации, компьютерное мошенничество, компьютерный подлог и т.п. В связи с этим все большую актуальность в наши дни приобретают исследования и разработки направленные на борьбу с киберпреступностью, которые могут стать основой для принятия управленческих решений и организации практических мер, необходимых для организации противодействия данному явлению.

Было разработано устройство полного копирования информации с накопиетля на жестких магнитных дисках (НЖМД) при отсутствии ее модификаций. В качестве основы проектируемого устройства был использован микропроцессор CY68013, характеризующийся низкой стоимостью, высокой степенью автоматизации обработки протокола USB, функциональностью и соответствующей ТЗ пропускной способностью при сопряжении интерфейсов USB и ATA. Обработка протокола USB производится микропроцессором автоматически с помощью приемопередатчиков уровня USB 2.0, после чего осуществляется либо передача данных без вмешательства ядра микропроцессора, либо, в случае операций записи в регистр НЖМД, их обработка микропроцессором. Питание микропроцессора CY68013 обеспечивается блоком питания, преобразующим напряжение, подводимое с шины USB. Внешняя микросхема ПЗУ обеспечивает независимость устройства от влияний компьютерной системы.

Данная разработка позволит исключить возможность модификации информации, подлежащей исследованию в процессе судебной компьютерно-технической экспертизы, что является обязательным условием ее успешного проведения.

СЕКЦИЯ 3. ПРОЕКТИРОВАНИЕ И ПРОИЗВОДСТВО ЭЛЕМЕНТОВ И КОМПОНЕНТОВ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

ЦИФРОВАЯ ТЕХНОЛОГИЯ ПОСТРОЕНИЯ СКРЫТЫХ ПИКСЕЛЬГРАММ

В.К. Ероховец, В.В. Ткаченко

Известны два подхода получения голограмм скрытых изображений для голографических защитных элементов: распределенных и локализованных. Как правило, изображения скрытых голограмм являются монохромными, и они формируются аналоговым способом на "голографическом столе". При введении скрытых элементов защиты в голограммы, получаемые цифровыми методами синтеза, приходится прибегать к дополнительным аналоговым технологиям на голографическом столе, что оказывает определяющее внимание на низкую производительность изготовления оригинал-матриц.

Скрытому изображению соответствует относительно простая пиксельграмма некого элемента алфавита или логотипа и представлена в виде матрицы M*ij* с относительно низкой информационной емкостью. Данной матрице соответствует суперпозиция микроскопических дифракционных решеток, записанных вплотную друг к другу, где каждый пиксель изображения формируется своей дифракционной решеткой, осуществляющей коммутацию лазерного пучка в *i*-й столбец и *j*-ю строку матрицы M*ij*, выходной плоскости формирования скрытого изображения. Здесь частотные и азимутальные параметры дифракционных решеток должны быть однозначно связаны с *ij*-адресами матрицы M*ij*. Таким образом, при размере дифракционных решеток ~20 мкм, воспроизводящий лазерный луч с диаметром 1,5 мм одновременно считывает коммутационную матрицу из ~5000 тыс. микроскопических дифракционных решеток, которые строят изображение скрытой пиксельграммы.

Для построения элементарных пиксельграмм используется непараксиальная модель воспроизведения голограммы [1], где справедливы следующие угловые соотношения:

$\sin\alpha=\sin\Theta\cos\varphi$, $\cos\alpha\sin\beta=\sin\Theta\sin\varphi$,

а синтез пиксельграмм выполняется в системе сферических координат. Из этой системы уравнений

$$\sin\Theta_I\cos\varphi_I=\mu(\sin\Theta_{WO}\cos\varphi\,\Theta_{WO}-\sin\Theta_{WR}\cos\varphi_{WR})+\sin\Theta_R\cos\varphi_R;$$

$$\sin\Theta_I\sin\varphi_I=\mu(\sin\Theta_{WO}\sin\varphi\,\Theta_{WO}-\sin\Theta_{WR}\sin\varphi_{WR})+\sin\Theta_R\sin\varphi_R,$$

моделирующих работу голограммы в непараксиальной области, получены условия пространственного разделения изображений при последовательном наложении голограмм путем изменения пространственной ориентации интерференционных плоскостей голограммы.

Литература

1. Борискевич А.А., Ероховец В.К., Ярмош Н.А. // Автометрия. 1987. № 6. С. 3–8.

АКТИВНЫЕ ОПТИКО-ЭЛЕКТРОННЫЕ ДАТЧИКИ СО СВЕТОВОЗВРАЩАЮЩИМИ ЭЛЕМЕНТАМИ

В.К. Ероховец, О.В. Мелех, В.В. Ткаченко, В.В. Шуляк

При необходимости охранять открытую или закрытую территорию с периметром от пяти до тысячи метров чаще всего на практике используются активные оптико-электронные датчики. Датчики включают приемники и передатчики, которые объединены в систему модулированных инфракрасных лучей и настроены на срабатывание при пересечении этих лучей.

В ОИПИ НАН Беларуси разрабатываются активные оптико-электронные датчики и различные их конструкции, отличающиеся высокой стабильностью и надежностью работы. Одна из конструкций основана на использовании световозвращающих элементов, причем оптический излучатель и фотоприемник расположены в непосредственной близости друг около друга, а их излучающая и принимающая поверхности обращены в область контролируемой зоны, где с обратной стороны установлен световозвращающий элемент.

Предлагаемая конструкция в сравнении с конструкцией, в которой передатчик и приемник пространственно разнесены, позволяет снизить требования к параллельности и их коллинеарному сопряжению при сканировании световых пучков в рабочем пространстве.

Таким образом, эта конструкция обеспечивает упрощение устройств в целом за счет установки оптической обратной связи при сканировании рабочего пространства, упрощаются процессы юстировки и диагностики активных оптико-электронных датчиков.

ОЦЕНКА НАДЕЖНОСТИ СИСТЕМЫ ОГРАНИЧЕНИЯ ДОСТУПА

О.В. Мелех, В.В. Ткаченко

Для расчета надежности системы ограничения доступа необходимо учитывать надежность совместной работы всех датчиков используемых в составе системы ограничения доступа. В таком случае разработчики и пользователи могут правильно оценить риски, связанные с использованием той или иной системы контроля доступом и сделать выбор с учетом конкретных условий использования.

В случае охраны периметра предлагается считать главными единичными показателями надежности датчиков вероятность пропуска нарушителя на охраняемый объект и вероятность ложных срабатываний датчика обнаружения. Причем, в зависимости от условий применения системы контроля доступа, значимость этих показателей определяется потребителем.

Предлагаемая методика комплексной оценки надежности системы ограничения доступа позволяет провести сравнительный анализ вариантов системы ограничения доступа и выбрать рациональный для практической реализации с учетом условий применения системы и оперативной обстановки в конкретных ситуациях, когда экономические затраты, являющиеся следствиями пропуска объекта и ложной тревоги, относятся как α_1/α_2. Эта методика также позволяет проводить адекватную оценку показателей надежности и впоследствии может быть использована для оптимизации конструкции, совершенствования схемотехники и алгоритмов функционирования систем ограничения доступа с учетом особых требований к надежности систем, работающих в условиях повышенного уровня внутренних шумов и внешних помех.

ПЕРЕХОДНЫЕ ПРОЦЕССЫ В СТАБИЛИЗИРОВАННЫХ ИСТОЧНИКАХ ПОСТОЯННОГО НАПРЯЖЕНИЯ

С.В. Богомаз, Г.В. Давыдов, В.А. Попов

В докладе рассмотрены переходные процессы в источниках постоянного напряжения устройства защиты речевой информации "Прибой" при включении.

В ходе производства и прогонной проверки, было замечено, что примерно в 1% устройств "Прибоя" при прогонной проверке выходила из строя одна из микросхем стабилизатора напряжения. Причина отказов — импульсное обратное напряжение на стабилизаторе при включении питания сети. Были проведены статистические измерения разницы импульсного напряжения между входом и выходом устройства стабилизации.

Для измерения разницы между входом и выходом стабилизирующего устройства использовался цифровой осциллограф BORDO USB. Предназначенный для исследования периодических и однократных электрических сигналов путем их оцифровки, занесения в память компьютера, отображения на экране монитора и изменения амплитудных и временных параметров.

В докладе анализируются переходные процессы в источниках постоянного напряжения при включении питания сети. Рассмотрена эквивалентная схема стабилизатора с учетом индуктивности электрических конденсаторов и сопротивления.

Выработаны рекомендации по построению стабилизированных источников напряжения и комплектующим элементам электрических схем.

Установлено, что переходной процесс в стабилизаторе напряжения имеет колебательный характер, максимальная амплитуда колебаний напряжения достигала 0,88 В, среднее значение 0,34 В. При изменении параметров сглаживающего фильтра установлено, что уменьшить колебательный характер переходного процесса можно путем правильного подбора емкостей на входе и выходе стабилизатора.

УЛЬТРАЗВУКОВОЕ УСТРОЙСТВО ЗАЩИТЫ НОСИТЕЛЕЙ ИНФОРМАЦИИ

П.В. Камлач, В.М. Бондарик

Носитель информации — строго определенная часть конкретной информационной системы, служащая для промежуточного хранения или передачи информации. Носителем информации является все, что может воспринимать, хранить и передавать информацию.

Носители информации хранятся, как правило, в пространстве ограниченного объема. Для защиты носителей используются устройства, основанные на отражении ультразвука (УЗ). Недостатком таких устройств является наличие "мертвой" зоны порядка нескольких десятков сантиметров. Для защиты носителей находящихся в малом объеме целесообразно использовать устройство, основанное на прохождении УЗ.

При прохождении УЗ колебаний через воздух коэффициент пропускания приблизительно равен коэффициенту затухания в воздухе. При попадании в воздушную среду объекта, характеристики которого отличаются от характеристик воздуха, образуется сложная акустическая система. Коэффициент пропускания в данном случае будет складываться из коэффициента затухания в различных средах и коэффициента отражения при прохождении УЗ через границы раздела сред.

Разработано УЗ устройство защиты носителей информации. Устройство состоит из двух УЗ датчиков, генератора колебаний УЗ (ГКУЗ), микроконтроллера (МК), клавиатуры. Устройство подключается к системе сигнализации. Акустический сигнал

с УЗ датчика проходит сквозь среду и поступает на второй УЗ датчик. Сигнал поступает на АЦП, встроенный в МК. При нажатии кнопки на клавиатуре МК запоминает значение с АЦП. Если носитель информации покинет воздушную среду, то изменятся параметры акустической системы, следовательно, изменится коэффициент пропускания. МК зафиксирует это изменение и включит сигнализацию.

Данное устройство может эффективно работать в малых объемах, таких как сейф, и быть дополнительной защитой для носителей информации.

КОМПЛЕКС ДЛЯ ДИСТАНЦИОННОЙ РЕГИСТРАЦИИ ТРЕМОРА КОНЕЧНОСТИ ЧЕЛОВЕКА

С.К. Дик, А.С. Терех, А.В. Смирнов

Тремор — непроизвольные колебательные движения конечностей человека. Тремор является одним из основных симптомов Болезни Паркинсона (БП). БП является одной из основных проблем пожилых людей.

Существует множество приборов для регистрации тремора конечностей человека (ТКЧ). Начиная от простейших устройств, принцип работы которых основан на способности испытуемых удерживать щуп рукой в рамках некого замкнутого пространства [1], и заканчивая приборами, основанными на использовании различного типа датчиков, закрепляемых на конечностях пациента. Для регистрации тремора в качестве датчиков могут использоваться акселерометры.

Но эти устройства обладают недостатками: наличием на конечности пациента массивных датчиков, которые могут повлиять на точность измерения, а также наличие соединительных проводов между датчиками и остальной частью устройства.

С целью исключения недостатков существующих приборов нами разрабатывается комплекс для регистрации ТКЧ — видеотреморограф, который состоит из четырех блоков: маркера, видеокамеры, ПЭВМ и отображающего устройства (ОУ).

На конечность пациента закрепляется цветной квадратный маркер, изготовленный из липкой бумаги, цвет которого подбирается таким образом, чтобы маркер выделялся на фоне исследуемой конечности человека. Запись движения маркера осуществляет видеокамера.

Поток данных, поступающий с видеокамеры, сохраняется в отдельном файле в памяти ПЭВМ. Обработка видеофайла производится программой, которая определяет координаты маркера на кадре и анализирует его смещение на двух соседних кадрах. В качестве ОУ может использоваться дисплей ПЭВМ. На нем выводится информация о смещении, представленная в виде графиков зависимости колебания ТКЧ во временной и частотной области.

ЭЛЕКТРОМЕХАНИЧЕСКИЕ ПЕРЕКЛЮЧАТЕЛИ

И.Л. Баранов, Б.С. Колосницын, А.С. Тымощик

В настоящее время успехи в технологии микроэлектроники обеспечили получение иммерсионной оптической литографией элементов с минимальными размерами около 30 мкм, а электронно-лучевой литографией — менее 10 нм.

Возможность изготовления таких наноразмерных элементов и использование новых материалов — углеродных нанотрубок и нанопроводов позволяют создавать новые устройства — наномеханические ключи.

Благодаря чрезвычайно малым размерам и массе подвижного электрода, такие ключи при использовании их в качестве элементов хранения информации обеспечат создание механической памяти, которая будет быстрее, дешевле и занимать значительно меньшую площадь, чем современная электронная.

Механическая память может работать, выполняя миллионы и миллиарды циклов в секунду. Механические ключи такой памяти потребляют в миллион раз меньше энергии, чем их электронные аналоги. С их помощью можно создать универсальную память, которая будет сочетать в себе скорость статического ОЗУ (SRAM), низкую стоимость динамического ОЗУ (DRAM) и энергонезависимость флэш-памяти. Новая память обеспечит надежное ее функционирование при воздействии высоких температур, электромагнитных полей и радиации.

МЕТОД ПОВЫШЕНИЯ ЧУВСТВИТЕЛЬНОСТИ ИЗМЕРИТЕЛЕЙ ПАРАМЕТРОВ ВЫСОКОВОЛЬТНЫХ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

А.А. Жданович

Развитие электроники привело к расширению пределов измеряемых токов полупроводниковых приборов. Согласно существующим потребностям измеритель параметров высоковольтных полупроводниковых приборов должен обладать чувствительностью по току до одного пикоампера.

Методы, используемые в известных измерителях параметров высоковольтных п/п приборов, не позволяют достичь требуемых результатов. Их суть заключается в измерении тока, протекающего через шунт, включенный в низковольтную цепь выходного трансформатора источника коллекторного напряжения, соединенную с общим проводом. Такое расположение шунта при измерении малых токов приводит к существенному влиянию помех сети на результат измерения.

Суть нового метода заключается в перенесении шунта в высоковольтную цепь выходного трансформатора источника коллекторного напряжения с использованием гальванической развязки измерителя тока от других частей прибора. Данная мера позволит существенно уменьшить влияние помех сети. Общим проводом для измерителя тока является высоковольтный вывод выходного трансформатора источника коллекторного напряжения. С помощью широкополосного аналого-цифрового преобразователя осуществляется преобразование измеренных мгновенных значений тока в цифровой сигнал. Гальваническая развязка осуществляется по цифровому сигналу с помощью инфракрасных приемо-передатчиков, разнесенных на небольшое расстояние.

Предложенный метод повышения чувствительности позволяет увеличить точность измерения вольт-амперных характеристик высоковольтных полупроводниковых приборов.

РАСШИРЕНИЕ НОМЕНКЛАТУРЫ ЭЛЕМЕНТОВ И КОМПОНЕНТОВ ЗА СЧЕТ МЭМС НА АОА ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Н.И. Мухуров, Г.И. Ефремов, А.С. Мусский

Развитие науки и техники в настоящее время направлено на создание ресурсо- и материалосберегающих устройств, в частности, на разработку микросистем, выполняющих управляющие, контролирующие, регулирующие и др. функции в автоматизации производств. Особое внимание уделяется микросистемам, использующим электростатический принцип актюации, который предопределяет снижение потребляемой электроэнергии и массогабаритных показателей.

Конструктивно устройства состоят из неподвижного (НЭ) и подвижного (ПЭ) разноименно заряженных электродов. При функционировании ПЭ за счет возрастающих при повышении напряжения электростатических сил перемещается к НЭ. Диапазон напряжений 1–100 В. Реализация таких микроэлектромеханических

систем (МЭМС) осуществляется на базе широкого спектра материалов и технологий. Большие перспективы в этом многообразии имеют конструкции, формируемые на анодном оксиде алюминия (АОА) с высокими электромеханическими параметрами. Детали из АОА выполняются с прецизионной точностью, планарной и объемной конфигураций с глухими и сквозными отверстиями, пазами, углублениями. Технологический процесс базируется на интегральных методах и электрохимических операциях выращивания и травления АОА и алюминия и нанесении тонких металлических покрытий. Габариты деталей (не предельные): толщина (0,001–0,2) мм, длина (3–14) мм, ширина (3–10) мм. Созданы МЭМС из АОА плоскопараллельной, консольной, торсионной компоновок с широким диапазоном функциональных возможностей. Применение такого типа элементов и компонентов позволит расширить номенклатуру и повысить надежность систем защиты информации.

МЕТОДИКА ПРОЕКТИРОВАНИЯ МНОГОВХОДОВЫХ ЛОГИЧЕСКИХ ЭЛЕМЕНТОВ С МИНИМАЛЬНОЙ ПЕРЕКЛЮЧАТЕЛЬНОЙ АКТИВНОСТЬЮ

А.И. НАУМОВИЧ

Системы защиты информации, обладающие пониженным энергопотреблением, будут также обладать повышенной отказоустойчивостью из -за более низкой вероятности выхода из строя устройств в условиях повышенных нагрузок. В этом плане одним из перспективных способов проектирования систем пониженного энергопотребления является разработка схем на основе многовходовых логических элементов с минимальной переключательной активностью. Данная задача является NP-полной и требует перебора всех возможных вариантов. В этом случае при большом числе входов значительно увеличивается время работы алгоритма.

Предложена методика, основанная на свойствах функции переключательной активности и того, что вероятности входов всегда меньше 1 и больше 0. Суть методики состоит в том, чтобы построить схему из двух оптимальных частей. Первая часть схемы проектируется из входов, произведения вероятностей которых не больше 0,5. Вторая часть схемы проектируется из оставшихся входов. Каждая часть схемы проектируется на основании синтеза последующего элемента, обладающего наименьшей переключательной активностью на данном этапе. Соединением двух оптимальных частей получается многовходовой логический элемент с минимальной переключательной активностью.

Показано, что данная методика в ряде случаев позволяет получить схемы с меньшей переключательной активностью по сравнению с традиционно используемыми методиками.

ЭЛЕКТРОМАГНИТНЫЙ ВИБРАЦИОННЫЙ ПРЕОБРАЗОВАТЕЛЬ ИНЕРЦИОННОГО ТИПА

С.В. СТАРКОВ, Я.В. КОРОЛЬКОВ

Для защиты речевой информации от утечки по виброакустическому каналу используется метод создания маскирующей помехи в речевом диапазоне частот. Источником помехи служит комбинированный сигнал, состоящий из "белого шума" и речеподобного сигнала с различными соотношениями. Вибрационные преобразователи создают вибрацию в ограничивающих конструкциях в широким диапазоном частот.

Электромагнитные преобразователи по сравнению с пьезоэлектрическими обладают более равномерной АЧХ в области низких частот и обеспечивают большее динамическое значение выталкивающей силы.

Одной из частей преобразователя, оказывающей наибольшее влияние на АЧХ прибора, является упругая уравновешивающая система в виде кольцевых прокладок. В качестве материала для прокладок испытывались резина и алюминий (разных форм и диаметров).

Были исследованы варианты с кольцом из дюралюминия и резиновое кольцо. Также было проведено уменьшение зазора между магнитоводом и мембраной, что привело к увеличению значения динамической выталкивающей силы. Увеличение толщины магнитовода привело к увеличению равномерности АЧХ.

Показано, что упругая уравновешивающая система в виде резинового кольца толщиной 1 мм и минимальный магнитный зазор, обеспечивает наилучшую равномерность АЧХ.

ГИДРОДИНАМИЧЕСКИЕ ОСОБЕННОСТИ ЭЛЕКТРОХИМИЧЕСКОЙ МЕТАЛЛИЗАЦИИ РЕЛЬЕФНЫХ МИКРОПОВЕРХНОСТЕЙ

В.А. Столер

К числу перспективных технологий микроэлектроники, позволяющих создавать рельефные поверхности сложного профиля, относится ультразвуковая (УЗ) технология, связанная с обработкой ультразвуком технологических сред при проведении электрохимических процессов получения тонких пленок металлов. При этом основной акцент ставится на существенное изменение гидродинамики электролита в приповерхностной зоне обрабатываемых тонкопленочных структур микро- и субмикронных размеров.

Учет граничных условий протекания технологического процесса при УЗ обработке электролита дает возможность рассматривать гидродинамическую ситуацию в приповерхностной зоне в зависимости от сложности рельефа обрабатываемой структуры. Так как УЗ воздействие проходило в режиме кавитации, которая сопровождалась турбулентными пульсациями среды и соответствующими потоками, возникающими в результате действия кавитационных полостей, то электролит в рассматриваемой зоне, представляли в виде четырехслойной структуры. Расчеты и анализ ситуации в рассматриваемых слоях с позиций ламинарности и турбулентности потока, показали, что на расстоянии 0,1 мкм вглубь рельефа реализуется ламинарный режим течения пуазейлевского профиля. Рассматривая зависимость потока от коэффициента молекулярной диффузии, и оценивая толщину диффузионного и вязкого пограничных слоев приходим к следующему выводу. При размерах рельефа меньше 1 мкм, кавитационный процесс может инициироваться и влиять на эффекты выравнивания и копирования поверхности при ее металлизации, только при определенном соотношении плотности тока проводимого электрохимического процесса, и давления, совместно создаваемого электрическим и ультразвуковым полем.

Результаты исследований закономерности микрораспределения меди в контрольных точках модельных образцов, позволили установить несколько механизмов воздействия ультразвука на объекты обработки, среди которых определяющим стал кавитационный. Использование выявленных механизмов, дало возможность получать осадки меди на основе пирофосфорнокислого электролита с улучшенными не только геометрическими, но и физико-механическими характеристиками, такими как размер зерна осадка и его микротвердость.

УСТРОЙСТВО ДЛЯ УЛЬТРАЗВУКОВОЙ ОБРАБОТКИ МИКРОСТРУКТУР В ЖИДКОФАЗНОЙ СРЕДЕ

В.А. СТОЛЕР, Д.В. СТОЛЕР

Существенное влияние на успешное развитие микротехнологий может оказать ультразвуковой (УЗ) метод формирования микроструктур, технологический процесс создания которых основывается на жидкофазных химических и электрохимических процессах формирования поверхностей. Положительный эффект от использования УЗ метода может быть получен в результате снятия концентрационно-диффузионных ограничений за счет действия в приповерхностной зоне кавитационных процессов, появления ударных волн концентрированной энергии и формирования устойчивых направленных микропотоков большой скорости.

В то же время, широкое использование ультразвука ограничивается отсутствием соответствующего оборудования, в частности, устройств для ввода УЗ энергии в зону обработки структур микронных размеров. Среди существующих самым эффективным, как показали исследования, является независимый метод возбуждения колебаний на основе многослойного составного преобразователя-концентратора переменного сечения.

Многослойный полуволновой пьезокерамический преобразователь с частотопонижающими накладками представляет собой разъемное соединение в виде четного числа высокочастотных пьезокерамических пластин круглой формы, излучающей дюралевой и отражающей стальной накладок, связанных между собой центральным винтом с определенным усилием. Такая комбинация позволяет получать колебания с частотой излучения в диапазоне 20–180 кГц. Расчет преобразователя осуществлялся с использованием метода синтеза активных и пассивных четырехполюсников.

Стержневой составной концентратор переменного сечения представляет собой трансформатор скорости в виде комбинации цилиндра и катеноиды. Основные расчетные соотношения были получены в результате рассмотрения задачи о продольных колебаниях стержней с переменным поперечным сечением. С учетом граничных условий, была составлена система уравнений, и получены основные параметры составного концентратора: максимальный коэффициент усилия, резонансная частота, длина. Расчет катеноидальной части составного концентратора проводился на компьютере методом последовательных приближений.

Использование разработанного устройства, позволило осуществлять дозированную концентрацию УЗ энергии с большим коэффициентом усиления в малых рабочих объемах, и обеспечило локальную обработка и формирование сложных поверхностей с заданными геометрическими параметрами.

СОКРАЩЕНИЕ ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ ДЛЯ ПОСТРОЕНИЯ ЛИНИЙ АРРЕНИУСА ПУТЕМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИИ СПРАВОЧНИКА О НАДЕЖНОСТИ

В.О. КРОТОВ, Г.В. СЕЧКО

Одним из способов определения длительности электротермотренировки радиоаппаратуры может быть прогнозирование наработки до отказа с помощью линий Аррениуса. Однако построение линии Аррениуса для температур 50-100 градусов Цельсия требует наличия большого объема экспериментальных данных. Сокращение таких данных для построения линий Аррениуса возможно путем использования информации справочника о надежности [1]. Действительно, в [1] сведены воедино данные о наработках до отказа радиоэлементов, которые все научные, в том числе закрытые учреждения науки и техники Советского Союза, собирали несколько

десятилетий. Более крупную базу данных на территории нынешнего СНГ не удалось собрать ни одному исследователю.

Чтобы использовать для построения линий Аррениуса информацию справочника [1], его значения интенсивности отказа необходимо пересчитать в наработку до отказа, учитывая при этом температурный коэффициент нагрузки. Данные коэффициенты приведены в [1] в диапазонах примерно от 20 до 100°С (для одних элементов этот диапазон шире, для других уже) через каждые 10°С. Таким образом, число экспериментальных точек для построения прямой Аррениуса равно 7–9, что намного превышает требуемые три точки для построения любой прямой методом наименьших квадратов.

Литература

1. Надежность изделий электронной техники производственно-технического назначения и народного потребления: Справочник. М., 1983.

ВЛИЯНИЕ ФАКТИЧЕСКОЙ БЕЗОТКАЗНОСТИ КАССОВЫХ СУММИРУЮЩИХ АППАРАТОВ НА ЗАЩИТУ ФИСКАЛЬНЫХ ДАННЫХ

Г.В. Сечко, А.М. Федюкович, П.И. Худик

Основным объектом защиты информации в кассовых суммирующих аппаратах (КСА) являются фискальные данные (ФД) — информация о проведенных на КСА денежных расчетах с населением, необходимая для правильного исчисления налогов и подлежащая ежесменной регистрации и долговременному хранению. Защита ФД по стандарту [1] осуществляется комплексом мероприятий. Одними из них могут быть мероприятия по физической защите оборудования КСА от угроз нарушения безопасности, представляемых окружающей средой. Под названными угрозами понимаются отказы и сбои КСА. В такой трактовке целями безопасности ФД в КСА [2], противостоящими угрозам ее нарушения, являются мероприятия по повышению надежности. Отдельным пунктом среди названных мероприятий стоят наблюдения за работой КСА во время эксплуатации: как записано в стандарте [1, п. 7.2.4] "необходимо регистрировать все подозреваемые и фактические неисправности, все действия по профилактике и ремонту". Такие наблюдения были проведены за работой КСА ВМ8007 (ТАИС.466137.002) разработки и производства МПОВТ. В течение нескольких лет наблюдалась работа 15 экземпляров таких КСА. По результатам наблюдений рассчитаны фактические показатели безотказности аппаратов ВМ8007 — наработка на отказ примерно 2000 ч, интенсивность отказов $5 \cdot 10^{-4}$ ч$^{-1}$. Эти показатели примерно в 3,5 раза хуже проектных, заданных в формуляре ТАИС.466137.002 ФО, что означает фактическую (при эксплуатации) потерю ФД в КСА из -за ненадежности, намного превышающую заданную на этапе проектирования.

Литература

1. СТБ П ИСО/МЭК 17799-2004. Предварительный государственный стандарт Республики Беларусь. Информационные технологии и безопасность. Правила управления информационной безопасностью. Мн., 2004.

2. СТБ 34.101.1-2001 Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. Мн., 2001.

ВЫБОР МАТЕРИАЛОВ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ С УЧЕТОМ МАССОСТОИМОСТНЫХ ПОКАЗАТЕЛЕЙ

Ф.А. Масленников, Т.Г. Таболич, И.С. Терех

В настоящее время предложено много материалов для изготовления экранов электромагнитного излучения (ЭМИ), начало систематическому изучению, которых положено в [1]. К ним относятся силикагель, шунгит, диоксид титана, влагосодержащие материалы и др. При изучении этих материалов основное внимание уделялось защитным характеристикам их от влияния ЭМИ [1]. Однако во многих случаях при выборе материала экрана знание его защитных характеристик является недостаточным, и для квалифицированного выбора материала экрана следует знать показатели массы и показатели стоимости материала. В качестве показателей массы материала в докладе выбрана масса его одного квадратного метра при толщине 2,5 мм. По этому показателю масса одних материалов может превышать массу других в 7 раз. В качестве показателя стоимости материала выбрана отпускная цена его с учетом НДС на территории Республики Беларусь. По этому показателю цена одних материалов превышает цену других также в несколько раз. Следует отметить также, что если масса материала является статическим показателем, то его цена динамически изменяется в зависимости от конъюнктуры рынка.

Литература

1. Лыньков Л.М., Богуш В.А., Глыбин В.П. и др. Гибкие конструкции экранов электромагнитного излучения / под ред. Л.М. Лынькова. Минск, 2000.
2. Колбун Н.В., Фан Н. Занг, Наумович Н.М., Веретенников И.В. // Тез. докл. 5-й Белорусско-российской НТК "Технические средства защиты информации", Нарочь, 28 мая–1 июня 2007 года. Мн., 2007. С. 70–71.

СТАБИЛЬНОСТЬ ОПТИЧЕСКОГО СВЕЧЕНИЯ СВЧ РАЗРЯДА НИЗКОГО ВАКУУМА

С.В. Бордусов, Ю.С. Шинкевич, С.И. Мадвейко

Применительно к задачам технологии производства элементной базы для систем защиты информации существенное значение имеет стабильность плазмы газовых разрядов, т.к. от нее зависит воспроизводимость процесса от цикла к циклу обработки.

Стабильность горения разрядов в атмосфере O_2, CF_4 и смеси с O_2 исследовалась в различном диапазоне давлений и мощностей. Исследовалось поведение одиночных оптических импульсов (форма переднего фронта и вершины, амплитуда, длительность) и группы импульсов (амплитуда отдельных импульсов и наличие закономерностей в их изменениях).

Эксперименты показали, что свечение комбинированного разряда в различных газах в исследуемом диапазоне давлений отличается не только по величине, но и по характеру изменения интенсивности свечения, областям устойчивого горения, соотношениям интенсивностей свечения в областях большего и меньшего вакуума и т.д.

Установлено, что оптические сигналы разряда в кислороде намного стабильнее оптических сигналов разряда в CF_4.

С использованием экспериментальных данных были построены графики функции распределения величины амплитуд импульсов оптического свечения плазмы. Для построения функции распределения выбирались пиковые значения из кривых, которые строились с помощью специализированного программного обеспечения, идущего в комплекте поставки вместе с АЦП. Для построения функции распределения брались амплитудные значения импульсов в разные интервалы времени: в начале процесса, после 30 с горения разряда и после минуты горения разряда. Сами графики

функций распределения строились с помощью MS Excel 2003. Функции распределения подтверждают то, что в O_2 разряд является более стабильным, чем в CF_4 или смеси CF_4+O_2. Функции распределения значений в O_2 имеют вид похожий на нормальный закон распределения случайной величины. Имеет место небольшой разброс значений амплитуд импульсов свечения плазмы, что свидетельствует о стабильности горения разряда.

Высокая стабильность СВЧ разряда в атмосфере кислорода может быть отнесена за счет высокой электроотрицательности этого газа, препятствующей развитию параметрической неустойчивости в объеме плазмы.

Анализируя результаты этих экспериментов, можно сделать следующие выводы:

– с понижением давления воспроизводимость световых сигналов (амплитуда и форма импульсов) во всех газах увеличивается и в области давлений ниже 13,3 Па оптические импульсы характеризуются практически полной повторяемостью;

– с повышением мощности СВЧ колебаний нестабильности горения разряда, выражающаяся в разбросе амплитуд импульсов оптического свечения разряда и неповторяемости формы вершины от импульса к импульсу, возрастает;

– в исследованном диапазоне давлений и мощностей разряд в O_2 характеризуется хорошей повторяемостью светового сигнала.

ИССЛЕДОВАНИЕ ПРОЦЕССА УДАЛЕНИЯ ФОТОРЕЗИСТА В ПЛАЗМЕ КОМБИНИРОВАННОГО РАЗРЯДА

С.В. Бордусов, Ю.С. Шинкевич, С.И. Мадвейко, А.Н. Гусев

В последнее время в процессах производства элементной базы средств защиты информации все чаще используется СВЧ разряд и его модификации. Одной из разновидностей сверхвысокочастотного (СВЧ) разряда является комбинированный разряд, формируемый путем наложения на СВЧ разряд электромагнитного поля низкочастотного (НЧ) или высокочастотного (ВЧ) диапазона, обеспечивающего возбуждение самостоятельного газового разряда. При таком способе поддержания плазмы появляется возможность дополнительного управления энерговкладом в плазменный объем и энергией заряженных плазменных частиц, что в свою очередь существенно изменяет физико-химические процессы в объеме неравновесной плазмы и на границе раздела плазма — твердое тело.

Проводилось изучение влияния внешнего энергетического воздействия низкочастотным полем (f = 10 кГц) на степень химической активности плазмы СВЧ разряда (f = 2,45 ГГц), возбуждаемой в реакторе объемного типа плазмотрона с аппликатором на базе резонатора прямоугольной формы. Исследовался процесс удаления фоторезистивных защитных покрытий с поверхности полупроводниковых пластин диаметром 100 мм.

Исследования проводились с плазмой комбинированного разряда, возбуждаемого следующими способами:

– непрерывным НЧ разрядом и пульсирующим (частота повторения 50 Гц) СВЧ разрядом;

– пульсирующими НЧ и СВЧ разрядами, синхронизированными по длительности и периоду следования.

Экспериментально установлено значительное влияние эффекта возбуждения разночастотного разряда на химическую активность плазмы. При определенных операционных условиях (давление кислорода, величина НЧ напряжения на потенциальном электроде, величина генерируемой СВЧ мощности) скорость удаления сплошной пленки фоторезиста с поверхности одной кремниевой пластины диаметром 100 мм, расположенной в центре реактора перпендикулярно газовому потоку, в комбинированном разряде в 6,5 раз выше, чем в НЧ разряде, и в 1,8 раза выше обработки в СВЧ разряде.

Добавка в основной газ (кислород) аргона (до 10% по объему) способствует повышению скорости процесса удаления фоторезиста по сравнению с обработкой только в кислородном разряда до 1,3 раза в зависимости от остальных операционных параметров. На скорость процесса удаления фоторезиста влияют также местоположение пластины в разрядной зоне и ее температура, количество одновременно обрабатываемых пластин, давление, состав и скорость прокачки плазмообразующей среды, величина напряжения на потенциальном электроде, величина вводимой в резонатор СВЧ мощности.

Основной вывод по результатам исследований заключается в том, что комбинированный разряд обладает преобладающей степенью химической активности по отношению к каждому из типов разряда в отдельности.

МОДЕЛИРОВАНИЕ ТОЧНОСТИ ВЫХОДНЫХ ПАРАМЕТРОВ РЭУ С РАЗЛИЧНЫМИ ЗАКОНАМИ РАСПРЕДЕЛЕНИЯ ПЕРВИЧНЫХ ПАРАМЕТРОВ

Ю.В. Иокуш, С.М. Боровиков

Задача моделирования и исследования выходных параметров радиоэлектронных устройств (РЭУ) является актуальной, так как большинство первичных (входных) параметров, влияющих на выходные, являются случайными. Метод Монте-Карло, называемый также методом статистических испытаний, используется в задачах анализа точности выходных параметров устройств на этапе их проектирования. Моделирование РЭУ позволяет обеспечить требования к точности его выходного параметра, т.к. при моделировании можно варьировать характеристиками точности первичных параметров, выбирая элементы с регламентируемыми производственными допусками. Характеристики точности выходного параметра во многом определяются законами распределения первичных параметров. В работе ставилась задача — выяснить влияние законов распределения первичных параметров на закон распределения выходного параметра. Решение этой задачи позволит более обоснованно определять результирующие характеристики точности исследуемого выходного параметра.

В большинстве случаев первичные параметры имеют нормальный, равновероятностный и экспоненциальный законы распределения. Для решения сформулированной в работе задачи использовалась программа для ЭВМ, реализующая метод Монте-Карло. Разработанная программа позволяет моделировать первичные параметры по следующим законам распределения: нормальному, закону равной вероятности, экспоненциальному и любому другому, задаваемому пользователем. При выполнении исследований выбирались различные законы распределения первичных параметров при одном и том же производственном (технологическом) их разбросе относительно средних значений. Исследования проводились с использованием тестовых математических моделей РЭУ, в качестве которых использовались линейный и квадратичный полиномы.

ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДА ПОРОГОВОЙ ЛОГИКИ С ПОМОЩЬЮ МОДЕЛИРОВАНИЯ ВЫЧИСЛИТЕЛЬНОГО ЭКСПЕРИМЕНТА НА ЭВМ

Е.Н. Шнейдеров, С.М. Боровиков

Эффективность любых методов является определяющим фактором при их выборе для применения. Практическая пригодность метода пороговой логики

для индивидуального прогнозирования параметрической надежности изделий электронной техники определяется не только математическим аппаратом обработки результатов обучающего эксперимента, простотой и оперативностью принятия решения о классе изделия по прогнозирующему правилу (алгоритму прогнозирования), но также вероятностями ошибочных решений, их соответствием допустимым ошибкам. Составляющие эффективности использования этого метода зависят от алгоритма получения решающей функции.

Ставилась задача: используя результаты обучающего эксперимента, исследовать несколько алгоритмов формирования решающей функции в методе пороговой логики и дать ответ на вопрос об эффективности этого метода прогнозирования в зависимости от используемого алгоритма. Кроме того, необходимо было выполнить сравнение по ошибкам прогнозирования предложенных авторами новых алгоритмов в методе пороговой логики с алгоритмами известных методов.

Для решения указанных задач использовался вычислительный эксперимент, выполняемый на ЭВМ. Суть его состояла в моделировании результатов обучающего эксперимента и применении для обработки данных такого эксперимента различных алгоритмов формирования решающей функции. Построение для каждого алгоритма прогнозирующего правила и оценка ошибочных решений, к которым оно может привести, дали ответ на вопрос об их эффективности.

ВЛАГОСОДЕРЖАЩИЕ ДИСПЕРСНЫЕ СИСТЕМЫ ДЛЯ ЭКРАНИРОВАНИЯ ЭМИ С РАЗЛИЧНЫМИ НАПОЛНИТЕЛЯМИ

Н.В. Колбун, Х.М. Альлябад

Вспененные материалы представляют собой грубодисперсные системы, содержащие большое количество микрообъемов воздуха, разделенных тонкими прослойками жидкости. В результате формируется множество границ раздела воздух-жидкость, а общий объем гетерогенного материала существенно превосходит объем содержащейся в нем жидкости, что значительно уменьшает его массу.

Взаимодействие электромагнитного излучения (ЭМИ) с пространственным каркасом жидкости вспененных материалов описывается процессами рассеяния на границах раздела двух сред с различными электромагнитными свойствами. Свойства материалов определяются кратностью пены и составом раствора пенообразующей жидкости и могут быть изменены путем использования различных наполнителей.

Исследования характеристик экранирования ЭМИ влагосодержащих вспененных материалов с различными порошкообразными наполнителями проводились в диапазоне частот 8…11,5 ГГц с использованием панорамного измерителя (КСВН) и ослабления и волноводного измерительного тракта. В качестве наполнителей в высокократную пену вводились мелкодисперсные порошки силикагеля и диоксида титана, обладающие относительно высокой диэлектрической проницаемостью в диапазоне СВЧ.

Измерения показали, что ослабление ЭМИ 2-х миллиметровым слоем вспененной эмульсии составляет 8,5 дБ. Максимальной эффективностью экранирования на уровне 12,1 дБ обладает образец, содержащий порошкообразный силикагель, равномерно распределенный по объему пены с концентрацией 30%. Характеристики отражения ЭМИ вспененными материалами находятся в пределах –7,4…–15,6 дБ.

Применение вспененных влагосодержащих материалов в качестве элементов экранов электромагнитного излучения является перспективным для снижения массы устройства и уменьшения коэффициента отражения ЭМИ.

СТАБИЛИЗАЦИЯ ВЛАГОСОДЕРЖАНИЯ И ЭКРАНИРУЮЩИХ ЭМИ СВОЙСТВ ВЛАГОСОДЕРЖАЩИХ СИЛИКАГЕЛЕВЫХ МАТЕРИАЛОВ

Т.А. Пулко, Н.В. Колбун

Влагосодержащие композиционные материалы на основе капиллярно-пористых матриц (волокнистых, порошкообразных и т.д.) обладают высокой эффективностью экранирования электромагнитного излучения (ЭМИ) диапазона СВЧ, начиная с сотен мегагерц. Однако их применение ограничивается необходимостью герметизации жидкой среды в объеме матрицы. Для этой цели могут применяться полимерные герметизирующие слои, пористые сорбенты, удерживающие влагу на поверхности твердого тела с образованием физических и химических связей. Целью исследований является повышение эффективности экранирования влагосодержащими материалами путем увеличения концентрации влаги в объеме капиллярно-пористой матрицы и стабилизация концентрации жидкости в композитном материале при отсутствии герметизирующих слоев.

Многие безводные соли металлов, например $CaCl_2$, LiBr, $MgCl_2$ и т.д. и их кристаллогидраты активно поглощают воду (до 75–85 г на 100 г сухого композитного сорбента) за счет образования с ее молекулами достаточно жесткой химической связи вследствие взаимодействия молекул воды с ионами диссоциированной соли.

Гравиметрические исследования динамики сорбции влаги гранулированным силикагелем, пропитанным 50 % масс. раствором $CaCl_2$, показали, что при отсутствии герметизации нестабильность влагосодержания композитного материала в течение 10 суток составляет ±9,5% масс.

С использованием панорамного индикатора КСВН и ослабления типа Р2 были исследованы экранирующие свойства образцов в диапазоне частот 8…11,5 ГГц непосредственно после пропитки и через 10 суток. Установлено, что экранирующие характеристики исследуемого композиционного материала не изменились, величина ослабления ЭМИ составила 7,6…7,8 дБ, коэффициента отражения –7,5…–15,5 дБ.

Применение безводных сорбентов на основе солей металлов позволяет существенно повысить стабильность влагосодержания и экранирующих характеристик растворосодержащих композиционных экранов и снизить требования к качеству герметизации или отказаться от ее использования, что значительно повышает эксплуатационные свойства таких экранов.

ЭТАПЫ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Н.В. Колбун, В.В. Аксенов

Проектирование инженерно-технической системы защиты информационного объекта проводится путем системного анализа построения существующей структуры информационного объекта и разработки вариантов, удовлетворяющих требованиям защищенности, путем поэтапного моделирования.

На первом этапе определяются модели объектов защиты с указанием всех источников информации с описанием факторов, влияющих на их безопасность, а также цена защищаемой информации каждого источника.

На основе полученных результатов на этапе моделирования угроз выявляются угрозы безопасности информации, производится оценка ожидаемого от их реализации потенциального ущерба и ранжирование угроз по потенциальному ущербу. Последовательность ранжированных угроз определяет последовательность выбора мер защиты, начиная с наиболее опасных, и учитывая критерий "эффективность-стоимость".

Выбором меры защиты, предотвращающей одну угрозу, завершается одна итерация проектирования системы защиты. После ее завершения корректируются модели объектов защиты и угроз информации. Эти меры виртуально меняют защищенность информации и, соответственно, характеристики угроз ей. Кроме того, при корректировке список угроз сокращается сверху на единицу.

Итерации продолжаются до достижения допустимого уровня безопасности или при превышении выделенного на защиту информации ресурса. При выполнении указанных условий процесс построения (совершенствования) требуемой системы завершается или продолжается с целью определения дополнительного ресурса.

После рассмотрения руководством предлагаемых вариантов (лучше двух для предоставления выбора), учета предложений и замечаний, наилучший, с точки зрения лица, принимающего решения, вариант (проект, предложения) финансируется и реализуется путем проведения необходимых закупок материалов и оборудования, проведения строительно-монтажных работ, наладки средств защиты и сдачи в эксплуатацию системы защиты или ее дополнительных элементов.

РАДИОПОГЛОЩАЮЩИЕ СВОЙСТВА ПОРОШКООБРАЗНОГО ШУНГИТА С ВКЛЮЧЕНИЯМИ МЕДИ, НИКЕЛЯ И КОБАЛЬТА

Е.А. Криштопова

Весьма перспективным представляется создание поглотителей электромагнитного излучения (ЭМИ) на основе природных минералов, достоинствами которых являются доступность и невысокая стоимость. Одним из таких минералов является шунгит, структурно представляющего собой матрицу из глобулярного углерода с включениями аморфного диоксида кремния.

Было экспериментально установлено, что в диапазоне частот 8–12 ГГц значение ослабления ЭМИ слоем порошкообразного шунгита толщиной 2,5 мм составляет 10 дБ, при значении коэффициента отражения –5 дБ. Методом химического восстановления из растворов солей металлов на поверхности частиц исследуемого минерала получены включения меди, никеля и кобальта и их соединения с кремнием. Это позволило повысить значение ослабления ЭМИ слоем порошкообразного шунгита с включениями меди до 16,5 дБ, никеля и кобальта до 17…18 дБ при значениях коэффициента отражения равных соответственно –4 дБ, –3…–3,5 дБ и –2 дБ.

Разница в радиопоглощающих характеристиках химически модифицированного минерала обусловлена выбором осаждаемого металла: вместе с ростом электропроводности, увеличиваются значения ослабления и коэффициента отражения. Этот фактор может быть использован для создания композиционных поглотителей ЭМИ с заданными функциональными характеристиками путем подбора вида металлических включений порошкообразного шунгита, его концентрации и типа связующего.

ПОГЛОТИТЕЛИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ШУНГИТА С ЖИДКОСТНЫМ НАПОЛНИТЕЛЕМ

Е.А. Криштопова, А.Н. Бинжук

Поглотители электромагнитного излучения (ЭМИ) могут быть эффективно использованы для создания технических средств защиты информации от утечки по каналам побочных электромагнитных излучений.

Установлено, что, выбором типа жидкостного наполнителя и величины его содержания в порошкообразном шунгите, можно получить поглотители ЭМИ с заранее заданными величинами коэффициентов передачи и отражения. Пропитка

порошкообразного шунгита водой, которая заполняет капиллярные поры и адсорбируется в виде пленки на поверхности каждой из его частиц, увеличивает электропроводность и диэлектрические потери в объеме синтезированного таким образом материала. При использовании водного раствора NaCl вследствие диссоциации соли на ионы будет получен жидкостные наполнитель с более высокой по сравнению с водой электропроводностью и, соответственно, значением ослаблением ЭМИ.

Для герметизированных полиэтиленом образцов из порошкообразного шунгита толщиной 3 мм экспериментально построена зависимость значений коэффициентов передачи и отражения от типа выбранного жидкостного наполнителя и его концентрации. Показано, что при содержании жидкостного наполнителя в концентрации 15–25% от массы сухого материала, значение коэффициента передачи снижается с –10 дБ до –20 дБ при использовании воды и –24 дБ при использовании водного раствора NaCl. Значение коэффициента отражения снижается с –5 дБ до –3…–3,5 дБ по сравнению с сухим материалом. При дальнейшем росте концентрации жидкостного наполнителя в объеме образца происходит резкое увеличение коэффициента отражения при неизменном значении коэффициента передачи.

МЕТОДИКА ИЗМЕРЕНИЯ ЭЛЕКТРИЧЕСКИХ ПАРАМЕТРОВ НЕЛИНЕЙНЫХ ДВУХПОЛЮСНИКОВ

Б.С. Колосницын, И.Л. Баранов

Для измерения электрических параметров тонкопленочных переключателей был разработан характериограф с учетом следующих характерных особенностей нелинейных двухполюсников:

1. Большинство двухполюсников обладает активной и реактивной составляющей комплексной проводимости. Для экспериментального исследования этих составляющих широко используются мостовые методы, метод синхронного детектирования и резонансные методы. В основу разрабатываемого устройства нами был положен известный метод компенсации одной из составляющих проводимости и измерения другой.

2. Специфика изготовления тонкопленочных переключающих элементов связана с присутствием тонких (до 5…10 нм) диэлектрических слоев через которые механизмы эмиссии электронов подчиняются определенным законам. Когда толщина диэлектрика мала (в D<5 нм), происходит туннелирование электронов через диэлектрик, описываемое соотношением j~exp (α/U), где j — плотность тока, U — прикладное напряжение, α — коэффициент. При больших толщинах диэлектрика зависимость плотности тока от прикладного напряжения: j~exp (βγ/U).

3. В случае контакта металл-полупроводник эта зависимость представляется выражением: j~exp (γ/U). В реальных приборах могут присутствовать все три механизма протекания тока через диэлектрик. Поэтому разумно представить результаты измерения в виде кривых в соответствующих координатах (I, ln|, U, 1/U), а характериограф должен включать в себя устройства, позволяющие реализовать указанные соотношения.

КОМПОЗИЦИОННЫЕ МЕТАЛЛОСОДЕРЖАЩИЕ МАТЕРИАЛЫ ДЛЯ ШИРОКОПОЛОСНЫХ ПОГЛОТИТЕЛЕЙ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Л.Г. Литвин, В.А. Богуш

В современных условиях функционирования различных информационных систем актуальной является тематика, связанная с разработкой электромагнитных экранов со сниженными массогабаритными характеристиками и уменьшенным коэффициентом отражения электромагнитной волны (ЭМВ) при обеспечении высокой эффективности в широком диапазоне частот. Использование наноструктурированных композитов является перспективным направлением создания новых материалов, подавляющих электромагнитное излучение.

Установлено, что метод химического осаждение никеля и кобальта из водных растворов их солей на поверхность волокнистого полиакрилонитрила, включающий сорбцию ионов металлов в волокне с их последующим восстановлением, приводит к формированию композиционных металлосодержащих материалов. Измерения ослабления ЭМВ образцами показали, что эффективность таких экранов составляет в среднем 15 дБ в диапазоне частот от 8 до 12 ГГц близким к 1 и уменьшающимся до 0,77 с увеличением частоты.

Известно, что полиакрилонитрильные волокна обладают плохой смачиваемостью и, соответственно, плохой адгезией частиц металлов на поверхности волокон, поэтому решено проводить предварительное модифицирование образцов раствором гидроксиламина и серной кислоты. Материалы, полученные осаждением никеля и кобальта из водных растворов их солей после предварительного модифицирования волокон, обладают лучшими экранирующими свойствами. Экспериментально показано, что коэффициент отражения для кобальтсодержащих волокон составляет от –3 до –11 дБ, а коэффициент передачи, обратно пропорциональный общей эффективности экранирования — от –6 до –18 дБ. Коэффициент отражения для никельсодержащих волокон составляет от –4 до –10 дБ, а коэффициент передачи — от –5 до –15 дБ в диапазоне частот от 8 до 12 ГГц.

Полученные материалы перспективны для использования в конструкциях широкополосных поглотителей электромагнитного излучения.

МИКРОТОПЛИВНЫЕ ЭЛЕМЕНТЫ НА ОСНОВЕ ПОРИСТОГО КРЕМНИЯ

В.Ф. Алексеев, С.А. Волчёк, А.А. Прошкина

Источники питания на микротопливных элементах способны заменить литий-ионные портативные источники питания. При их разработке учитываются главные характеристики: параметры удельной мощности на единицу объема и веса, толщина элемента, его масса, а также стабильность работы, экологическая безопасность. Микротопливные элементы (МТЭ) на основе пористого кремния являются весьма перспективным направлением в создании МТЭ, так как существует мощная индустрия интегральных схем с базовыми процессами, которые хорошо сочетаются с методами микромеханики и получением пористого материала.

Пористый кремний получают с помощью электрохимического травления в электролитах, содержащих плавиковую кислоту. В зависимости от пористости различают макро-, мезо- и микропористый кремний. Удельная площадь поверхности кремния разной пористости меняется от 0,1 до 600 $м^2/см^3$, а удельная электропроводность — от ~1 до 10^{-14} Ом/см. Это означает, что из одного и того же материала можно изготовить электроды мембранно-электродной сборки с малым сопротивлением для электронов, газодиффузионные слои с хорошо развитой поверхностью реакции и диэлектрический каркас для протонпроводящей мембраны.

Процесс изготовления макропористых слоев кремния имеет ряд особенностей: электрохимическое травление (анодирование) кремния в растворе плавиковой кислоты; "вскрытие пор" для получения пластины со сквозными каналами; аттестация пористых кремниевых слоев, т.е. характеризация образцов по таким параметрам, как общая и удельная площади внутренней поверхности пористой части кремниевого электрода.

ШИРОКОПОЛОСНЫЙ РАДИОПОГЛОЩАЮЩИЙ МАТЕРИАЛ

В.Б. Соколов, С.Э. Саванович

Предлагается использовать для создания высокоэффективных широкополосных композиционных радиопоглощающих материалов полимерную композицию, содержащую в качестве основной поглощающей компоненты титанат бария, который благодаря высокой диэлектрической проницаемости в СВЧ-диапазоне обладает высокими показателями поглощения ЭМИ в широком частотном диапазоне. Дополнительными компонентами композиции являются присадки, существенно влияющими на физические, и в частности, электрические свойства радиопоглощающего материала. В качестве присадок использовались тонкодисперсные порошки (5–12 мкм) силикагеля и углерода. Связующим в данной композиции является полимерно-каучуковая основа. Композиция фиксируется на поверхности матрицы из волокнистого наноканального минерала водного силиката магния $Mg_3Si_2O_5(OH)_4$.

Целью работы являлось изучение зависимостей поглощения и отражения ЭМИ композиционным материалом на основе наноканальной матрицы с добавками титаната бария, силикагеля и углерода в полимерно-каучуковом связующем.

Экранирующие свойства композиции измерялись в частотном диапазоне 8…11,5ГГц. Ослабление ЭМИ измерялось только для образцов без металлического отражателя, который существенно увеличивает общую эффективность экранирования (свыше 40 дБ).

Установлено что слой композиционного материала толщиной 1–5 мм создает ослабление порядка 6–12 дБ при величине отражаемой энергии от –14÷–28 дБ. Отражение электромагнитной энергии снижается при использовании фольгового отражателя. Снижение уровня отражения обусловлено улучшенным согласованием с волновым сопротивлением свободного пространства за счет создания градиента диэлектрической проницаемости по толщине образца. Использование описанного композиционного материала позволяет создавать поглотители ЭМИ с повышенной эффективностью и расширенным диапазоном частот за счет высоких диэлектрических потерь в композиции и переотражения ЭМИ от границ раздела.

ИССЛЕДОВАНИЕ РАДИОПОГЛОЩАЮЩИХ СВОЙСТВ НАНОКАНАЛЬНОГО ВОЛОКНИСТОГО МАТЕРИАЛА

В.Б. Соколов

Наиболее распространенным видом радиопоглощающих материалов (РПМ) являются композиционные материалы, синтезированные на основе различных волокнистых матриц. При этом основной проблемой является надежная фиксация входящих в композицию активных составляющих на несущей матрице. С этой целью широко применяются различные способы фиксации и герметизации. Весьма перспективным материалом для несущей матрицы, позволяющем фиксировать как твердые, так и жидкие составляющие композиции является волокнистый наноканальный минерал водного силиката магния $Mg_3Si_2O_5(OH)_4$. Целью

исследований является оценка эффективности радиопоглощающих свойств водного силиката магния и пригодности его в качестве несущей матрицы для синтеза композиционных РПМ.

Исследуемый материал представляет собой волокнистую структуру из плотно упакованных трубчатых волокон с внешним диаметром 300–500 Å, и внутренним диаметром 20–150 Å.Пористость материала (объем каналов к общему объему) составляет 5–6%, причем внутренние объемы каналов заполнены "связанной водой", удаление которой весьма проблематично, т.к. требует длительного отжига при температурах превышающих 150°С.

Для определения эффективности радиопоглощения проводились измерения коэффициента стоячей волны по напряжению (КСВН) подготовленных образцов. Для инструментального определения КСВН экспериментальных образцов использовался измерительный комплекс, в состав которого входили генератор РГ4-14, анализатор Я2Р-70 и волноводная линия. Измерения КСВН проводились в диапазоне частот 8–12ГГц, с учетом возможности дальнейшего применения исследуемого материала.

Установлено, что волокнистый наноканальный материал толщиной 2,5 мм обладает КСВН в пределах 1,4–2,3.

ГИБКИЕ ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ С ВЛАГОСОДЕРЖАЩИМИ И СУХИМИ ГЕЛЕВО-ПОРОШКОВЫМИ НАПОЛНИТЕЛЯМИ

С.В. Головатая, О.И. Зубаревич, А.А. Позняк

Для снижения радиолокационной заметности и дальности обнаружения металлических объектов на них устанавливают маскирующие радиопоглощающие материалы (РПМ); в результате, сигнал, отражаемый от металлических поверхностей, преобразуется и становится близок к фону окружающей среды. В качестве таких РПМ исследовали полиакрилонитрильное полотно толщиной 2 мм с влагосодержащими и сухими гелево-порошковыми наполнителями [1]. Для получения сухих образцов некоторые влагонаполненные образцы не герметизировали, а подвергали полному высушиванию в термостатированном сушильном шкафу при температуре 55°С. Исследования проводили в частотном диапазоне 8–12 ГГц.

Анализ показал, что экранирующие свойства образцов при высыхании не сохраняются, что обусловлено определяющим влиянием воды на подавление электромагнитного излучения (ЭМИ). Резко увеличивается коэффициент передачи ЭМИ и становится даже большим, чем у текстильной матрицы без какого-либо наполнителя. Это говорит о том, что сухой наполнитель выступает в качестве проводящего ЭМИ материала. Коэффициент отражения у всех образцов очень мал и не представляет интереса.

Особое внимание нужно уделить показателям отражения образцов, стоящих на пути распространения ЭМИ непосредственно перед металлической поверхностью. По полученным данным коэффициентов отражения с отражающей поверхностью влагонаполненнных и сухих образцов составлена таблица, из которой хорошо видно, как изменяется этот показатель при полном высыхании экспериментального образца (в таблице приведены усредненные по частоте значения $S11_{отр.\ ср.}$).

Из таблицы видно, что высушенные образцы с наполнителями на основе гелей имеют более низкие коэффициенты отражения с отражающей поверхностью ($S11_{отр.}$), чем аналогичные образцы, не подвергавшиеся высушиванию, и чем текстильная матрица без наполнителя ($S11_{отр.\ ср.}$ –3,5 дБ). Исключением стал лишь образец с наполнителем из смеси желатина и ZrO_2, который во влагонаполненном состоянии показал наибольшее поглощение ($S11_{отр.}$ –8 дБ). А из сухих образцов самое низкое

отражение имеет текстильная матрица с наполнителем из смеси диоксида циркония и ПВС ($S11_{отр.}$ до –6,9 дБ).

Значения среднего коэффициента отражения $S11_{отр.\ ср.}$ для различных РПМ

Наполнитель		Поливиниловый спирт (ПВС)			Крахмал		Желатин			Обойный клей	
		TiO_2	ZrO_2	Шунгит	TiO_2	Шунгит	TiO_2	ZrO_2	Шунгит	Без добавок	Шунгит
$S11_{отр.\ ср.}$	влагосодержащий	–4,5	–5,6	–2,9	–3,2	–1,9	–2,8	–7,0	–2,4	–2,1	–1,6
	сухой	–5,2	–6,1	–4,3	–4,3	–5,0	–4,2	–4,1	–4,0	–3,6	–4,6

Так как высушенные образцы практически не потеряли своей гибкости и цельности, не требуют герметизации, более удобны в применении и имеют меньший удельный вес, чем влагосодержащие полотна, то именно сухие композиционные материалы наиболее перспективны в качестве радиопоглощающих покрытий для металлических объектов в исследуемом диапазоне частот.

Литература

1. Головатая С.В., Зубаревич О.И., Позняк А.А. // Технические средства защиты информации: материалы докладов и краткие сообщения V Белорусско-российской НТК. Минск, 28 мая – 1 июня 2007 г. Минск, 2007. С. 74–75.

ИССЛЕДОВАНИЕ ЭКРАНИРУЮЩИХ СВОЙСТВ МАТЕРИАЛОВ НА ОСНОВЕ ГИДРОГЕЛЯ

Ю.В. Смирнов

Гидрогель — это новое поколение материалов, обладающих способностью поглощать и удерживать до 2-х л жидкости на 10 г гидрогеля или около 0,11 л питательного раствора на 1 г препарата. Гидрогель стерилен и нетоксичен, сохраняет свои свойства при высоких и низких температурах.

В работе исследовались изменения экранирующих свойств гидрогеля с различными наполнителями в зависимости от содержания щелочных и кислых пропитывающих жидкостей. В качестве пропитывающей жидкости для гидрогеля использовались вода с 10% раствором соды и вода с 7% раствором уксуса в соотношении 1:1. Гидрогель помещался в пропитывающую жидкость, затем производилась герметизация образцов при помощи полиэтиленовых пленок.

Получено, что увеличение в объеме гидрогеля в растворе соды в 7 раза выше, чем в уксусном растворе. Коэффициент ослабления в растворе соды в диапазоне частот от 8 до 12 ГГц колеблется от 16 до 23 дБ, а коэффициент отражения от 3,4 до 4,5 дБ. Коэффициент ослабления в уксусном растворе в диапазоне частот 8–12 ГГц колеблется от 6 до 9 дБ, а коэффициент отражения от 3,6 до 5 дБ.

Из результатов видно, что в щелочном растворе гидрогель впитывает жидкость намного эффективнее, чем в кислом, и имеет лучшие характеристики коэффициентов отражения и ослабления.

ИЗУЧЕНИЕ МОРФОЛОГИИ ПОВЕРХНОСТИ УГЛЕРОДНЫХ ВОЛОКОН, ОБРАБОТАННЫХ НАПРАВЛЕННЫМ ПОТОКОМ ИОНОВ

Д.А. Котов, В.И. Дубкова, А.Г. Флерко

Полимерные волокнистые материалы (элементарные волокна, нити, пряди, жгуты войлок, ткани) широко используются в качестве упрочняющего наполнителя композиционных материалов, а также как основа для гибких экранов электромагнитного излучения. И к армирующим наполнителям и к гибкой основе, помимо прочностных показателей, предъявляют требования повышенной адгезии к связующей матрице или тонкопленочным слоям формируемым с целью обеспечения различных функциональных свойств, например, малой или высокой теплопроводности, эрозионной стойкости, защиты от электромагнитных излучений и др. Для этих целей волокнистые материалы подвергаются различным видам обработки, из которых наиболее перспективной как с точки зрения увеличения прочности на границе раздела фаз, так и придания функциональных свойств композиционному материалу является модификация поверхности волокон направленными ионными и плазменными потоками, которые позволяют изменять химические и/или физические параметры и свойства поверхности.

В работе представлены результаты исследования влияния параметров процесса ионно-лучевой обработки: энергии ионов, плотности ионного тока и угол падения ионов на изменения морфологии поверхности углеродного волокна. Показаны зависимости характеристик нанорельефа от параметров технологического процесса обработки. Установлены факторы, которые являются определяющими для изменения рельефа поверхности углеродного волокна по глубине и равномерности обработки.

ИССЛЕДОВАНИЕ УГЛОВЫХ ЗАВИСИМОСТЕЙ ОПТИЧЕСКИХ ХАРАКТЕРИСТИК МАТЕРИАЛОВ ДЛЯ ЭКРАНОВ ЭМИ ВИДИМОГО ДИАПАЗОНА ДЛИН ВОЛН

М.С. Павлович

Работа посвящена созданию композиционного материала, позволяющего имитировать спектрально-поляризационные характеристики растительности, и изучению угловых зависимостей степени поляризации и спектрального коэффициента яркости (СКЯ) излучения, отраженного от растительности (образец 1 — одиночный живой лист) и синтезированного материала (образец 2 — молотый сухой лист, закрепленный в связующем компоненте). Для исследования угловых зависимостей СКЯ и степени поляризации были выбраны три информативных спектральных интервала: 550–560 нм, что соответствует максимуму спектральной чувствительности человеческого глаза, 680...690 нм — полоса поглощения хлорофилла, 680...690 нм — максимум в спектрах отражения зеленой растительности.

Установлено, что в исследуемых диапазонах яркость излучения, отраженного образцами 1 и 2, практически одинакова при малых углах наблюдения (β=0–30°, углы наблюдения отсчитывались от нормали к плоскости исследуемого объекта через 10°). Для β=40–70°СКЯ композиционного материала становится больше СКЯ растительности на значение не более 1,5. Показано, что в диапазонах 550...560 и 780...790 нм наибольшее превышение степени поляризации излучения, отраженного образцом 2 по отношению к степени поляризации излучения, отраженного растительностью, наблюдается для β=30–60° и не превышает значения 0,1. В диапазоне 680...690 нм данная разница не превышает значения 0,02 для всех β.

Таким образом, композиционный материал на основе молотого сухого листа, закрепленного в связующем компоненте можно использовать для создания экранов, снижающих заметность объектов на фоне растительности.

СЕКЦИЯ 4. ОРГАНИЗАЦИОННО-ПРАВОВОЕ, МЕТОДОЛОГИЧЕСКОЕ И ОБРАЗОВАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

АСПЕКТЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ

М.П. Батура, Л.М. Лыньков

Современные телекоммуникационные технологии широко применяются в различных сферах человеческой деятельности: промышленности, науке, быту, финансовых организациях, управлении и др. Во многих случаях информация, обрабатываемая телекоммуникационными системами, носит конфиденциальный характер. В настоящее время на рынке появляются новые технологии и оборудование для защиты информации, многие производители телекоммуникационного оборудования вводят функции, обеспечивающие информационную безопасность, в серийные устройства. Развитие технологий защиты информации идет очень высокими темпами, и в системе высшего образования необходимо обеспечить высокий уровень подготовки специалистов, способных с одной стороны эффективно обслуживать и эксплуатировать современные телекоммуникационные системы и устройства защиты информации, а с другой стороны разрабатывать и совершенствовать алгоритмы, устройства и системы информационной безопасности.

В связи с этим разрабатывается комплекс программных средств для реализации возможности обучения и тестирования студентов по всем разделам защиты информации. В этом комплексе представлены основные компоненты теоретических, методологических, организационных и технических сторон защиты информации.

Данная работа предназначена для обучения студентов физическим, аппаратным, программным, криптографическим, техническим средствам и методам защиты информации. Кроме того, данная программа может быть использована для дистанционного обучения.

Основное содержимое создаваемого электронного учебного пособия основывается на следующих блоках дисциплин:

– основы организационно-правового обеспечения информационной безопасности и теоретические основы защиты информации;
– криптографическая защита информации;
– защита информации в информационно-вычислительных системах;
– защита программного обеспечения и баз данных;
– защищенные телекоммуникационные системы;
– защита речевых сообщений от несанкционированного перехвата;
– защита информации в банковских технологиях;
– защита объектов связи от несанкционированного доступа.

По каждому из выше указанных блоков дисциплин создается учебно-лабораторный комплекс, в котором лабораторная и лабораторно-практическая работа выполняется на специальном обучающем программном обеспечении или с использованием соответствующего технического средства, учитывая последние научные и производственные достижения в сфере информационной безопасности.

Для всех специальностей БГУИР введен общий курс "Основы защиты информации". Дисциплина носит не только ознакомительный характер, но и ставит задачу проведения лабораторно-практических занятий.

На данный момент в БГУИР в учебном процессе используется комплекс программно-аппаратных лабораторных работ по защите информации от утечки по техническим каналам, прикладной криптографии, защите объектов связи

от несанкционированного доступа, защите информации в банковских технологиях организованных по описанным выше принципам. Для контроля знаний студентов применяются компьютерные программы, содержащие информацию описательного характера и систему оценки знаний (коллоквиумы).

Основным достоинством разрабатываемого унифицированного учебного комплекса является его возможность использования в качестве базового для формирования содержания новых дисциплин по основам информационной безопасности по смежным специальностям.

В БГУИР с 2006 г. начата подготовка магистров по специальности "Методы и средства защиты информации. Информационная безопасность", где выпускники вузов смогут получить степень магистра технических наук в области защиты информации. Особенности подготовки магистров связаны с введением в программу обучения дополнительно к курсам по современным телекоммуникационным технологиям и компьютерным сетям различных системных и методологических дисциплин, таких как "Организационно-правовое и методологическое обеспечение безопасности", а также специальных дисциплин по организации научных исследований, проектированию и эксплуатации технических средств защиты информации и защищенных объектов.

Подготовка специалистов осуществляется на кафедре защиты информации, обеспеченной высококвалифицированным профессорско-преподавательским составом, насчитывающим 6 докторов наук, профессоров и 6 кандидатов наук. Кафедра имеет современное компьютерное оборудование для проведения модельных расчетов и экспериментальных исследований, тесно сотрудничает с предприятиями и научно-исследовательскими институтами республики. Научная тематика магистерских диссертаций связана с разработкой новых алгоритмов, материалов, комплексных интегральных систем защиты, что позволяет удовлетворять растущие требования по подготовке специалистов, и формирует необходимую образовательную и научную базу для дальнейшего повышения квалификации в аспирантуре.

В НИЧ БГУИР ведутся исследования в сфере защите информации. Так, например, разработаны устройства защиты информации от утечки по вибрационному каналу, использующие в качестве маскирующих сигналов белый шум и речеподобные сигналы. Уровень маскирующего сигнала, который поступает от такого устройства на преобразователи и изменяется динамически с изменением уровня речевого сигнала в защищаемом помещении, что значительно снижает шумовое воздействие на самого человека, работающего в данном помещении, сохраняя при этом высокие показатели защищенности. В данной лаборатории также ведутся работы по исследованию и разработки новых материалов, поглощающих электромагнитное излучение в широком диапазоне частот. Такие материалы могут использоваться в защитных конструкциях, снижающих уровень побочных электромагнитных излучений и наводок противодействуя перехвату информации по электромагнитному каналу, кроме того, использование таких материалов возможно и в конструкциях, защищающих организм человека от внешних электромагнитных полей природного и антропогенного происхождения.

ЭФФЕКТИВНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ

Л.В. Евлаш

Обеспечение защиты информации на практике происходит в условиях случайного воздействия самых разных факторов. Некоторые из них систематизированы в стандартах, некоторые заранее неизвестны и способны снизить эффективность или даже скомпрометировать предусмотренные меры. Оценка эффективности защиты должна обязательно учитывать как объективные обстоятельства, так и вероятностные факторы.

Особую важность приобретает обоснование оптимальных значений показателей эффективности, учитывающее целевое предназначение информационной системы.

Основные причины проблем:

– игнорирование системного подхода как методологии анализа и синтеза систем защиты информации (СЗИ);

– отсутствие механизмов полного и достоверного подтверждения качества СЗИ;

– недостатки нормативно-методического обеспечения информационной безопасности, прежде всего в области показателей и критериев.

СЗИ должна быть именно системой, а не простым набором некоторых технических средств и организационных мероприятий. Системный подход к защите информации должен применяться, начиная с подготовки технического задания и заканчивая оценкой эффективности и качества СЗИ в процессе ее эксплуатации.

Сертификация продукции на соответствие требованиям государственных стандартов по безопасности информации должна подтверждается с определенной степенью достоверности.

В методическом плане определение эффективности СЗИ должно заключаться в выработке суждения относительно пригодности способа действий персонала или приспособленности технических средств к достижению цели защиты информации на основе измерения соответствующих показателей.

Для ответа на вопрос, в какой мере система защиты информации обеспечивает требуемый уровень безопасности, необходимо оценивать эффективность СЗИ показателями, носящими вероятностный характер. Совершенствование нормативной базы, методического обеспечения в области информационной безопасности должно происходить, прежде всего, в этом направлении.

ПРОБЛЕМА КАТЕГОРИРОВАНИЯ КРИТИЧЕСКИХ ОБЪЕКТОВ В РЕСПУБЛИКЕ БЕЛАРУСЬ

И.А. Картун, Е.А. Доценко

В современный период развития информационных технологий отмечается тенденция их использования практически во всех инфраструктурах государства. В связи с этим вопрос информационной безопасности приобретает все большую важность для нормального функционирования организаций и предприятий.

Особое внимание следует обратить на критические инфраструктуры, т.к. нарушение их информационной безопасности может привести к угрозе нанесения ущерба жизни или здоровью граждан, имуществу, окружающей среде, угрозам нарушения взрывобезопасности, биологической, механической, пожарной, промышленной, термической, химической, электрической, радиационной и иным типам безопасности. К таким критическим инфраструктурам относятся информационные объекты (системы) органов государственного управления, управления войсками, связи, финансов, энергетики, транспорта и т.д. На данный момент в Республике Беларусь утверждены лишь инструкции по определению объектов, представляющих повышенную техногенную и экологическую опасность с точки зрения физического воздействия на них. Однако не меньшую опасность представляют преднамеренные злоумышленные кибернетические воздействия на информационные системы, используемые на этих объектах.

Поэтому важно определить, какие конкретно объекты (системы) относятся к категории критических. Необходимо критические объекты (системы) категорировать по уровню критичности для рационального выбора системы защиты их информационных ресурсов и, как следствие, для рационального распределения экономических средств. Важнейшим критерием при категорировании является размер возможного причиненного ущерба, как людского, так и экономического, и при категорировании необходимо учитывать каждый из них в комплексе.

Проблема информационной безопасности каждого отдельного объекта (системы) критической инфраструктуры по своему масштабу является общенациональной и для своего решения требует пересмотра устоявшихся подходов, принятия единых стандартов, как в промышленности, так и в бизнесе, создания национальной системы подготовки специалистов соответствующего профиля, широкого информирования населения об угрозах и мерах по их предотвращению.

КОМПЬЮТЕРНОЕ СОПРОВОЖДЕНИЕ ЛАБОРАТОРНОГО ПРАКТИКУМА ПО ФИЗИКЕ ДЛЯ СТУДЕНТОВ СПЕЦИАЛЬНОСТИ "ЗАЩИТА ИНФОРМАЦИИ"

В.Н. Кушнир, С.Л. Прищепа

Изучение явлений или закономерностей физических процессов в любом физическом эксперименте лабораторного практикума по физике означает выявление функциональных связей между физическими величинами. Следовательно, эксперимент включает в себя в качестве необходимой составляющей обработку и анализ данных, полученных в результате непосредственных измерений. Как правило, студенты не осознают важности данного этапа эксперимента (в реальном эксперименте часто — наиболее трудоемкого и длительного). Этим мотивируется необходимость дополнения лабораторного практикума по физике полноценными заданиями по анализу и обработке экспериментальных данных. Уровень развития компьютерной техники и программного обеспечения, достигнутый в настоящее время, позволяет в полной мере реализовать данную задачу. Процедуру анализа и обработки данных мы демонстрируем на примере наиболее простых классических лабораторных работ по физике. В качестве оптимальных компьютерных средств представления, обработки и анализа данных рассматривается графический пакет Origin, а также математический пакет MathCAD. Возможность быстрого и полного анализа измерений, доставляемая компьютерными средствами, способствует качественному росту понимания студентом предмета исследования с одной стороны, а с другой — дает представление о минимуме исследовательской работы, необходимой для получения достоверного результата

СОЗДАНИЕ ПОДСИСТЕМЫ ЗАЩИТЫ ОТ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

А.В. Пугач

В настоящее время внутренние факторы заметно опережают внешние в рейтинге угроз безопасности информации. Наибольшие опасения специалистов вызывают утечки данных (76%) и халатность сотрудников (67%). Поэтому крайне важно минимизировать негативное влияние внутренних нарушителей на работу организации путем своевременного их обнаружения, адекватного реагирования и применения к ним дисциплинарных и правовых мер пресечения. Для решения этой задачи необходимо активизировать весь арсенал доступных средств, включая юридические, организационные и программно-технические механизмы защиты.

С юридической точки зрения необходимо в соответствии с действующим законодательством закрепление за организацией патентных и авторских прав, а также прав на защиту товарных знаков и коммерческой тайны. Договор (контракт) с работником должен содержать перечень требований по неразглашению коммерческой (служебной) тайны и ответственность работника за неправомерные действия.

Политика безопасности организации должна четко определять, что вся информация, хранимая, обрабатываемая и передаваемая по каналам связи в корпоративной сети является собственностью этой организации. Должны быть

категорически и открыто запрещены несанкционированный доступ, раскрытие, дублирование, изменение, удаление и ненадлежащее использование сведений. Служебная информация должна использоваться только в производственных целях. Границы допустимого использования этих данных должно определять руководство организации. Пользователи информационных систем должны быть предупреждены, что все программно-аппаратное обеспечение находится под наблюдением, и в случае необходимости вся последовательность их действий может быть восстановлена.

Программно-технические средства защиты могут включать контекстные анализаторы, системы статической и динамической блокировки устройств.

МЕТОДИКА И ПРОГРАММНЫЕ СРЕДСТВА АНАЛИЗА И ОЦЕНКИ КАЧЕСТВА ПРОФИЛЕЙ ЗАЩИТЫ И ЗАДАНИЙ ПО БЕЗОПАСНОСТИ

Е.П. Максимович, В.К. Фисенко, М.С. Шибут

В докладе излагается подход к автоматизации оценки качества ПЗ и ЗБ по показателям полноты, связности и непротиворечивости, принятым, соответственно, в национальных предстандартах СТБ П 34.101.7-2003 и СТБ П 34.101.6-2003. Для повышения эффективности процесса оценки предлагаются следующие направления усовершенствования системы показателей оценки качества ПЗ (ЗБ): учет различий важности описательных и базовых структурных составляющих ПЗ (ЗБ); разработка системы критериев для определения весов каждой структурной составляющей для различных ПЗ (ЗБ); использование настраиваемых лингвистических шкал для оценки степени соответствия ПЗ (ЗБ) требованиям стандартов, что позволяет определять интегральные показатели качества ПЗ (ЗБ) в более широком диапазоне значений. На основе предложенного подхода разрабатываются соответствующие программные средства поддержки принятия решений, автоматизирующие процесс оценки ПЗ (ЗБ) как последовательность следующих этапов.

Эксперты, осуществляющие оценку, вводят свои идентификационные данные и данные относительно объекта оценки. Наиболее опытный эксперт (или группа) осуществляет настройку шкал весовых коэффициентов и шкалы экспертных оценок. Затем эксперты задают систему весовых коэффициентов для показателей полноты, связности и непротиворечивости ПЗ (ЗБ). После этого выполняется оценка значений указанных показателей путем определения степени соответствия документа требованиям по лингвистической шкале следующего вида: "не соответствует", "низкая степень соответствия", "средняя степень соответствия", "высокая степень соответствия", "строгое соответствие". Затем результаты экспертной оценки формально обрабатываются на основе заданной системы шкал и весовых коэффициентов. Получаемое обобщенное мнение экспертов выдается в форме, удобной для лица, принимающего решение относительно итоговой оценки ПЗ (ЗБ). После полного обследования ПЗ (ЗБ) формируется отчет, содержащий оценку выполнения требований для каждого из показателей по каждому из разделов ПЗ (ЗБ).

ЗАЩИТА ИНФОРМАЦИИ — РЕШАЮЩЕЕ УСЛОВИЕ РАЗВИТИЯ МЕЖДУНАРОДНОЙ ПОЧТОВОЙ СВЯЗИ

Л.М. Лыньков, В.В. Соловьёв, Г.И. Власова

Безопасность станет наиболее часто обсуждаемым вопросом в связи с усилением терроризма, перевозкой наркотиков, отмыванием денег. Для почтовой отрасли важность стандартов "POST" в качестве домена, с которым установлены доверительные

отношения, для услуг, основанных на информационно-коммуникационных технологиях. Почтовый сектор вполне отвечает требованиям надежного управления идентификационной информацией в Интернете, представляя юридически действующий электронный адрес в дополнение к физическому, что снижает риск мошенничества, связанный с определением подлинности отправителя. При этом, с помощью "POST" физические адреса можно преобразовать в электронные, заложив тем самым фундамент универсальной почты будущего.

Кроме того, благодаря комбинированному использованию этой системы адресации и электронного почтового штемпеля почтовые службы могут предлагать услуги с оптимальной на сегодняшний день степенью защиты.

Государственные почтовые операторы работают в таких правовых рамках, которые позволяют им выступать в качестве сертификационных органов. Важнейшим фактором как для отправителей, так и для адресатов является защищенная доставка, при которой эти документы могут быть использованы только адресатами.

Всемирный почтовый союз, как орган стандартизации, разработавший более ста международных стандартов, в том числе стандарты для электронной передачи информации (контроль за прохождением сообщений, контроль данных и товаров), электронный почтовый штемпель, обеспечивают населению унифицированную почтовую связь в режиме онлайн в масштабе всего мира. Неотъемлемой частью этих стандартов является безопасность.

ИСПОЛЬЗОВАНИЕ ЦИФРОВОЙ ПОДПИСИ В ДИСТАНЦИОННОМ ОБУЧЕНИИ

Е.В. Новиков, Д.А. Мельниченко

Дистанционное обучение, рассматриваемое как совокупность кейсовых, телекоммуникационных и Интернет-технологий, в настоящее время заняло полноценное и полноправное место среди традиционных форм образования. Важнейшей составляющей такого обучения является коммуникативная, включающая в себя как асинхронные (электронная почта, mail-list, FTP), так и синхронные (talk, ytalk, chat) средства, что позволяет обеспечивать многовариантную связь между участниками учебного процесса, в первую очередь между преподавателем и учащимися. При этом основной проблемой при выполнении целого ряда учебных процедур является авторизация и идентификация каждого пользователя, а также сохранение целостности передаваемой информации и защита ее от несанкционированного доступа.

Для обеспечения подлинности и авторства документов, участвующих в документообороте дистанционного обучения, целесообразно использование цифровой электронной подписи, которая исключает возможность изменения документа без нарушения подлинности данной подписи и жестко увязывает в одно целое содержание документа. Причем подписывать можно как весь документ, так и любую его часть, а сам файл может содержать информацию разного рода (текст, графику, изображения).

Введение данной технологии позволяет не только существенно упростить процедуру идентификации и авторства работ учащихся, но и резко повышает их ответственность за представляемые материалы. Появляется также возможность совместного использования электронной подписи и видеоканалов для организации взаимодействия "преподаватель-студент". При реализации этого подхода в число образовательных процедур, реализуемых дистанционно, может быть включен прием экзаменов и зачетов.

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В УЧРЕЖДЕНИЯХ ОБРАЗОВАНИЯ

Д.А. МЕЛЬНИЧЕНКО, Е.В. НОВИКОВ

Научно-исследовательские работы, связанные с созданием и использованием информационных технологий, средств защиты информации, которые выполняются в рамках государственной программы информатизации Республики Беларусь, охватывают не только производственные отрасли, но также и образовательную сферу.

Современный подход к организации взаимодействия образовательных учреждений и обучающихся предполагает внедрение нового электронного документа, совмещающего в себе функции социальной и банковской карточки, а также функции управления доступом.

Электронный студенческий билет представляет собой пластиковую карту с электронным модулем, закрепленным на пластиковом основании. Электронный чип позволяет идентифицировать пользователя, управлять доступом в учебные центры и исследовательские лаборатории, оплачивать образовательные услуги, а также обеспечивает безопасность хранимых данных. Конфиденциальность информации, хранящейся в модуле, обеспечивается стандартными программными и техническими средствами, применяемыми для защиты информации.

Внедрение электронного студенческого билета гармонично дополняет информационно-коммуникационную инфраструктуру, создаваемую в республике на базе технических решений и возможностей центра обработки данных РУП "Белтелеком". Это позволит наладить и укрепить связи между учреждениями образования различных ступеней и видов, контролировать и проводить достоверный анализ процессов в сфере обучения, следить за его качеством и повышать эффективность.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

А.В. ТРУХАН

Образовательные компьютерные сети, как правило, не требуют специальных мер обеспечения безопасности. Однако их безопасность в значительной мере связана с обеспечением качества обслуживания.

Постоянно возрастающий спрос на использование мультимедийных приложений в сетях телекоммуникаций привел к усилению требований по обеспечению качества обслуживания (QoS) этих приложений. Среди таких требований можно выделить следующие: большая ширина полосы пропускания каналов связи, минимальное время ответа конечных узлов, минимальное значение вариации времени ответа конечных узлов сети, минимальное количество потерянных пакетов, а также повышенный уровень надежности.

Для решения описанных выше проблем представлено решение задачи линейного программирования для оптимальной маршрутизации информационных потоков в сетях телекоммуникаций для различных стратегий обеспечения живучести. Разработанные модели отличаются от известных тем, что при выборе оптимального пути, с точки зрения минимальной стоимости единицы передаваемой информации и обеспечения живучести, учитывается также требование заданного качества обслуживания.

Также предложен один из вариантов QoS-протокола, обеспечивающий оптимальное распределение ресурсов сети между пользователями, на основе критериев пользователей, предъявляемых к качеству обслуживания: задержка, вероятность потерь, дрожание пакетов, скорость передачи данных.

ОСОБЕННОСТИ ПРОГРАММЫ ДИСЦИПЛИНЫ "ЭЛЕКТРОПИТАНИЕ СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ" ДЛЯ СПЕЦИАЛЬНОСТИ "ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ"

Н.И. Шатило

Естественные импульсные помехи, наводимые в электрических сетях от молний, и помехи искусственного происхождения, возникающие от воздействия мощных электромагнитных импульсов, например, при коротком замыкании высоковольтной линии электропередачи, соизмеримы друг с другом и достигают единиц килоджоулей.

Эти помехи в первую очередь воздействуют на блоки питания телекоммуникационной аппаратуры, причем это воздействие может быть катастрофическим — энергия разрушения современных интегральных микросхем составляет единицы– сотни микроджоулей.

Поэтому в программе "Электропитание систем телекоммуникаций" должен быть предусмотрен специальный раздел, посвященный защите блоков питания от непреднамеренных помех, и в котором необходимо рассмотреть помехоустойчивые структурные и схемотехнические решения блоков питания.

В частности, анализ прохождения различных видов импульсных помех через сетевые фильтры показывает, что подавление наносекундных и микросекундных помех не может быть обеспечено одним фильтром.

В зависимости от требуемого уровня защиты используются различные схемотехнические решения. При требовании сохранения работоспособности после воздействия мощной помехи достаточно включения ограничителей сигналов, а при требовании сохранения выходных параметров блока питания необходимы дополнительные преобразования сетевого напряжения.

МЕТОДИКА ФОРМИРОВАНИЯ И ОЦЕНКИ ПРОФИЛЕЙ ЗАЩИТЫ

В.В. Маликов

При практической реализации комплекса защитных мер по обеспечению безопасности функционирования объектов возникает проблема комплексной оценки эффективности задействованных средств защиты, которая, как правило, является основополагающим критерием успешного предупреждения/предотвращения угроз. Разрабатываемая многоаспектная распределенная корпоративная система безопасности функционирования объектов на основе профилей защиты по перечню критериев безопасности для эффективного практического внедрения требует проведения оценки эффективности средств защиты.

Предлагается новая поэтапная методика формирования и оценки профиля защиты безопасности функционирования проектируемой системы:

1) формирование уравнения параметров фактической безопасности проектируемой системы на основе полной оценочной (базовой) сигнатуры рисков идеальной системы обеспечения безопасности.

2) проведение оценки уравнения параметров фактической безопасности проектируемой системы безопасности с эталонными уравнениями безопасности категорий безопасности по профилю защиты, сформированными на основе сигнатур рисков по сравнительному анализу с идеальной системой обеспечения безопасности и присваивания итоговых весовых коэффициентов.

3) формирование уравнения фактических угроз проектируемой системы на основе полной оценочной (базовой) сигнатуры угроз идеальной системы обеспечения безопасности по этапам жизненного (технологического) цикла системы.

4) проведение оценки уравнения фактических угроз проектируемой системы безопасности с эталонными уравнениями угроз безопасности категорий безопасности

по профилю защиты, сформированными на основе сигнатур угроз по сравнительному анализу с идеальной системой этапов жизненного (технологического) цикла обеспечения безопасности и присваивания итоговых весовых коэффициентов.

5) Формирование итоговой системы уравнений проектируемой (анализируемой) системы безопасности, включающей уравнения:

6) Сравнение уравнений итоговой системы уравнений проектируемой (анализируемой) системы безопасности с присвоенными профилями защиты.

В качестве дополнительных мер по совершенствованию проектируемой системы безопасности предлагаются методы:

– параметрическое повышение/понижение выбранного уровня профиля защиты:

– аналитическое повышение/понижение выбранного уровня профиля защиты согласно дополнительных сигнатур подавления параметров/угроз проектируемой системы.

ЗНАЧЕНИЕ ПРОФЕССИОНАЛЬНОЙ ОРИЕНТАЦИИ В ПОДГОТОВКЕ АБИТУРИЕНТА К УЧЕБНОМУ ПРОЦЕССУ

В.В. Борботько

Значение профессиональной ориентации и личностного развития молодых специалистов в условиях трансформации социальных отношений, сопровождающейся системной социальной неопределенностью, значительно возрастает. Повышение роли профессиональной ориентации в оптимизации социальных процессов связано с направленностью профориентации на формирование и активизацию адаптационных возможностей индивида не только в сфере труда, но и в широком социальном контексте его жизнедеятельности.

Профориентация очень объемное понятие, предполагающее широкий, выходящий за рамки педагогики и психологии, комплекс по оказанию помощи в выборе профессии, основными элементами которой являются профориентация и профконсультация, а так же профессиональное самоопределение. И профориентация и профконсультация заключается в ориентировании школьника, тогда как профессиональное самоопределение больше соотноситься с самоориентированием учащегося.

Возникает вопрос, какие факторы оказывают влияние на выбор профессии. На практике оказывается, что склонности учитываются в последнюю очередь, а вот мнение родителей оказывает огромное влияние.

Выбор профессии — одно из важнейших решений, принимаемых человеком в жизни, поскольку все мы хотим, чтобы работа соответствовала нашим интересам и возможностям, приносила удовлетворение и достойно оплачивалась. С этой целью возникает потребность в разработке и использовании психологического тестирования и беседы с профконсультантом помогающим учащимся сориентироваться в мире профессий, выбрать профильное обучение, школу, колледж, вуз, определить направление дальнейшего развития и спланировать подготовку к поступлению в вуз.

Профориентационная работа проводиться со старшеклассниками, рассматривающими вопрос о выборе профессии и высшего или среднего специального учебного заведения, а также с выпускниками школ, еще не имеющими опыта работы. При выборе профессии очень важно соответствие между психологическими особенностями человека и соответствующими характеристиками профессии. Процесс включает вопросы на оценку интересов и личностных качеств, оценку уровня развития способностей. Тем самым, позволяя совместить анализ интересов, способностей и личностных качеств, учащихся в рамках диагностики их профессиональных склонностей.

Таким образом, в данном случае понятие "профессиональная склонность" следует трактовать как интерес, подкрепленный соответствующими личностными качествами и

развитием соответствующих способностей, то есть, как совпадение интересов, способностей и характера человека, требуемых для определенной профессии.

Нередко в ходе профориентационного анализа выясняется, что у юноши или девушки наблюдаются противоречия между сферой интересов, сферой личностных качеств и сферой способностей, то есть, фактически, нет явно выраженных склонностей. Очень часто вызывает интерес сфера искусства и другие виды творческой деятельности, но при этом недостаточно выражены определенные способности.

Итак, для того, чтобы выбрать профессию, необходимо не только разбираться в мире существующих профессий, но, прежде всего, познать себя — свои личностно-психические качества. Именно с этой целью помочь выпускнику общеобразовательных учреждений познать себя и вводиться этот необходимым элементом модели.

ПРОБЛЕМЫ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ ДЛЯ УЧРЕЖДЕНИЙ ОБРАЗОВАНИЯ

И.В. Гасенкова, Е.П. Лавринович,
Н.И. Мухуров, М.М. Марченко, Е.А. Прокопчик

Эффективная защита интеллектуальной собственности (ИС) является важной составляющей, обеспечивающей развитие науки и экономики, наращивание экспортного потенциала. В настоящее время в Республике Беларусь созданы нормативно-правовая база и инфраструктура органов, обеспечивающие охрану авторских прав. Объем правовой охраны, предоставляемый белорусским законодательством произведениям науки, литературы и искусства, фонограммам, передачам эфирного и кабельного вещания соответствует основным международным договорам в данной сфере. Обладатели авторских и смежных прав имеют право осуществлять использование созданных ими объектов, передавать свои имущественные права по договорам и получать вознаграждение за каждый вид использования произведений, а в случае нарушения защищать свои права в суде.

Учреждения образования (УО) осуществляют научную и образовательную деятельность, результатами которой являются различные объекты интеллектуального труда, основанные на тех или иных объектах интеллектуальной собственности (ОИС). ОИС УО являются конкретные результаты его интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, продукции, выполняемых работ и услуг. Субъектами правоотношений в области правовой охраны ОИС являются:

– УО как единый учебно-научно-производственный комплекс;

– работники — авторы служебных ОИС;

– лица, содействовавшие созданию, правовой охране и использованию ОИС.

УО устанавливает политику, определяющую характеристики, процедуры, развитие, обязанности, права на использование ИС для студентов и сотрудников. Политика организуется в пяти различных областях в зависимости от режима правовой охраны и области применения:

– авторское право;

– патенты;

– программное обеспечение;

– товарные знаки и знаки обслуживания,

– коммерческая информация (ноу-хау).

Все студенты и сотрудники обязаны соглашаться с этим и соблюдать политику УО, как необходимое условие учебы или работы. Время от времени УО может вносить изменения в эту политику, направленные на ее усовершенствование.

Деканы факультетов, руководители иных структурных подразделений, заведующие кафедрами, отделами и лабораториями выполняют следующие функции до момента, когда сведения о сущности ОИС становятся общедоступными

(опубликование, изготовление, применение, экспонирование, передача третьим лицам и т.п.):

1) обеспечивают выявление ОИС УО;

2) принимают меры к исключению из практики подразделений подачу заявок на выдачу патентов (регистрацию) на служебные ОИС в РБ и иностранных государствах на имя работников-авторов данного подразделения, сторонних юридических и физических лиц, а также несанкционированную передачу третьим лицам сведений о сущности ОИС до подачи заявки УО или принятия им решения об отказе в подаче заявки;

3) совместно с экспертными комиссиями осуществляют меры по предотвращению преждевременного (до правовой охраны ОИС) полного или частичного разглашения сущности разработанных подразделением ОИС УО внутри страны и в зарубежных странах;

4) участвуют в определении целесообразности правовой охраны ОИС;

5) возлагают на научных руководителей и ответственных исполнителей охраноспособных НИР, выполняемым по бюджетным темам, ГНТП, проектам и грантам, ответственность за планирование в смете по таким НИР расходов на оплату патентных исследований, патентных пошлин и регистрационных сборов.

Работники-авторы ОИС УО имеют следующие права:

1) ходатайствовать перед вузом о правовой охране ОИС, созданного в связи с выполнением служебных обязанностей или полученного от работодателя конкретного задания;

2) быть указанным в качестве автора в заявках на выдачу охранных документов и регистрацию, произведениях науки, литературы и искусства;

3) подать заявку и получить патент на свое имя в оговоренных случаях;

4) получить информацию о решении УО прекратить поддержание патента в силе;

5) получить вознаграждения за использование ОИС, правообладателем которого является УО, в порядке и размере, установленном соответствующим приказом руководителя УО.

Лица, содействующие созданию и использования ОИС УО, имеют право на получение вознаграждения за содействие созданию и использованию ОИС в порядке и размере, установленном соответствующим приказом руководителя УО. Защита прав в области ИС УО осуществляется в административном и судебном порядках.

Общей задачей для УО является совершенствование отношений в сфере ИС между авторами-работниками УО, УО как работодателем, государством и другими заказчиками. Общественная значимость УО будет определяться не только в связи с предоставлением традиционных услуг в области образования и научно-исследовательской деятельности, но и с инновационной деятельностью и трансфером результатов учебно-научной деятельности.

Основными задачами в стратегическом управлении интеллектуальной собственностью являются:

– систематизация и анализ использования ОИС;

– выявление избыточных и необходимых ОИС;

– определение форм и методов правовой охраны ОИС;

– определение доминирующего ОИС;

– осуществление правовой охраны ИС;

– коммерциализация ИС;

– пресечение нарушений исключительных прав.

Хотя все типы ОИС обладают некоторыми общими свойствами, они имеют значительные отличия.

Одним из важных элементов стратегического планирования ИС является решение вопроса о том, какой вид ИС – изобретения, промышленные образцы, товарные знаки, объекты авторского права или ноу-хау, следует принять в качестве доминирующего в перспективном планировании деятельности УО. По данному вопросу

ведутся многочисленные дебаты, однако зарубежными специалистами отмечается возрастающая роль торговых марок и знаков обслуживания в стратегическом управлении ИС. В основном, это связано с тем, что торговые марки имеют неограниченный срок жизни вследствие возможности неоднократного продления их регистрации, а получение и поддержка правовой охраны торговых марок дешевле, чем, например, патентов на изобретения.

УПРАВЛЕНИЕ ПЕРСОНАЛОМ И СОВЕРШЕНСТВОВАНИЕ РАБОТЫ КАДРОВЫХ СЛУЖБ, КАК ФАКТОР ИНФОРМАЦИОННОЙ ЗАЩИТЫ ПРЕДПРИЯТИЯ

В.В. Минина

Важнейшим фактором производства и информационной защиты, определяющим эффективность деятельности предприятия, является человеческий капитал, поэтому управление персоналом на предприятии является основным направлением деятельности руководства компании и имеет особую значимость в условиях глобализации экономики, развития рынка и роста значения информации. Особенное внимание необходимо уделить особенностям индивидуального и коллективного поведения работников и особенностям поведения руководителей и членов управленческой команды.

В рамках предприятия УП "Научно-исследовательский институт средств автоматизации" было проведено исследование, целью которого была разработка основных направлений и подготовка мероприятий по повышению эффективности управления персоналом как фактора, влияющего на утечку информации. Работа включает в себя несколько ключевых этапов: 1) изучение теоретико-методологических подходов к управлению персоналом на предприятии; 2) обзор отечественных и зарубежных технологий управления; 3) анализ управления персоналом на предприятии и разработка мер по увеличению его эффективности и информационной защиты; 4) расчет экономического эффекта от предлагаемых мероприятий.

Результаты работы могут быть полезны для деятельности кадровых служб предприятия. Автоматизация деятельности отдела кадров является одним из важнейших и, на данном этапе развития современных технологий в управлении, абсолютно необходимым шагом на пути построения эффективной системы управления кадрами, с учетом современных информационных технологий.

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

МАТЕРИАЛЫ ДОКЛАДОВ И КРАТКИЕ СООБЩЕНИЯ
VI Белорусско-российской научно–технической конференции
19 –23 мая 2008 г., Минск

Компьютерный дизайн и верстка А.М. Прудник

В авторской редакции

Подписано в печать 16.05.2008. Формат 60×84 ⅛. Гарнитура «Century Schoolbook».
Печать ризографическая. Усл. печ. л. 23,83. Уч. изд. л. 21,45. Тираж 100 экз. Заказ 83.

Напечатано с оригинал-макета заказчика в типографии «Бестпринт».
220007, г.Минск, ул. Фабрициуса, д. 5, к. 1.

Специальное разрешение (лицензия) № 02330/0056811 от 02.03.2004.
Специальное разрешение (лицензия) № 02330/0133106 от 30.04.2004.

Издательство:
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство № 1954 от 03.12.2002.