X БЕЛОРУССКО-РОССИЙСКАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

29 - 30 мая 2012 г.

Минск БГУИР 2012

Министерство образования Республики Беларусь
Белорусский государственный университет информатики и радиоэлектроники
Федеральная служба технического и экспортного контроля Российской Федерации
Оперативно-аналитический центр при Президенте Республики Беларусь
Государственное предприятие "НИИ ТЗИ"
Центр повышения квалификации руководящих работников и специалистов Департамента охраны МВД Республики Беларусь
Объединенный институт проблем информатики НАН Беларуси
Академия управления при Президенте Республики Беларусь
Научно-производственное предприятие "Марфи"
Белорусское инженерное общество

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов X Белорусско-российской научно–технической конференции

(Минск 29–30 мая 2012 г.)

Минск БГУИР 2012

УДК 004.56 (043.2)

Технические средства защиты информации: Тезисы докладов X Белорусско-российской научно-технической конференции, 29–30 мая 2012 г., Минск. Минск: БГУИР, 2012. — 100 с.

Издание содержит тезисы докладов по техническим средствам защиты информации: организационно-правовому обеспечению защиты, средствам обнаружения и подавления каналов утечки информации, программно-аппаратным средствам защиты информации в компьютерных и телекоммуникационных сетях, методам и средствам защиты хозяйственных объектов, вопросам подготовки кадров.

ISBN 978-985-488-885-9

СОДЕРЖАНИЕ

СЕКЦИЯ 1. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

- **Гамов Е.А.** Применение стандартов информационной безопасности в Республике Беларусь. Разработка методики оценки требований информационной безопасности на основе общих критериев 7
- **Казеев М.Ю.** Безопасность КВОИ: организационно-правовые методы 7
- **Першин В.Т.** Методологические, организационные и технические компоненты создания системы защиты конфиденциальной информации 8
- **Нефедов С.Н., Погодин А.М.** Техническое регулирование и защита информации в сфере игорного бизнеса 9

СЕКЦИЯ 2. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

- **Алефиренко В.М.** Определение качественных характеристик блокираторов сотовых телефонов 10
- **Давыдов Г.В., Gao Jian Qiang, Yuan Rui** База фонем для синтеза речеподобных сигналов на китайском языке 11
- **Готовко М.А., Корунос П.С., Потапович А.В.** Вибрационные преобразователи для систем активной защиты речевой информации 12
- **Железняк В.К., Раханов К.Я.** Оценка разборчивости речи в каналах утечки информации методом ЛЧМ-сигнала программно-аппаратной системой 12
- **Каван Д.М.** Оценка защищенности помещений от утечки речевой информации 13
- **Мартинович А.В., Казека А.А.** Выделение информации по каналам побочных электромагнитных излучений средств вычислительной техники 14
- **Мартинович А.В., Скиб И.И.** Корреляционно-временное уплотнение шумовых сигналов 14
- **Воробьев В.И., Попов В.А., Шамгин Ю.В.** Подход к выявлению аппаратных недекларированных возможностей в вычислительной технике 15
- **Демидчук А.И., Чернявский Ю.А.** Метод обнаружения скрытой передачи данных, использующей стеганографический метод Коха-Жао 15
- **Зельманский О.Б.** Устройство синтеза речеподобных сигналов на разных языках 16
- **Зеневич А.О., Тимофеев А.М., Ахмеджанов Ф.А.** Использование квантовых систем для обнаружения каналов утечки оптической информации 17
- **Тимофеев А.М., Ахмеджанов Ф.А.** Использование маломощных оптических сигналов в системах обнаружения несанкционированного доступа 18
- **Утин Л.Л., Григорьев В.Л., Кред Х.М.** Особенности моделирования электромагнитного поля в защищаемых помещениях 18
- **Саванович С.Э., Давыдов А.Б.** Выбор частотного диапазона измерения электромагнитных составляющих первичного источника излучения, определяемого структурой персональной электронно-вычислительной машины 19
- **Хоминич А.Л.** Оценка информационной безопасности современных устройств отображения информации 20
- **Худолей И.С., Соловьев В.В.** Анализ требований к оптически прозрачным акустическим панелям для снижения разборчивости речи 21
- **Трушин В.А., Рева И.Л., Иванов А.В.** Расчет методической погрешности оценки разборчивости речи в задачах защиты информации 22

СЕКЦИЯ 3. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

- **Бильдюк Д.М.** Параллельные вычисления основных криптографических операций в системах на основе эллиптических кривых 23
- **Борискевич А.А.** Иерархическая система условного доступа к мультимедийному контенту с защитой от коалиционных атак 23
- **Борискевич А.А., Шут Д.М.** Алгоритм генерации хаотических последовательностей с улучшенными криптографическими характеристиками 24
- **Борискевич И.А.** Алгоритм обнаружения низкоконтрастных объектов в видеопоследовательности на основе избыточного дискретного вейвлет-преобразования 25
- **Брич Н.В., Голиков В.Ф.** Анализ криптостойкости двухэтапного протокола квантового распределения ключей 26
- **Липницкий В.А., Белюженко Е.В.** Нейросетевые технологии в криптографической проблеме передачи ключей 26
- **Богрецов В.А., Липницкий В.А.** Об алгебраических уравнениях над полями Галуа 27
- **Budzko A.A., Almiahi O.M.H.** Algorithms of Fast Walsh-Trahtman Transform 27

- **Nmadu Daniel, Prischepa S.L., Bobov M.N., Kosari A.** Burg-Töeplitz approach for voice-signal feature selection and extraction 28
- **Kosari Arash, Prischepa S.L., Bobov M.N., Nmadu D.** Optimize the security and reduce the fails detection in fingerprint biometric devices by using the hierarchical fingerprint matcher method 28
- **Липницкий В.А., Михайловский Е.Б.** О декодирующих возможностях непримитивных кодов Хемминга 29
- **Липницкий В.А., Олексюк А.О.** Особенности коррекции ошибок кодами с малым конструктивным расстоянием 30
- **Ганкевич С.А.** Анализ аналого-цифровой системы фазовой синхронизации 30
- **Губчик К.В., Иванюк А.А.** Методика получения истинно случайных чисел для задач защиты информации 31
- **Давыдов Г.В., Кухаренко А.И., Попов В.А., Тереня А.А.** Аппаратный генератор случайных чисел 32
- **Борисевич Дм.А., Давыдов Г.В.** Анализ критериев детектирования речи 32
- **Барановский Е.О.** Детектирования речи русскоязычного диктора-билингва 33
- **Ивашкевич А.В., Стройникова Е.Д.** Тестирование на простоту больших чисел специального вида 34
- **Мельников К.В., Бирючинский С.Б.** Архитектура многоканальных квантовых криптографических систем ... 35
- **Орлов Е.Е., Барановский О.К.** Исследование влияния недокументированного отладочного режима процессоров фирмы AMD на безопасность компьютерных систем 35
- **Охрименко А.А., Саломатин С.Б.** Маршрутизация по требованию с множественными путями на основе вектора расстояний в беспроводных сенсорных сетях 36
- **Комликов Д.А.** Формирование робастного подхода к управлению приоритетами при обнаружении и противодействии компьютерных атак 37
- **Новикова Л.В.** К вопросу аналитического моделирования DoS атак 38
- **Митюхин А.И.** Сегментация скрытных объектов изображений 39
- **Родионов М.М., Вашкевич М.И., Петровский А.А., Станкевич А.В., Петровский Ал.А., Качинский М.В.** Высокопроизводительные аппаратные реализации процессоров алгоритма шифрования DES на базе ПЛИС с архитектурой FPGA 40
- **Плетнёв С.А.** Гибридный криптографический алгоритм защиты данных в сенсорной сети 41
- **Плетнёв С.А.** Информационная безопасность в беспроводных сенсорных сетях 41
- **Прощеряков А.А., Иванюк А.А.** Использование физически неклонируемых функций для защиты цифровых устройств, реализуемых на ПЛИС 42
- **Шилин Д.Л., Бывшев С.С., Почебут М.В.** Шифрование данных с использованием систем фазовой синхронизации 43
- **Почебут М.В., Воробьева Ю.В.** Система контроля технологических процессов буровой установки 43
- **Шилин Д.Л., Почебут М.В.** Система криптографической защиты передачи информации на основе устройств ФАПЧ 44
- **Ревотюк М.П., Кароли М.К.** Безопасное прерывание процедур метода динамического программирования 45
- **Ревотюк М.П., Батура П.М., Хормози Р.** Безопасное прерывание процедур метода ветвей и границ 45
- **Ревотюк М.П., Зобов В.В.** Безопасное обслуживание потоков запросов процедурами облачных сервисов 46
- **Савченко И.В.** Программные средства синтеза речи 47
- **Савченко П.В., Пелькин Е.Р.** Поддержка Digital rights management в мобильных устройствах на базе Android 48
- **Нестор Альфредо Салас Валор** Неравная защита данных при помощи неравномерного двумерного кодировании информации 48
- **Сацук С.М., Пинаева М.М.** Механизм проводимости МДМ-структур на основе анодных оксидных пленок, содержащих иттрий 49
- **Сацук С.М.** Свойства анодных пленок на алюминии содержащих редкоземельные металлы 49
- **Сидоренко А.В., Мулярчик К.С.** Шифрование данных на основе дискретных хаотических систем и отображений 50
- **Стригалев Л.С.** Структурно-информационные аспекты безопасности сложных систем 51
- **Стригалев Л.С.** Критерии оценки качества средств защиты информации 51
- **Пачинин В.И., Таболич Т.Г., Шеремет Д.В.** Анализ простоев сервера Intel Server Board S5520UR по причинам их возникновения 52
- **Гивойно А.А., Николаенко Е.В., Сечко Г.В.** Архиватор с дополнительными опциями по защите информации 53
- **Михальцов М.В., Пачинин В.И., Таболич Т.Г.** Постановка задачи составления профиля защиты баз данных систем компьютерной диагностики автотехники 54
- **Хоанг Нгок Зыонг** Защита данных при последовательной норменной обработке информации 55
- **Юревич А.А., Цветков В.Ю.** Пакетная фильтрация трафика в беспроводных ячеистых сетях на основе распределенного межсетевого экрана 55

- **Журавлев А.А., Цветков В.Ю.** Анализ бортовых систем видеофиксации для охраны распределенных объектов с использованием беспилотных летательных аппаратов 56
- **Селиванова Ю.А., Цветков В.Ю.** Анализ защищенности систем видеоконференц-связи 56
- **Саломатин С.Б., Панькова В.В.** Криптографический анализ алгебро-геометрических кодов на соответствие требованиям систем защиты информации 57
- **Пискун Д.Н.** Мониторинг системы безопасности сети 2G/3G (UMTS) 57
- **Саломатин С.Б., Андрианова Т.А.** Кодовая коррекция смещения в генераторах случайных чисел 58
- **Шелестович П.В.** Обеспечение информационной безопасности с помощью облачных сервисов 59

СЕКЦИЯ 4. ЭЛЕМЕНТЫ И КОМПОНЕНТЫ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

- **Бойправ О.В., Неамах М.Р.** Оценка влияния мощности электромагнитных излучений на характеристики ослабления защитных экранов 60
- **Абдулькабер Хамза Абдулькадер, Борботько Т.В., Аксой Синан** Теплообменный аппарат контактного типа для систем снижения тепловой заметности объектов 60
- **Боровиков С.М., Шнейдеров Е.Н., Матюшков В.Е., Цырельчук И.Н., Гришель Р.П.** Методика прогнозирования надёжности электронных устройств для системы АРИОН 61
- **Бересневич А.И.** Использование напряжения коллектор–эмиттер в качестве имитационного фактора для прогнозирования постепенных отказов биполярных транзисторов 62
- **Аль-Махди М., Власова Г.А., Насонова Н.В., Лыньков Л.М.** Материалы для экранов ЭМИ на основе волокнистых матриц 63
- **Колосницын Б.С., Бушковский М.Д.** Моделирование сопротивлений исток-сток открытых мощных МОП транзисторов 63
- **Врублевский И.А., Чернякова К.В., Горбачев Д.В., Казанцев А.П.** ИК-фильтры на основе мембран пористого оксида алюминия для детекторов банкнот 64
- **Ахмед Али Абдуллах Аль-Дилами, Врублевский И.А., Чернякова К.В., Пухир Г.А.** Нанокомпозитные пленки анодного оксида алюминия с кобальтовыми нанопроволоками для экранирования электромагнитного излучения 64
- **Грабарь И.А., Насонова Н.В.** Моделирование радиопоглощающих свойств многослойных конструкций экранов ЭМИ 65
- **Гуринович А.Б., Лущицкая И.В.** Применение клистронов-генераторов различных конструкций 66
- **Гурский М.С.** Получение функциональных покрытий методом магнитоэлектролиза 66
- **Маковская Т.И., Данилюк А.Л.** Моделирование образования кратеров на поверхности металла при воздействии плазменных потоков 67
- **Паркун М.В., Драпеза А.И., Лобан В.А., Скороход Г.А., Судник Ю.М.** Информационная защищенность автоматизированных систем экспрессной оценки эффективности противомикробных препаратов 68
- **Махмуд М.Ш., Алаллак Н.Х.М., Криштопова Е.А.** Экранирующие электромагнитное излучение цементные материалы 68
- **Луговский В.П.** Особенности защиты информации в системах удаленного мониторинга параметров электросетей 69
- **Луговский В.П.** Оптимизация структуры информационно-измерительных систем показателей качества электроэнергии 69
- **Махмуд М.Ш., Пухир Г.А.** Взаимозаменяемость компонентов композиционных материалов защитных экранов электромагнитного излучения СВЧ-диапазона 70
- **Махмуд М.Ш., Авси М.М., Аль-Хизаи М.А., Прудник А.М., Лыньков Л.М.** Оптические свойства шунгитсодержащих материалов 70
- **Мельников К.В., Бирючинский С.Б.** Фотоприемное устройство модуля автоматической юстировки приемопередатчика системы атмосферной оптической связи 71
- **Мищенко В.Н.** Моделирование процессов переноса электронов в гетероструктурах GaAs–$Al_xGa_{1-x}As$ 72
- **Петров С.Н., Эпему А.М., Прудник А.М., Борботько Т.В.** Модифицированная установка для определения акустических характеристик звукоизолирующих панелей 72
- **Петров С.Н., Готовко М.А., Эпему А.М., Прудник А.М.** Звукоизолирующие свойства панелей электромагнитно-акустической защиты 73
- **Хуссейн Мохамед Альлябад, Яхия Таха Аль-Адеми, Пулко Т.А.** Экранирующие свойства композиционных материалов на основе синтетического полимера 73
- **Яхия Таха Аль-Адеми** Композиционные влагосодержащие материалы для элементов защиты человека в СВЧ-диапазоне 74
- **Смирнов Ю.В., Пулко Т.А.** Полимерные водосодержащие материалы для средств экранирования 75
- **Яхия Таха Аль-Адами, Пулко Т.А., Давыдов М.В.** Имитаторы радиопоглощающих свойств биологических тканей 75
- **Столер В.А., Столер Д.В.** Конструктивно-технологические особенности тепловых пироприемников 76

- **Лыньков Л.М., Борботько Т.В., Столер Д.В.** Рассеивающие покрытия оптического диапазона на основе органических композиционных материалов ... 77
- **Тымощик А.С., Тамашевич Е.С., Черных А.Г., Корницкий М.А.** Микроминиатюрное радиоприемное устройство на углеродных нанотрубках ... 77
- **Аль-Аль-Фурайджи О.Дж., Аль-Шамери К.Т., Аль-Алем А.С. Цветков В.Ю.** Инвариантная к параллаксу параметризация реперов для эффективного кодирования многоракурсных изображений в системе видеомониторинга ... 78

СЕКЦИЯ 5. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ХОЗЯЙСТВЕННЫХ ОБЪЕКТОВ

- **Воловач В.И.** Законы распределения дальности действия устройств обнаружения пространственных охранных систем ... 79
- **Воловач В.И.** К вопросу определения накапливающейся вероятности обнаружения в зоне контроля пространственных охранных систем ... 79
- **Катковский Л.В., Воробьев С.Ю., Богуш Р.П., Бровко Н.В.** Разработка аппаратно-программного видеотеплового комплекса дистанционного обнаружения пожаров ... 80
- **Валаханович Е.В.** Использование теории игр при минимизации рисков в банковских системах ... 80
- **Маликов В.В., Бенедиктович И.В., Чурюканов С.А.** Концептуальные основы организации и проведения аудитов систем комплексной безопасности критически важных объектов информатизации ... 82
- **Мамедов А.С.** К вопросу об использовании фазового метода для обнаружения смещения объектов в результате анализа изображений ... 83
- **Мирончик В.В.** Методика оценки достоверности скрытия наземных объектов в оптическом диапазоне длин волн ... 83
- **Михно Е.А., Цырельчук И.Н.** Модернизация СВЧ-извещателей для одновременного обнаружения наземной и подземной активности ... 84
- **Барановский О.К.** Вопросы технической защиты информации в системах физической защиты объектов критической инфраструктуры ... 85
- **Джамаль Саад Омер, Цикман И.М., Беляев Ю.В.** Спектральные зависимости степени линейной поляризации объектов с сеточным покрытием при различных фазовых углах ... 85
- **Романова Е.С., Савощик В.В.** Международные стандарты финансовой отчетности: требования к раскрытию информации ... 86
- **Денисенко И.Г., Ольховик А.А.** Роботизация средств управления сложных военно-технических систем в контексте защиты информации ... 87
- **Мелец А.Ф., Нефедов Д.С.** Система обнаружения воздушного вторжения на базе электростатических датчиков ... 87
- **Мухуров Н.И., Ясин Мохсин Вахиох, Прудник А.М.** Детектор для систем дозиметрического контроля на радиационно-опасных объектах ... 88

СЕКЦИЯ 6. ПОДГОТОВКА КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- **Будько А.А.** Особенности обучения студентов на английском языке ... 89
- **Боровиков С.М., Шнейдеров Е.Н., Бересневич А.И., Цырельчук И.Н., Матюшков В.Е.** Лабораторный практикум с использованием виртуальных объектов и систем по дисциплине «Теоретические основы проектирования электронных систем безопасности» ... 89
- **Боровиков С.М., Шнейдеров Е.Н., Бересневич А.И., Жагора Н.А., Бруй А.А.** Сценарий компьютерных лабораторных работ по исследованию эффективности функционирования электронных систем безопасности ... 90
- **Ганжа В.А., Чичко О.И.** Безопасность информации и обеспечение надёжности компьютерных сетей ... 91
- **Дерюшев А.А.** Мобильная система экспресс-опроса студентов ... 91
- **Маликов В.В.** Повышение эффективности подготовки специалистов по направлению комплексной безопасности ... 92
- **Крюкова Э.П.** Роль человека в системе компьютерной безопасности АЭС ... 93
- **Маруда Д.Н., Николаенко В.Л., Сечко Г.В.** Практическое занятие по основам управления интеллектуальной собственностью с уклоном в практику защиты информации ... 94
- **Шатило Н.И.** Особенности дисциплины «Функциональные устройства и электропитание систем телекоммуникаций» для специальности «Защита информации в телекоммуникациях» ... 95
- **Савицкая Д.Г., Бурцева В.П.** Энергетический паспорт типовой квартиры ... 96
- **Жигадло Т.В.** Дисциплина «Почтовая безопасность»: сущность и содержание ... 96
- **Кухаренко Е.А.** Влияние сети интернет на идентификацию личности ... 97
- **Кухаренко Е.А.** Креативное мышление как неотъемлемый навык современного специалиста ... 98

СЕКЦИЯ 1. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

ПРИМЕНЕНИЕ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ. РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ОБЩИХ КРИТЕРИЕВ

Е.А. ГАМОВ

На сегодняшний день актуальным для Республики Беларусь является вопрос создания либо адаптации методик оценки требований информационной безопасности (далее — ИБ). Этот процесс требует не только глубоких знаний стандартов, но и учета особенностей их применения. Важнейшим этапом является выбор стратегии оценки и определение набора оценочных критериев.

Для Республики Беларусь можно выделить такие специфические факторы ИТ как:

– относительно небольшая (в сравнении с мировой практикой) область распространения ИТ;

– невысокая степень международной интеграции;

– отсутствие широкого спектра информатизированных межотраслевых связей;

– сильное государственное регулирование.

В контексте стандартизации эти особенности означают следующее:

– внедрение требований и осуществления контроля их исполнения может осуществляться достаточно быстро и централизовано;

– принятие проработанного набора требований не вступит в противоречие с существующими субъектами информационных технологий.

При разработке методики оценки помимо требований «Общих критериев» также должны быть реализованы следующим положения:

– методология оценки должна иметь возможность адаптации к меняющимся условиям и быть применимой к новым технологиям;

– методика оценки должна предполагать механизм ранжирования продуктов;

– использование максимальной глубины декомпозиции и детализации параметров;

– процесс оценки должен быть разделен на этапы. Каждый этап должен базироваться на результатах предыдущего;

– при оценке должны быть учтены параметры среды функционирования;

– оптимальным будет являться применение модульности.

БЕЗОПАСНОСТЬ КВОИ: ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕТОДЫ

М.Ю. КАЗЕЕВ

В Республике Беларусь безопасность критически важных объектов информатизации (КВОИ) регламентируется Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации». Безопасность КВОИ должна основываться на методах установившейся практики с учетом мирового

опыта в области информационной безопасности, регламентируемых следующими нормативно правовыми актами:

– постановление Совета Министров Республики Беларусь от 26 мая 2009 г. № 675 «О некоторых вопросах защиты информации»;

– СТБ ISO/IEC 27001-2011 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Методология обеспечения безопасности КВОИ должна включать в себя:

– создание службы (подразделения) безопасности КВОИ;

– разработку и внедрение системы менеджмента информационной безопасности КВОИ;

– создание системы защиты информации КВОИ;

– проведение внутреннего и внешнего контроля безопасности КВОИ.

Таким образом, безопасность КВОИ в Республике Беларусь должна основываться на интеграции установившихся методологий и учитывать лучшие мировые практики в области информационной безопасности, опираясь на комплексный подход, включающий мероприятия правового, организационного и технического характера.

МЕТОДОЛОГИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ КОМПОНЕНТЫ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В.Т. ПЕРШИН

Цель работы — анализ условий и предпосылок для построения комплексной системы защиты конфиденциальной информации (КСЗКИ). Излагаемые в докладе соображения предполагают необходимость использования, создания и разработки совокупности взаимообусловленных и взаимоувязанных методологических, организационных и технических элементов КСЗКИ, которые базируется на использовании методологии построения комплексной системы защиты конфиденциальной корпоративной информации. Методология представляет собой совокупность способов и приемов рассмотрения вопросов информационной безопасности и методов их решения в целях построения комплексной системы информационной безопасности.

Методологические, организационные и технические компоненты КСЗКИ разрабатываются и создаются в рамках трех направлений работ:

– методическом;

– организационном;

– техническом.

Обсуждаемые в докладе условия и предпосылки для построения КСЗКИ в рамках единого подхода позволяют использовать согласованное применение разнородных средств в качестве компонентов при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ И ЗАЩИТА ИНФОРМАЦИИ В СФЕРЕ ИГОРНОГО БИЗНЕСА

С.Н. НЕФЕДОВ, А.М. ПОГОДИН

Защита информации в сфере игорного бизнеса направлена на обеспечение законных интересов: игроков (обеспечение заданного процента выигрыша), организаторов игорного бизнеса (недопущение мошеннических действий недобросовестных игроков) и государства (контроль оборота денежных средств и соблюдения установленных правил).

Указом Президента Республики Беларусь от 19 ноября 2010 г. № 599 «О некоторых мерах по совершенствованию порядка осуществления деятельности в сфере игорного бизнеса» определены основные мероприятия по обеспечению решения данных вопросов. Указом установлено, что с 1 июля 2011 г. все игровые автоматы, используемые в Республике Беларусь, должны быть обязательно включены в Государственный реестр игровых автоматов, а с 1 июля 2012 г. все игровые автоматы должны быть, подключены к специальной компьютерной кассовой системе (СККС). Ожидается, что срок подключения к СККС будет в ближайшее время перенесен.

Обязательные требования к игровым автоматам установлены в государственных стандартах СТБ 2180-2011 «Игровые автоматы. Классификация. Термины и определения» и СТБ 2181-2011 «Игровые автоматы. Технические требования и методы испытаний», а порядок проведения испытаний, с целью включения в Государственный реестр ТКП 296-2011 «Игровые автоматы. Порядок проведения испытаний, экспертизы и технического освидетельствования». В докладе рассматриваются основные требования данных документов и особенности их применения.

СЕКЦИЯ 2. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

ОПРЕДЕЛЕНИЕ КАЧЕСТВЕННЫХ ХАРАКТЕРИСТИК БЛОКИРАТОРОВ СОТОВЫХ ТЕЛЕФОНОВ

В.М. АЛЕФИРЕНКО

Широкое использование сотовой связи для оперативной коммуникации между сотрудниками фирм предоставляет потенциальным конкурентам возможность перехвата информации с помощью специальных программных и технических средств. Особенно актуальной проблема защиты информации становится во время ведения конфиденциальных переговоров, когда по различным (в том числе и этическим) причинам отсутствует возможность изъятия мобильных телефонов и проверки их отсутствия у лиц, ведущих переговоры. В этом случае могут применяться блокираторы сотовых телефонов, работающие скрытно. Современный рынок технических средств защиты информации предлагает широкий выбор разных моделей блокираторов сотовых телефонов, выпускаемых различными фирмами. Поэтому выбор наиболее оптимальной по своим техническим характеристикам модели представляет определенные трудности не только для руководителя фирмы, но даже и для специалиста. Одним из методов такого выбора предлагается метод определения уровня качества с использованием комплексного показателя, включающего в себя соответствующие единичные показатели. В качестве единичных показателей для блокираторов сотовых телефонов были выбраны их основные технические характеристики, такие как диапазон рабочих частот, радиус действия, подавляемые стандарты, количество антенн, время непрерывной работы, вид источника питания, а также характеристики, присущие любым техническим средствам, такие как габариты, вес, цена. Для сравнения были выбраны следующие модели: «ВР-1050», «Скорпион Ультра-1030», «Мозаика-НЧ», «Шершень», «Паук», SEL SP-162 «Батог», «ЛГШ-701», «Октава-2С». Расчет проводился с использованием средневзвешенного арифметического показателя, который по сравнению со средневзвешенным геометрическим показателем позволял использовать в расчетах единичные показатели, принимающие нулевое значение после проведении операции нормировки. Результаты расчетов показали, что комплексные показатели качества для выбранных моделей блокираторов сотовых телефонов лежат в пределах от 0,24 («Паук») до 0,66 («ЛГШ-701»), который и является лучшим. Близкие к нему значения имеют также блокираторы 0,58 («Скорпион Ультра-1030») и 0,56 («ВР-1050»). Таким образом, определение качественных характеристик блокираторов сотовых телефонов, выраженных численными значениями, позволило провести их сравнение и определить лучшую модель по выбранным характеристикам.

БАЗА ФОНЕМ ДЛЯ СИНТЕЗА РЕЧЕПОДОБНЫХ СИГНАЛОВ НА КИТАЙСКОМ ЯЗЫКЕ

Г.В. ДАВЫДОВ, GAO JIAN QIANG, YUAN RUI

Одним из методов защиты речевой информации в выделенном помещении, когда звукоизоляция помещения недостаточная, является метод, основанный на создании маскирующих сигналов в ограждающих элементах конструкций. В качестве маскирующих сигналов широко используется "белый шум" в речевом диапазоне частот. Однако, в последнее время для повышения эффективности систем защиты речевой информации начали применяться и комбинированные маскирующие сигналы. Эти сигналы получаются путём смешивания "белого шума" речевого диапазона частот с так называемыми "речеподобными" сигналами [1]. Речеподобные сигналы формируются из элементарных структурных элементов речи таких, как аллофоны или фонемы. При этом по случайному закону синтезируется текст, не содержащий никакой информации, с соблюдением вероятностных характеристик речи для заданного языка. Вероятностные характеристики это — вероятности появления определённых аллофонов или фонем, присущих данному языку, а также вероятностные характеристики длины слов, количества слов в предложении, количества предложений в фоноабзаце. Особенность комбинированных маскирующих сигналов заключается в том, что речеподобные сигналы формируются по базе аллофонов или фонем конкретного диктора. Тогда выделить информационную составляющую речи этого диктора на фоне комбинированных маскирующих сигналов с речеподобными сигналами сформированными по базе аллофонов или фонем этого диктора чрезвычайно сложно. Это объясняется тем, что форманты речевого информационного сигнала совпадают с формантами маскирующих речеподобных сигналов, и частота основного тона для речеподобных сигналов будет совпадать с частотой основного тона информационного сигнала речи. Вместе с тем, в комбинированных маскирующих сигналах могут использоваться и речеподобные сигналы нескольких дикторов.

Особенность формирования речеподобных сигналов на китайском языке заключается в том, что китайский язык является тональным и выделить отдельные аллофоны для этого языка и синтезировать из них речеподобные сигналы не представляется возможных из-за необходимости наложения тона на фонему для того чтобы речеподобные сигналы были похожи на речь на китайском языке. Поэтому синтез речеподобных сигналов на китайском языке необходимо выполнять по базе фонем.

База фонем китайского языка создавалась путем анализа словарей современного китайского языка и составлена была из 406 фонем одинаковой транскрипции на английском языке, а с учетом тональностей языка база фонем составила 1239. Число фонем современного китайского языка оказалось меньше числа иероглифов. Это обусловлено тем, что имеется ряд иероглифов, которые имеет одинаковые фонемы, т.е. имеют одно и тоже произношение, включая и тональные особенности произношение. Для базы фонем определены вероятности их появления в речи на китайском языке.

Литература

1. Воробьёв В.И., Давыдов А.Г., Давыдов Г.В. Доклады БГУИР. 2009. № 3. С. 9–16.
2. Давыдов Г.В., Каван Д.М., Попов В.А., Потапович А.В. Докл. БГУИР. 2009. № 4. С. 49–54.

ВИБРАЦИОННЫЕ ПРЕОБРАЗОВАТЕЛИ ДЛЯ СИСТЕМ АКТИВНОЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

М.А. ГОТОВКО, П.С. КОРУНОС, А.В. ПОТАПОВИЧ

В настоящее время является актуальным защита речевой информации в выделенных помещениях от утечки по виброакустическим каналам. Такими каналами являются опорно-несущие и ограждающие конструкции, инженерные коммуникации такие как трубопроводы центрального отопления, водопроводы, системы вентиляции, также оконные и дверные проёмы. Существует два основных метода защиты речевой информации в выделенном помещении: пассивные и активные методы. К пассивным методам относятся звукоизоляция помещений, уменьшения (ослабления) уровня речевого сигнала. Активные методы защиты речевой информации основаны на использовании виброакустической маскировки информационных речевых сигналов. Для возбуждения колебаний в ограждающих элементах и инженерно коммуникационных конструкций помещений могут использоваться следующие вибрационные преобразователи: электромагнитные, пьезоэлектрические, электродинамические.

Пьезоэлектрические преобразователи не обеспечивают высокой эффективности в области низких частот (100–500 Гц). Электродинамические преобразователи отличаются сложностью конструкторской реализации, заключающейся в наличии мембраны, малым магнитным зазором для обеспечения большой индукции. Преимущество электродинамического преобразователя перед электромагнитными заключается в более широком диапазоне рабочих частот.

Электромагнитные преобразователи весьма эффективны в области низких частот и обеспечивают динамические значения выталкивающей силы 0,1 Н во всем речевом диапазоне частот.

Электромагнитный преобразователь представляет собой устройство состоящее из корпуса в котором установлен постоянный магнит для создания магнитно поля, в отверстии магнита установлен магнитопровод с катушкой индуктивности для возбуждения переменного магнитного поля между магнитом и мембранной со штоком.

Роль оконечных устройств в системах виброакустической маскировки, осуществляющих преобразование электрических шумовых колебаний в акустические колебания речевого диапазона частот, обычно выполняют малогабаритные широкополосные громкоговорители, а осуществляющих преобразование электрических шумовых колебаний в вибрационные — виброизлучатели, как правило электромагнитного или пъезоэлектрического типов.

ОЦЕНКА РАЗБОРЧИВОСТИ РЕЧИ В КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ МЕТОДОМ ЛЧМ-СИГНАЛА ПРОГРАММНО-АППАРАТНОЙ СИСТЕМОЙ

В.К. ЖЕЛЕЗНЯК, К.Я. РАХАНОВ

Совершенствование методов и средств извлечения слабых сигналов в каналах утечки речевой информации из шумов высокого уровня (например, очисткой сигнала от шумов) обусловило развитие методов и средств оценки их защищенности, что является актуальным. Из существующих методов оценки защищенности информации метод шумового сигнала функционально ограничен, методически не совершенен. Метод гармонического сигнала обладает рядом преимуществ, но обладает некоторыми методическими погрешностями.

Анализ этих методов определил направление исследования, заключающееся в обосновании и разработке на новом принципе метода оценки защищенности присущих речевому сигналу каналов утечки информации. Новый метод базируется на преимуществах предложенного широкополосного ЛЧМ-сигнала в надпороговой области при устранении основного его недостатка — порогового эффекта. Частотно-временное представление сигнальной энергии функцией Вигнера позволило учесть тонкую структуру ЛЧМ-сигнала. Дополнение к корреляционной теории разборчивости речи, разработанной для метода гармонического сигнала, позволяет значительно снизить методические (теоретические) погрешности, обусловленные рядом факторов, искажающих акустический сигнал в замкнутом объеме.

В этой связи основным направлением исследований является научное обоснование, разработка оценки разборчивости речи в каналах утечки информации методом ЛЧМ-сигнала, внедренного во вновь разработанную программно-аппаратную систему. Выбранное направление исследований является ключевым, так как решает задачу оценки нормативных показателей в виде критерия разборчивости речи с высокой точностью, благодаря теоретическому обоснованию, снижающего методическую (теоретическую) погрешность метода, реализованного автоматизированной программно-аппаратной системой.

ОЦЕНКА ЗАЩИЩЕННОСТИ ПОМЕЩЕНИЙ ОТ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

Д.М. КАВАН

Оценка степени защищенности речевой информации в выделенном помещении выполняется на базе методов оценки звукоизоляции помещений и дальнейшем определении разборчивости речи, распространяющейся по ограждающим элементам конструкций помещений, в местах возможного ее перехвата. Для обеспечения защиты речевой информации в выделенном помещении могут применяться в первую очередь пассивные методы, которые реализуются при строительстве зданий и активные методы, основанные на создании в элементах ограждающих конструкций маскирующих сигналов со спектром частот, перекрывающим частоты речевых сигналов.

Акустические волны, образующиеся в выделенном помещении в результате речевой деятельности, воздействуют на ограждающие элементы конструкций помещений с уровнями звукового давления порядка 70 дБ в частотном диапазоне от 50 Гц до 10 кГц. При этом акустические волны воздействуют на ограждающие элементы конструкций помещений под различными углами и имеет место наличие многократно отраженных акустических волн.

Кроме того, рассмотрены механизмы образования акустических каналов утечки речевой информации и доказано, что основным видом колебаний, за счет которых происходи перенос речевой информации за пределы выделенного помещения являются изгибные колебания ограждающих элементов конструкций.

В качестве примера были выполнены расчеты форм собственных колебаний гипсоблочной стены с использованием программного пакета ANSYS.

Показано, что речевые сигналы, представленные в виде акустических волн, проходят через ограждающие элементы конструкций помещений за счет возбуждения многомодовых изгибных колебаний ограждающих конструкций.

Для оценки разборчивости речи целесообразно использовать инструментально-расчетный метод, основанный на результатах экспериментальных исследований.

Показатель словесной разборчивости речи можно использовать и оценки эффективности закрытия технических каналов утечки речевой информации, но при этом метод артикуляционных измерений из-за сложности и длительности проведения в практической деятельности неприемлем. Целесообразно разбивать речевой диапазон частот на спектральные полосы, вносящие одинаковый вклад в разборчивость речи, то есть, имеющие одинаковый весовой коэффициент. Разборчивость речи определяется по отношению уровень речевого сигнала в канале утечки/уровень акустического или маскирующего шума.

ВЫДЕЛЕНИЕ ИНФОРМАЦИИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

А.В. МАРТИНОВИЧ, А.А. КАЗЕКА

Одним из возможных каналов утечки информации средств вычислительной техники (СВТ) является канал побочных электромагнитных излучений (ПЭМИ). Наиболее опасным с точки зрения перехвата данных является видеотракт СВТ [1]. Видеоадаптер формирует сигнал, представляющий собой квазипериодическую последовательность импульсов, частота генерации которых зависит от режимов его работы (разрешение экрана монитора, частота кадровой синхронизации).

В настоящее время процесс выявления информационных сигналов осуществляется на основе принципов энергетического приема. Для обеспечения качественной синхронизации предлагается использовать автокорреляционный приемник (АКП), выделяющий колебания тактовой частоты и позволяющий в $N>>1$ раз увеличивать число накапливаемых кадров для восстановления элементов сигнальной последовательности.

В работе приведены алгоритмы обнаружения и выделения информационных компонент сигналов по каналам ПЭМИ, выполнено математическое моделирование устройства обнаружения и выделения сигнальной последовательности на основе АКП, рассмотрены возможности восстановления изображения, выводимого на экран монитора по сигналам ПЭМИ. Использование предлагаемых алгоритмов позволяет производить оценку защищенности информации от утечки по каналам побочных электромагнитных излучений и при необходимости принимать меры для снижения уровня ПЭМИ СВТ.

Литература

1. Хорев А.А. Специальная техника. № 4–5. 2007.

КОРРЕЛЯЦИОННО-ВРЕМЕННОЕ УПЛОТНЕНИЕ ШУМОВЫХ СИГНАЛОВ

А.В. МАРТИНОВИЧ, И.И. СКИБ

В теории техники связи могут быть использованы частотный, временной и амплитудный ресурсы, которые имеют объективные границы, не позволяющие выйти за пределы «объема» сигнала. Существующие сигнально-кодовые конструкции (СКК) на основе шумоподобных сигналов не позволяют обеспечить требуемой информационной емкости из-за ограниченности ансамблей псевдослучайных последовательностей (ПСП), что приводит к перегрузке каналов передачи информации в заданной полосе частот. Вместе с тем, уплотнение информационных потоков за счет разнесения по задержке одной и той же

реализации (носителя информации) создает возможность увеличения числа передаваемых информационных потоков [1].

Предлагаемые СКК на основе шумовых носителей позволяют уплотнять информационные потоки без использования дополнительных частотных и временных ресурсов, обеспечивая при этом высокую структурную скрытность систем передачи информации (СПИ).

В работе приводится синтез и математическое моделирование устройств формирования и обработки шумовых сигналов на основе корреляционно-временного уплотнения информационных потоков для помехозащищенных СПИ. Показано влияние помех на качество выделения информационных потоков, даны оценки качественных характеристик СПИ, использующих предлагаемые СКК.

Литература

1. Ипатов В.П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М., 2007.

ПОДХОД К ВЫЯВЛЕНИЮ АППАРАТНЫХ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ

В.И. ВОРОБЬЕВ, В.А. ПОПОВ, Ю.В. ШАМГИН

Известны способы и устройства [1] выявления аппаратных недекларированных возможностей (АНДВ) в вычислительной технике (ВТ). В докладе обосновывается целесообразность сосредоточения внимания на:

– поиске АНДВ, в первую очередь, во внешних устройствах и аксессуарах основного оборудования ВТ;

– анализе возможностей использования в исследуемом оборудовании АНДВ, работающих в официально выделенном для интерфейсов Wi-Fi и Bluetooth частотном диапазоне.

Предложения связаны с тем, что внешние устройства и аксессуары основного оборудования ВТ весьма удобны для быстрой установки в них и обеспечения электропитания камуфлированных под стандартные элементы и узлы АНДВ. в частотном же диапазоне, используемом интерфейсами Wi-Fi и Bluetooth, сравнительно просто маскировать маломощные электромагнитные сигналы АНДВ. Поиск демаскирующих работу АНДВ сигналов целесообразно осуществлять на всех входах и выходах основного оборудования ВТ, подключаемых к внешним проводным линиям, включая линию электропитания. Важным средством выявления АНДВ следует считать визуальный осмотр и даже разборку аксессуаров и внешних устройств ВТ. Поиск информативных радиоизлучений исследуемого оборудования в каждом конкретном случае требует индивидуального подхода.

Литература

1. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь. М., 2004. 432 с.

МЕТОД ОБНАРУЖЕНИЯ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ, ИСПОЛЬЗУЮЩЕЙ СТЕГАНОГРАФИЧЕСКИЙ МЕТОД КОХА-ЖАО

А.И. ДЕМИДЧУК, Ю.А. ЧЕРНЯВСКИЙ

Жао Цянь и Экхард Кох предложили выполнять встраивание скрываемого сообщения в процессе JPEG-сжатия [1]. В каждом блоке дискретно-косинусного преобразования из 8-ми среднечастотных коэффициентов выбираются три

коэффициента ДКП и подвергаются следующей модификации: для кодирования 1 и 0 коэффициенты изменяются так, чтобы два из них были больше или меньше третьего на определенное пороговое значение D.

Анализу подвергаются все коэффициенты ДКП из области модификации каждого блока (8 коэффициентов). Для этого в каждом блоке вычисляется среднеквадратичное отклонение (СКО) и формируется массив коэффициентов СКО. для полученного массива строится гистограмма распределения коэффициентов, по которой находится значение наиболее часто встречающееся — s_{max}. для пустых контейнеров и контейнеров заполненных с порогом D>1 значение s_{max} будет больше ς=0,354. для случая D=1 вычисляется отношения количества наиболее часто встречающихся значений к общему количеству коэффициентов СКО. Полученное значение отношения сравнивается со значениями вероятности нахождения скрытой информации по таблице значений, полученных эмпирическим путем.

Предложенный критерий стеганографического анализа JPEG-изображений дает высокий процент (порядка 90%) верных результатов в случае порога D>1. Оценка с порогом встраивания D=1 дает результат с ошибкой второго рода равной 15,6%. для пустых контейнеров ошибка первого рода примерно равна 20%. Использование предложенного метода оценки изображения в формате JPEG на предмет определения наличия скрытой информации методом Коха–Жао обеспечивает эффективное решение задач стегоанализа.

Литература

1. Zhao J., Koch E. // IEEE Workshop on Nonlinear Signal and Image Processing. Greece, 1995. P. 123–132.

УСТРОЙСТВО СИНТЕЗА РЕЧЕПОДОБНЫХ СИГНАЛОВ НА РАЗНЫХ ЯЗЫКАХ

О.Б. ЗЕЛЬМАНСКИЙ

Задачей предлагаемого устройства защиты речевой информации является генерирование речеподобных сигналов на разных языках и в режиме реального времени, маскирующих речь участников переговоров. Работа устройства осуществляется следующим образом.

Блок формирования псевдотекста составляет псевдотекст на выбранном языке или нескольких языках с использованием их статистики, получаемой, например, от баз русского, арабского и английского языков. Блок компиляции аллофонов в зависимости от диктора и выбранного языка выбирает необходимые базы аллофонов и озвучивает полученный псевдотекст. в результате получается шумовой речеподобный сигнал, который поступает на управляемый усилитель.

В случае, если требуется синтезировать речеподобный сигнал непосредственно из речи участников переговоров, речевой сигнал, поступающий от встроенного или выносного микрофона, фиксируется блоком детектирования речи. Далее он поступает в блок верификации диктора по голосу, а также в блоки сегментации и классификации с целью формирования аллофонов, которые в свою очередь заносятся в базу аллофонов соответствующего диктора. В базу аллофонов какого диктора следует занести каждый аллофон определяется блоком верификации диктора по голосу, который распознает и подтверждает личность каждого из участников переговоров на основании уникальной информации, выделенной из их речи заранее в процессе регистрации до начала переговоров. Кроме того данный блок позволяет выбрать уже имеющуюся базу аллофонов конкретного диктора для использования в блоке компиляции аллофонов.

Предложенное устройство позволяет защитить речевую информацию от утечки через такие элементы ограждающих конструкций как потолок, пол, стены, оконные стекла, элементы конструкций отопительных и водопроводных сетей, дверные тамбуры и вентиляционные каналы.

ИСПОЛЬЗОВАНИЕ КВАНТОВЫХ СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ КАНАЛОВ УТЕЧКИ ОПТИЧЕСКОЙ ИНФОРМАЦИИ

А.О. ЗЕНЕВИЧ, А.М. ТИМОФЕЕВ, Ф.А. АХМЕДЖАНОВ

В связи с интенсивным развитием в последние годы волоконно-оптических систем связи возрос интерес к созданию средств обнаружения каналов утечки оптической информации, передаваемой по таким системам. Квантово-криптографические системы передачи информации, в которых для кодирования данных используются состояния фотонов оптического излучения, позволяют обеспечить безусловную защищенность передаваемой информации, однако имеют ряд недостатков, в частности низкие скорости передачи информации (СПИ) — до 50 кбит/с [1], что может ограничивать область применения этих систем. Возможной альтернативой квантово-криптографическим системам передачи информации могут быть квантовые системы передачи и приема информации, в которых для трансляции оптической информации так же, как и в квантово-криптографических системах, используются отдельные фотоны, однако не применяется кодирование передаваемых двоичных символов состояниями передаваемого фотона. Отметим, что защита передаваемой информации в квантово-криптографических системах обеспечивается за счет использования состояний передаваемых фотонов (несанкционированный доступ приводит к нарушению поляризации фотонов, что и выявляет факт доступа к передаваемой информации), а в квантовых — за счет контроля вероятности ошибки регистрации данных (несанкционированный доступ увеличивает вероятность ошибки регистрации данных, что приводит к уменьшению СПИ, контроль которой выявляет наличие канала утечки информации). До настоящего времени квантовые системы передачи и приема информации, позволяющие обнаруживать каналы утечки оптической информации, не разработаны. Поэтому целью данной работы является создание квантовых систем обнаружения каналов утечки оптической информации.

В работе предложены квантовые системы передачи и приема информации, в которых в качестве приемного модуля использовался счетчик фотонов, построенный на базе лавинного фотоприемника.

Выполнена классификация квантовых систем передачи и приема оптической информации, согласно которой такие системы можно разделить по числу фотонов, используемых для передачи каждого бита информации, на однофотонные и многофотонные, а также по способу синхронизации источника и приемника — на синхронные и асинхронные.

Выполненные экспериментальные исследования по определению СПИ созданных квантовых систем показали, что максимально возможная СПИ синхронных однофотонных квантовых систем составила 1,2 Мбит/с, асинхронных — до 50 кбит/с.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор № Т11ОБ-043).

Литература

1. Килин С.Я., Хорошко Д.Б., Низовцев А.П. и др. // Квантовая криптография: идеи и практика. Минск, Белорусская наука, 2007.

ИСПОЛЬЗОВАНИЕ МАЛОМОЩНЫХ ОПТИЧЕСКИХ СИГНАЛОВ В СИСТЕМАХ ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

А.М. ТИМОФЕЕВ, Ф.А. АХМЕДЖАНОВ

В последние годы в телекоммуникациях преимущественно используют волоконно-оптические системы связи, которые, в частности, обеспечивают высокие скорости передачи информации (СПИ). Защита данных от несанкционированного доступа (НСД) в таких системах особенно важна при организации межправительственной связи, передаче информации банковских служб и пр. Задача обнаружения НСД может быть решена при использовании квантовых систем передачи и приема информации, в которых каждый бит информации передается маломощными оптическими импульсами, содержащими от одного до десяти фотонов. Применение таких сигналов позволяет выявить любую попытку перехвата информации за счет контроля числа принятых фотонов, длительности и моментов времени их поступления на приемный модуль. Однако подобный контроль возможен только при наличии высокочувствительных приемных модулей, в качестве которых наиболее часто используют счетчики фотонов, построенные на базе лавинных фотоприемников (ЛФП) [1]. До настоящего времени отсутствуют исследования влияния интенсивности оптического излучения и напряжения питания ЛФП на СПИ квантовой системы передачи и приема информации. Поэтому целью настоящей работы является исследование влияния интенсивности оптического излучения и напряжения питания ЛФП на СПИ квантовой системы передачи и приема информации.

Выполнены исследования зависимости квантовой эффективности регистрации и мертвого времени счетчика фотонов от перенапряжения, а также зависимости СПИ от интенсивности оптического излучения.

Установлено, что достижение максимально возможной СПИ квантовой системы передачи и приема информации возможно при подборе напряжения питания ЛФП, работающего в режиме счета фотонов, и интенсивности оптического изучения, при которых мертвое время счетчика фотонов минимально, а квантовая эффективность — максимальна.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор № Т11ОБ-043).

Литература

1. Гулаков И.Р., Холондырев С.В. Метод счета фотонов в оптико-физических измерениях. Минск, 1989. С. 48–58.

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ В ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЯХ

Л.Л. УТИН, В.Л. ГРИГОРЬЕВ, Х.М. КРЕД

Одним из мероприятий защиты от утечки информации через каналы побочных электромагнитных излучений и наводок является размещение ЭВМ на максимальном удалении от границ контролируемой зоны. Основным достоинством данного мероприятия является отсутствие необходимости приобретения дополнительных средств защиты, если потенциальная дальности излучения ЭВМ не выходит за границу контролируемой зоны [1]. В случае не выполнения данного условия, целесообразно проведение исследований контуров излучений ЭВМ при ее размещении в различных точках защищаемого помещения

[1]. В результате подобных исследований должно быть выявлено такое место для размещения ЭВМ в объекте информатизации, при котором радиоизлучения ЭВМ за пределы контролируемой зоны будут минимальны. Кроме того, могут быть определены наиболее опасные направления излучений, на которых рекомендуется использовать пассивные или активные средства защиты.

Данные исследования желательно проводить путем измерения уровней электромагнитного поля в помещении и за его пределами. Однако стоимость таких измерений высока [1]. Уменьшение расходов возможно при применении средств моделирования распространения электромагнитного поля от источника излучения к разведывательной аппаратуре. Использование аналитических методов моделирования затруднено из-за отсутствия достоверных сведений о характеристиках средств перехвата излучений, сложности формализации изменений мощности электромагнитного поля в результате диффузного взаимодействия радиоволн от различных источников, энергетических потерь в препятствиях, имеющих различные коэффициенты поглощения и геометрические размеры, статистического воздействия естественных и искусственных помех.

Использование методов имитационного моделирования позволяет получить представление о зонах излучения ЭВМ в помещении и за его пределами. Моделирование зоны суммарного излучения ЭВМ осуществлялось с учетом особенностей распространения радиоволн в ближней и дальней зоне, Кроме того, учитывалось ослабление сигналов при прохождении радиоволн через различные объекты, а также потери энергии при отражении от границ препятствий.

Разработанная имитационная модель позволяет:

– отображать суммарную зону электромагнитных излучений ЭВМ и других электронных устройств, находящихся в помещении с учетом статистического воздействия на сигнал различных факторов;

– определять расстояние до точки, в которой еще возможен перехват информативных излучений ЭВМ радиоприемной аппаратурой злоумышленников с учетом затухания электромагнитного поля при прохождении его через различные препятствия;

– находить место размещения ЭВМ в защищаемом помещении, на котором суммарная площадь зоны ее излучения за пределы контролируемой зоны будет минимальна;

– отображать потенциально опасные направления распространения излучений за пределы контролируемой зоны.

Литература

1. Утин Л.Л., Григорьев В.Л., Кред Х.М. // Доклады БГУИР. 2010. № 7. С. 53–58.

2. Утин Л.Л., Кред Х.М., Управление информационными ресурсами: материалы 8-й междунар. науч.-практич. конф. Минск. 10 февр. 2011 г. Минск, Акад. упр. при Президенте Респ. Беларусь, 2011. С. 162.

ВЫБОР ЧАСТОТНОГО ДИАПАЗОНА ИЗМЕРЕНИЯ ЭЛЕКТРОМАГНИТНЫХ СОСТАВЛЯЮЩИХ ПЕРВИЧНОГО ИСТОЧНИКА ИЗЛУЧЕНИЯ, ОПРЕДЕЛЯЕМОГО СТРУКТУРОЙ ПЕРСОНАЛЬНОЙ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНОЙ МАШИНЫ

С.Э. САВАНОВИЧ, А.Б. ДАВЫДОВ

Электромагнитное поле, создаваемое персональными электронно-вычислительными машинами (ПЭВМ), представляет собой совокупность

спектральных составляющих электромагнитных излучений от отдельных технических блоков входящих в состав персонального компьютера (ПК).

Уровень электромагнитного излучения будет определяться техническими характеристиками оборудования и его режимами работы, а также удаленностью оператора от источника излучений.

Рекомендованные методики для измерения параметров электромагнитных излучений (ЭМИ) не рассматривают воздействия электромагнитного поля на пользователя в диапазоне частот свыше 400 кГц и не учитывают воздействие на пользователя излучений системного блока, являющегося источником повышенного уровня электромагнитного излучения.

Разработанная методика измерения излучений создаваемого ПЭВМ предполагает измерение следующих составляющих: Е (электрическую составляющую), Н (магнитную составляющую) и ППЭ (плотность потока энергии), необходимых для оценки воздействия создаваемого электромагнитного поля, как на оператора, так и на расположенную в поле действия электромагнитных помех радиоэлектронную аппаратуру.

Целью разработанной методики является измерение уровней электромагнитных излучений, создаваемых системным блоком ПЭВМ, во всем частотном диапазоне от 400 кГц до 3000 МГц в ближней зоне в условиях окружающего фонового уровня ЭМИ и определение изменения параметров электромагнитных излучений в зависимости от выполняемых на рабочем месте пользователем ПК стандартных операций и его положения относительно источника излучения.

Литература

1. СанПиН 2.2.4/2.1.8.9-36-2002 «Электромагнитные излучения радиочастотного диапазона (ЭМИ РЧ)».

2. СанПиН 9-131 РБ 2000 «Гигиенические требования к видеодисплейным терминалам, электронно-вычислительным машинам и организации работы» с изменениями от 4 февраля 2009 г. № 12.

ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ УСТРОЙСТВ ОТОБРАЖЕНИЯ ИНФОРМАЦИИ

А.Л. ХОМИНИЧ

На протяжении многих лет в задачах защиты информации остается популярной тема несанкционированного съема информации с устройств отображения (дисплеев) по каналу паразитных электромагнитных излучений и наводок (ПЭМИН). Эту проблему поднимают специалисты в области компьютерной безопасности, разработчики и производители защитных покрытий и экранов и многие другие. Поэтому актуальна задача оценки вероятности съема информации с современных дисплеев, выполненных на базе жидкокристаллических, светодиодных и плазменных панелей, за счет их ПЭМИН.

Перечисленные дисплеи, несмотря на использование существенно разных физических принципов преобразования «сигнал-свет», строятся по практически одинаковым структурных схемам и в общем случае включают в себя модуль интерфейсов, модуль обработки видеосигналов (видеопроцессор) и схему адресации панели. Обработка сигналов выполняется в цифровом виде, преобразование в аналоговый (либо дискретный) вид осуществляется непосредственно перед подачей на электроды данных панели.

Известно, что вероятность декодирования данных, перехваченных по каналу ПЭМИН, существенно выше при их последовательной передаче, ибо в параллельном интерфейсе электромагнитные излучения от каждого проводника суммируются, причем с одинаковыми весовыми коэффициентами для всех разрядов, в результате демодуляция и декодирование такого суммарного излучения становится невозможной, особенно при большом количестве разрядов. Анализ схемотехники рассматриваемых дисплеев показывает, что передача сигналов изображений между их блоками осуществляется в полностью параллельном, либо параллельно-последовательном виде. В результате даже если данные будут перехвачены, восстановить правильное цветное изображение невозможно, хотя вероятность восстановление черно-белого изображения теоретически существует. На практике же это, ввиду малой амплитуды и широкой полосы частот передаваемых сигналов, будет чрезвычайно сложной задачей. На основании этого можно сделать о высокой степени защищенности современных устройств отображения информации по каналам ПЭМИН даже без использования защитных средств и систем.

АНАЛИЗ ТРЕБОВАНИЙ К ОПТИЧЕСКИ ПРОЗРАЧНЫМ АКУСТИЧЕСКИМ ПАНЕЛЯМ ДЛЯ СНИЖЕНИЯ РАЗБОРЧИВОСТИ РЕЧИ

И.С. ХУДОЛЕЙ, В.В. СОЛОВЬЕВ

При обеспечении защиты информации от утечки по акустическому каналу определяющее значение приобретает снижение разборчивости речи, при прохождении речевого сигнала через ограждающие конструкции, наряду со снижением звукового давления. В первую очередь это относится к обеспечению защиты помещений, имеющих повышенные требования к уровню секретности.

Окна, занимающие по условиям освещенности достаточно большие площади ограждающих конструкций помещения, являются одним из наиболее слабых его элементов с точки зрения утечки акустической информации. Поэтому необходимость разработки оптически прозрачных акустических панелей требует особого внимания.

Можно выделить следующие основные моменты, имеющие определяющее значение при разработке оптически прозрачных акустических панелей:

– для повышения звукоизоляции может осуществляться использование многокамерных стеклопакетов: чтобы шум гасился наиболее эффективно, расстояния между стеклами в одном блоке должны быть разными;

– пространство между листами остекления может быть заполнено аэрогелем, пористость которого имеет показатель свыше 60% и плотность ниже 0,6 г/см^3;

– в промежутках между листами стеклопакета могут быть образованы каналы, по которым прокачивают газ или жидкость. Поскольку коэффициент прохождения звуковой волны в движущуюся среду меньше коэффициента прохождения звуковых волн в среду, находящуюся в состоянии покоя, то при прокачке по каналам газа или жидкости эффект звукоизоляции повышается;

– для дополнительного снижения разборчивости речи в заполненную жидкостью камеру стеклопакета осуществляется подача воздуха через трубку с отверстиями малого диаметра, находящуюся в нижней ее части. Посредством этого происходит формирование большого количества воздушных пузырьков малого диаметра. В момент всплытия происходит столкновение пузырьков, вследствие чего возникает управляемая вибрация. Управление осуществляется изменением давления воздуха, подаваемого в трубку, находящуюся в камере стеклопакета.

РАСЧЕТ МЕТОДИЧЕСКОЙ ПОГРЕШНОСТИ ОЦЕНКИ РАЗБОРЧИВОСТИ РЕЧИ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. ТРУШИН, И.Л. РЕВА, А.В. ИВАНОВ

Доклад посвящен исследованию погрешностей методики оценки словесной разборчивости речи в задачах защиты информации. Приведен ряд факторов влияющих на погрешность используемой в настоящее время методики. Приведены результаты артикуляционных испытаний со связными текстами, которые расходятся с расчетными результатами по существующей методике. Проведена оценка погрешностей, сделаны выводы по полученным зависимостям.

Используемая методика оценки представляет собой косвенные измерения, следовательно, расчет погрешности сводится к расчету погрешности косвенных измерений. В результате получены зависимости, приведенные в виде графиков, абсолютной и относительной погрешностей от отношения сигнал/шум (для двух типов шумов: белый и формантоподобный) и от значения словесной разборчивости. В результате погрешность косвенной оценки словесной разборчивости оказалась весьма значительна. Относительная погрешность достигает 21%, а при учете разброса порога слышимости (±6 дБ) для зависимости коэффициента восприятия относительная погрешность достигает 70%. Соответственно при такой погрешности можно упростить методику и отойти от большого количества экспоненциальных членов вычислительных формул используемой методики.

СЕКЦИЯ 3. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

ПАРАЛЛЕЛЬНЫЕ ВЫЧИСЛЕНИЯ ОСНОВНЫХ КРИПТОГРАФИЧЕСКИХ ОПЕРАЦИЙ В СИСТЕМАХ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Д.М. БИЛЬДЮК

Преимуществом криптосистем на эллиптических кривых является то, что при выполнении операции шифрования отсутствует очень медленная операция возведения больших чисел в степень по модулю, характерная для других криптосистем с открытым ключом (например, RSA). Базовой операцией в группе точек эллиптической кривой, определяемой конкретным уравнением, являются операции сложения и удвоения точек в аффинных координатах, связанных с модулярным умножением.

Наиболее распространенным методом при реализации модульного возведения в степень (в классических криптосистемах, например RSA) является метод Монтгомери. Реализация последнего имеет большую скорость выполнения по сравнению с другими методами умножения больших чисел и последующего вычисления остатка от деления (например, умножение по методу Карацубы и последующее вычисление остатка на основе спуска Ферма). Однако при выполнении операции модульного умножения метод Монтгомери не имеет преимуществ по скорости и его использование становиться неэффективным. Параллельная реализация указанных методов в позиционных системах счисления позволяет значительно повысить скорость выполнения базовых операций известных криптосистем с открытым ключом, но недостатки метода Монтгомери относительно эллиптических кривых сохраняются. Параллельная реализация модульного умножения по методу Монтгомери в непозиционной системе счисления на основе остаточных классов дает значительный прирост в скорости, и позволяет рассматривать указанный метод как наиболее эффективный.

Сравнительный анализ скорости выполнения базовых операций в криптосистемах с открытым ключом осуществлялся на основе технологии параллельных вычислений CUDA.

ИЕРАРХИЧЕСКАЯ СИСТЕМА УСЛОВНОГО ДОСТУПА К МУЛЬТИМЕДИЙНОМУ КОНТЕНТУ С ЗАЩИТОЙ ОТ КОАЛИЦИОННЫХ АТАК

А.А. БОРИСКЕВИЧ

В настоящее время среди пользователей глобальной сети все более востребованными становятся службы передачи мультимедийных данных. Актуальными становятся задачи организации условного доступа к платному мультимедийному контенту в глобальной сети Интернет. Система условного доступа должна обеспечивать доступ к контенту с различным качеством, при этом, учитывая среду распространения контента, система должна быть защищена от коалиционных атак.

Условный доступ к мультимедийным данным с разным качеством основан на декомпозиции контента, представлении его в виде множества пакетов, селективном или полном шифровании пакетов. Шифрование пакетов может быть произведено несколькими способами. Простейший способ заключается в шифровании каждого пакета независимыми ключами. При этом множество ключей декоррелированно, что не дает возможности осуществить коалиционную атаку на ключи. Однако в этом случае лицензия, выдаваемая пользователю, должна содержать множество ключей, необходимых для расшифрования контента с заданным качеством. Количество передаваемых ключей зависит от параметров декомпозиции контента и предоставляемого уровня качества. Другим подходом к решению проблемы является использование иерархии ключей. При использовании иерархии ключей лицензия содержит только один ключ, необходимый для расшифрования контента. Нижестоящие в иерархии ключи определяются через одностороннюю хэш-функцию. Недостатком применения иерархии ключей является их подверженность коалиционным атакам при более двух типах декомпозиции и отсутствии дополнительных мер защиты.

Для организации защищенного от коалиционных атак условного доступа к мультимедийному контенту предлагается система условного доступа, основанная на модифицированной структуре иерархических ключей. Защита от коалиционных атак осуществляется за счет введения дополнительных защитных субключей и основывается на дополнении или замещении исходной иерархии ключей защищенной иерархией. При этом предлагаемая система имеет режим частичной защиты с запрещением перехода к высшим уровням качества и режим полной защиты от коалиционных атак. Режим частичной защиты обеспечивает большее быстродействие за счет незначительного увеличения структуры ключа. Данный режим может быть использован для контента с большим количеством типов и уровней декомпозиции. Режим полной защиты полностью предотвращает коалиционные атаки на секретные ключи, но требует большее количество защитных субключей и имеет меньшее быстродействие. Предлагаемая система поддерживает как полное, так и селективное шифрование контента в зависимости от требований к быстродействию и деградации качества при восстановлении контента без вышестоящих в иерархии ключей.

Гибкость разработанной системы дает возможность использовать ее для широкого спектра задач, направленных на организацию условного доступа к мультимедийному контенту в глобальной сети.

АЛГОРИТМ ГЕНЕРАЦИИ ХАОТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С УЛУЧШЕННЫМИ КРИПТОГРАФИЧЕСКИМИ ХАРАКТЕРИСТИКАМИ

А.А. БОРИСКЕВИЧ, Д.М. ШУТ

Генерация псевдослучайных последовательностей с хорошими криптографическими характеристиками является одной из важнейших задач в области защиты информации. Одной из причин использования цифровых хаотических систем для улучшения качества генераторов является простота реализации и тесная взаимосвязь между хаотическими (эргодичность, высокая чувствительность к начальным условиям/ управляющему параметру, детерминированная динамика и структурная сложность) и криптографическими свойствами (перемешивание, рассеяние, детерминированная псевдослучайность, алгоритмическая сложность).

Предложен алгоритм генерации бинарных хаотических последовательностей, основанный на использовании модели детерминированного хаоса, генерации начальных значений (сеансовых ключей) из секретного ключа, генерации последовательности целых и вещественных хаотических значений, перемешивании вещественных хаотических значений с помощью целочисленных хаотических значений, бинаризация перемешанных хаотических значений.

Разработанный алгоритм позволяет формировать бинарные и вещественные хаотические последовательности с улучшенными криптографическими свойствами (баланс {0, 1}, большая длина цикла, высокая линейная сложность, и т.п.) за счет увеличения пространства ключей (начальное значение хаотической переменной, управляющий параметр и параметр безопасности) и использования операции перемешивания.

Проведена оценка качества сгенерированных последовательностей с использованием пакета из 15 статистических тестов NIST, целью которой было определение и подтверждение случайного характера бинарных хаотических последовательностей.

АЛГОРИТМ ОБНАРУЖЕНИЯ НИЗКОКОНТРАСТНЫХ ОБЪЕКТОВ В ВИДЕОПОСЛЕДОВАТЕЛЬНОСТИ НА ОСНОВЕ ИЗБЫТОЧНОГО ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

И.А. БОРИСКЕВИЧ

Для обнаружения низкоконтрасных объектов на ИК-изображениях требуется выделить пиксели целей на фоновом изображении в условиях низкого отношения сигнал/шум. Известные алгоритмы не позволяют обнаружить цели с заданной степенью достоверности. В связи с этим предложен алгоритм, основанный на вычислении избыточного дискретного вейвлет-преобразования, попиксельной и локальной обработке матриц аппроксимирующих и/или детализирующих вейвлет-коэффициентов, формировании интегрального вейвлет-изображения с близкой к требуемой форме гистограммы, бинаризации и бинарной морфологической операции наращивания. Он позволяет обнаружить низкоконтрастные объекты за счет использования свойств избыточного дискретного вейвлет-преобразования с определенным уровнем разложения, оптимальных вейвлет-функций и выбранного правила объединения вейвлет-матриц. Избыточное дискретное вейвлет-преобразование производит локализацию компонент исходного изображения в пространственно-частотной области с сохранением его энергии, что гарантирует отсутствие искажения значимых деталей и позволяет произвести анализ динамики изменения локальных статистических параметров изображения на разных уровнях.

Оценка эффективности предложенного алгоритма была произведена с использованием ROC-кривых (Receiver Operating Characteristic), позволяющих оценить соотношение вероятности правильного обнаружения и ложной тревоги. Из анализа кривых следует, что предложенный алгоритм увеличивает вероятность правильного обнаружения на величину до 50% по сравнению с известными алгоритмами за счет большей устойчивости к изменению размеров целей и инвариантности к сдвигу. Моделирование проведено в среде Matlab для пяти уровней разложения и четырех вейвлет-функций. Последовательность тестовых изображений содержит низкоконтрастные малоподвижные объекты размером 3–25 пикселей, искаженные аддитивным гауссовским шумом.

АНАЛИЗ КРИПТОСТОЙКОСТИ ДВУХЭТАПНОГО ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Н.В. БРИЧ, В.Ф. ГОЛИКОВ

Пользователи, желающие обменяться защищенной информацией, должны обладать общим секретным ключом. Задача конфиденциальной доставки ключевой информации решается методами асимметричной криптографии. Однако до сих пор не существует математических доказательств односторонности функций, используемых в криптоалгоритмах. Рост производительности компьютеров вынуждает увеличивать размер используемых ключей и сложность односторонних функций. Новые технологии — квантовая механика — вообще переводят экспоненциальные задачи в разряд задач, решаемых за полиномиальное время.

Чтобы исключить возможность создания препятствий для установления связи между санкционированными пользователями по квантовому каналу, был предложен новый протокол передачи ключевой информации, основанный на протоколе BB84. Предложенный двухэтапный протокол формирования ключевой информации основан на невозможности верного определения базисов передающей и принимающей стороны криптоаналитиком для второго сеанса передачи ключа, даже если во время первого сеанса криптоаналитику удалось перехватить передаваемую последовательность с точностью до нескольких битов.

Одним из наиболее распространенных типов атак является съем информации в квантово-криптографическом канале с использованием непосредственного измерения поляризационного состояния фотона. Способ сводится к измерению непосредственно передаваемого состояния, а затем перепосылке нового состояния в зависимости от результата измерения.

В результате исследования установлено, что в некоторых случаях использование согласованных базисов на втором этапе являются уязвимостью протокола. Сделан вывод о необходимости дальнейшего усовершенствования предложенного двухэтапного протокола квантового распределения ключей.

НЕЙРОСЕТЕВЫЕ ТЕХНОЛОГИИ В КРИПТОГРАФИЧЕСКОЙ ПРОБЛЕМЕ ПЕРЕДАЧИ КЛЮЧЕЙ

В.А. ЛИПНИЦКИЙ, Е.В. БЕЛЮЖЕНКО

Защита информации от несанкционированного доступа всегда была актуальной проблемой для нашей цивилизации. К 70-м годам XX века криптография вышла за рамки секретных служб и приобрела публичный характер. Это обусловлено широчайшей информатизацией общества, когда точность, достоверность и конфиденциальность информации становится приоритетом не только для государственных служб, но и для фирм, организаций, компьютерных и телекоммуникационных сетей.

Введение в практику защиты информации односторонних функций, открытых ключей, новейших математических алгоритмов позволило наряду с симметричной криптографией использовать криптографические методы с открытыми ключами. Этот фактор и послужил основой массового применения криптосистем, к примеру, в ситуациях типа «банк-клиент».

Важным применением ассиметричной криптографии явилась возможность открытой передачи ключей для быстродействующих систем, работающих, как правило, с симметричными ключами (протокол Диффи-Хелмана). В 2005 г.

В. Канцель и И. Кантер предложили использовать нейронные сети для передачи ключей между удаленными нейронными сетями.

Разработана практическая компьютерная модель функционирования двух нейронных сетей по обмену секретными ключами. Проведены компьютерные испытания данной модели с исследованием возможностей подключения третьей несанкционированной сети. Получены обнадеживающие результаты в криптостойкости данной модели.

ОБ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЯХ НАД ПОЛЯМИ ГАЛУА

В.А. БОГРЕЦОВ, В.А. ЛИПНИЦКИЙ

Проблема решения алгебраических уравнений привлекает внимание научного общества едва ли не с зари человеческой цивилизации. Усилиями Дж. Кардано, К.Ф. Гаусса, Н.Х. Абеля, Э. Галуа и многих других, казалось бы, поставлена точка в этом вопросе. Но решать алгебраические уравнения приходится. При этом привлекаются или методы численного анализа или аппарат специальных функций. Вынужденная специализация полей, из которых берутся коэффициенты уравнений и их корни, возникшая из конкретных задач XX века, привнесла в данную проблему новые сложности.

Проблемы коррекции многократных ошибок, обработки сигналов и изображений, современной физики и генетики привели в 70-е годы XX века к необходимости решения уравнений над конечными полями. Выяснилось, что теория уравнений над полями Галуа практически отсутствует, а классические формулы и методы не работают.

В докладе обсуждаются результаты систематизации подходов и методов решения уравнений над полями Галуа. Предложены компьютерные реализации методов Чэня и формул Чэня, сведения к системам линейных уравнений, модификаций метода Фаддеева–Берлекемпа, норменного метода.

Разработанные программные средства могут быть полезны в приложениях, где требуется практическое решение уравнений над полями Галуа.

ALGORITHMS OF FAST WALSH-TRAHTMAN TRANSFORM

A.A. BUDZKO, O.M.H. ALMIAHI

Walsh functions can be ordered in different ways. But for practical applications it is interesting only symmetrical systems of ordering, like well known Hadamard, Paley, Kachmaz and Trahtman. The main purpose of this report is to introduce the definition of Trahtman system of ordering of Walsh functions. Here is considered representation of Walsh functions in matrix form. The construction of Walsh-Trahtman matrix any size is derived by the mirror imaging rule and can be obtained using recurrent formula which is considered. To obtain any element of Walsh-Trahtman matrix exponent formula is derived. This formula can be used for construction of Walsh function generators of different types and for deriving algorithms of fast Walsh transform. In the report a lot of attention paid to how to derive the «wonderful» algorithms of fast Walsh transform and proposed most interesting.

BURG-TÖEPLITZ APPROACH FOR VOICE-SIGNAL FEATURE SELECTION AND EXTRACTION

DANIEL NMADU, S.L. PRISCHEPA, M.N. BOBOV, A. KOSARI

This work presents new applications of Töeplitz matrix eigenvalues approach in image description, feature extraction and recognition [1]. It discusses the possibility of treating the speech signal graphically in order to extract the essential image features as a basic step in successful data mining applications in the biometric techniques. The considered object here is the human-voice signal. The suggested frequency spectral estimation and Töeplitz-based approach, built on the linear predictive coding principle, has proved the possibility of selecting signal features from the power spectral plot and entering Töeplitz matrix in a manner similar to its application on images of written texts, signature, palm-print, face geometry or fingerprints. These topics have shown a success rate of about 98% in many cases. The extracted feature-carrying image comprises the elements of Töeplitz matrices to consecutively compute their minimal eigenvalues and introduce a set of feature vectors within a class of voices.

The basic idea of the work is derived from applying Töeplitz matrix minimal eigenvalues algorithm to Burg's model. This implies a graphical approach for feature extraction, selection and hence signal-image description confronting the conventional and traditional methods. Töeplitz matrix approach is employed to verify a variety of biometrics, including the recognition of hand and machine written texts, off and on-line signature, face, and voice. In all, it has proved a promising success rate. The same algorithm has also shown its possible application in hybrid systems where multiple forms of classifying and identifying tools are fused in one system. The image of a voice signal in any of its classical forms is rather complicated and usually does not convey exactly similar images of the same signals, even when spoken by the same person.

However, Burg`s model is very fruitful approach for investigation of voice-signal information protection. This fact concerns the possibility of looking at the voice-signal image in a manner similar to any other object image. This enabled extending Töeplitz matrix applications to cover speech signal description, as well.

References

1. Gray R.M. Töeplitz and Circulant Matrices: A Review. Technical Report, Stanford University Press, 2000.

OPTIMIZE THE SECURITY AND REDUCE THE FAILS DETECTION IN FINGERPRINT BIOMETRIC DEVICES BY USING THE HIERARCHICAL FINGERPRINT MATCHER METHOD

ARASH KOSARI, S.L. PRISCHEPA, M.N. BOBOV, D. NMADU

The main factors responsible for the intra-class variations are: displacement, rotation, partial overlap, non-linear distortion, variable pressure, changing skin condition, noise, and feature extraction errors. Therefore, fingerprints from the same finger may sometimes look quite different whereas fingerprints from different fingers may appear quite similar .The aim of our work is to optimize and improve efficiency of fingerprint algorithms and make it much more secure and create new method to estimate the immunity level of fingerprint facilities of authentication which we call that Hierarchical fingerprint matcher.

The novelty of this matching technique is to use of features (pores and ridge contours) provide complementary information which can be used along with features (minutiae) to lower the error rates, namely FAR and FRR.

We have tried to overcome the real challenges in fingerprint matching namely, non-linear distortion, small overlap between query and template images, error and noise introduced by feature extraction algorithms, error introduced in registration and due to unfavorable skin conditions. Localized matching was used for matching all feature types, in-order to minimize the effects of distortion. Also, rotationally invariant structures (pores and minutia) and features (ridge contours) are used and as a result any type of alignment (registration) is not required at any stage. The use of (pores and ridge contours) features is beneficial in deciding match/nonmatch, with increased accuracy, in case of fingerprints with small overlap, beside that we noticed how to apply some additional information in the field of Timing Analysis without vast any extra timing process. So the proposed hierarchical matcher has a matching time suitable for automated fingerprint verification systems. Pores and minutiae are matched using an elastic string matching algorithm which is capable of overcoming the errors introduced by feature extraction algorithms.

О ДЕКОДИРУЮЩИХ ВОЗМОЖНОСТЯХ НЕПРИМИТИВНЫХ КОДОВ ХЕММИНГА

В.А. ЛИПНИЦКИЙ, Е.Б. МИХАЙЛОВСКИЙ

Защита информации от несанкционированного доступа вызывает наибольший интерес в научных и околонаучных кругах. Однако для всех телекоммуникационных систем (ТКС) наиболее актуален другой аспект защиты информации — противодействие всякого рода помехам и шумам, неизбежно засоряющим реальные каналы передачи и системы хранения информации. Поэтому все современные ТКС (за исключением волоконно-оптических) обязательно функционируют с применением помехоустойчивых кодов, синхронно исправляющих возникающие ошибки и искажения информации.

Применение помехоустойчивых кодов сопряжено с определенной проблемой: повышение кратности исправляемых ошибок влечет за собой снижение скорости декодирующих устройств, что недопустимо при постоянном росте информационных потоков. Разрешение этого противоречия неизбежно приводит к преодолению «проблемы селектора» — необходимости перебора огромного количества возможных ошибочных комбинаций. Исторически первые коды — коды Хемминга, называемые также примитивными [1, 2], несмотря на свою совершенность, исправляют только одну ошибку на каждый блок передаваемой информации.

Непримитивные коды Хемминга, получаемые из примитивных достаточно широкого спектра координат с сохранением цикличности, ведут себя хаотично. Тем не менее, компьютерные исследования показали, что непримитивные коды Хемминга, длины которых не имеют малых простых делителей, могут иметь минимальное расстояние, превышающее конструктивное, равное, как известно, трем [1].

Построен ряд непримитивных кодов Хемминга с минимальным расстоянием, принимающим значения 5, 7, …, 15. Результаты проведенного исследования свидетельствуют о перспективности применения данных кодов в реальных ТКС.

Литература

1. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. Пер. с англ. М., 1979.

2. Липницкий В. А., Конопелько В. К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.

ОСОБЕННОСТИ КОРРЕКЦИИ ОШИБОК КОДАМИ С МАЛЫМ КОНСТРУКТИВНЫМ РАССТОЯНИЕМ

В.А. ЛИПНИЦКИЙ, А.О. ОЛЕКСЮК

В современных инфокоммуникационных системах защита информации стоит на одном из первых мест. Проблему составляют не только конфиденциальность передаваемой информации, но и защита ее от помех. Реальные каналы связи неизбежно содержат различного рода шумы и помехи, что сказывается на точности и достоверности передаваемой информации.

Современные ИКС, как правило, снабжены устройствами, применяющими помехоустойчивые коды. Экспоненциальный рост информационных потоков предъявляет все более жесткие требования к применяемым помехоустойчивым кодам, в сторону увеличения кратности корректирующих и повышения скорости работы декодирующих устройств.

Массовые применения в высокоскоростных системах связи приобрели БЧХ-коды (сотовая связь, диспетчерские службы и др.), как правило, примитивные [1]. Однако декодеры на их основе слабо адаптируются к повышению кратности корректируемых ошибок [1, 2].

Проведенные исследования показали, что существуют, и в достаточно большом количестве, не примитивные БЧХ-коды, имеющие невысокое конструктивное расстояние, но существенно большее реальное минимальное расстояние.

в докладе обсуждаются алгоритмы быстрого декодирования многократных ошибок не примитивными БЧХ-кодами с конструктивным расстоянием 5.

Литература

1. MacWilliams F.J., Sloane N.J.A. The Theory of Error-Correcting Codes. North-Holland Mathematical Library. 1977. Vol.16. 762 p.
2. Липницкий В. А., Конопелько В. К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.

АНАЛИЗ АНАЛОГО-ЦИФРОВОЙ СИСТЕМЫ ФАЗОВОЙ СИНХРОНИЗАЦИИ

С.А. ГАНКЕВИЧ

Анализируется цифровая система фазовой синхронизации (ЦСФС) с астатизмом второго порядка, с управляемым генератором, выполненным в виде аналоговой системы фазовой автоподстройки частоты (ФАПЧ), включенной в основной контур ЦСФС. Эталонный сигнал для ФАПЧ формируется высокостабильным задающим генератором (ЗГ). Формирование эталонного и опорного сигналов в управляемом генераторе производится методом нониуса, что позволяет уменьшить дискрет подстройки фазы без увеличения частот ЗГ и генератора, управляемого напряжением (ГУН), и за счет этого повысить точность синхронизации. Коррекция фазы опорного сигнала, формируемого ГУН, производится по сигналу ЗГ и сигналу фазовой ошибки в основном контуре. Фильтрующие свойства ЦСФС обеспечиваются основным узкополосным контуром

слежения. В качестве ФНЧ используются изодромное звено в основном контуре и пропорционально-интегрирующее звено в контуре управляемого генератора.

Приводятся результаты анализа математической модели по основным показателям качества и результаты моделирования. Определены требования к параметрам контуров слежения с целью обеспечения заданных показателей устойчивости, точности и быстродействия. Обеспечивая более высокие показатели точности по сравнению с системой с астатизмом первого порядка [1], анализируемая система более критична к выбору ФНЧ, удовлетворяющему требованиям устойчивости. В частности, ФНЧ в виде апериодического звена в контуре управляемого генератора не удовлетворяет этим требованиям.

Литература

1. Ганкевич С.А. Технические средства защиты информации: Тезисы докладов IX Белорусско-российской научно технической конференции, 28–29 июня 2011 г., Минск. Минск: БГУИР, 2011.С. 26.

МЕТОДИКА ПОЛУЧЕНИЯ ИСТИННО СЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ

К.В. ГУБЧИК, А.А. ИВАНЮК

Последовательности случайных чисел (СЧ) являются необходимым инструментом решения многих задач защиты информации (протоколы аутентификации, генерация сессионных ключей, защита авторских прав и др.). В работе [1] был предложен метод реализации физически неклонируемой функции (ФНФ) на базе статического ОЗУ (СОЗУ), который основан на анализе начального состояния памяти при включении питающего напряжения. Недостаток разработанного метода: большинство ячеек СОЗУ принимают одно из состояний чаще, чем другое, поэтому нарушается требование непредсказуемости данного физического отпечатка [1]. Чтобы обойти эту проблему, предлагается методика использования сигнатуры памяти вместо физического отпечатка памяти. При этом, зная сигнатуру, практически невозможно предсказать исходный физический отпечаток памяти. Это происходит за счет сжатия с потерями исходной ЧП при помощи алгоритма формирования сигнатур (LFSR-анализатор, CRC-анализатор, адаптивный сигнатурный анализатор [2]). Полученная сигнатура может использоваться в качестве начального состояния генератора СЧ, когда не требуется высокой скорости генерации СЧ. Создание ГИСЧ (генератора истинно случайных чисел) является актуальной проблемой в областях защиты информации, т. к. в них требуются истинно случайные и невоспроизводимые числа, при этом сами генераторы должны обладать свойством неклонируемости как для различных технологий, так и для идентичных устройств, выполненных по единой технологии. В качестве источника случайности предлагается использовать сигнатуру состояния памяти, что позволит обеспечить высокие требования к качеству ЧП, формируемых при помощи ГИСЧ.

Литература

1. Holcomb D.E., Burleson W.P., Fu K. IEEE Transactions on Computers, September 2009. P. 1198–1210.

2. Иванюк А.А., Петроненко Д.С. Доклады БГУИР. 2004. № 4. С. 84–92.

АППАРАТНЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ

Г.В. ДАВЫДОВ, А.И. КУХАРЕНКО, В.А. ПОПОВ, А.А. ТЕРЕНЯ

Генераторы случайных чисел (ГСЧ) широко применяются для создания криптостойких паролей, ключей шифрования, защиты каналов передачи данных и др. Удобно реализовать генератор случайных чисел программными средствами. Однако существует опасность, что алгоритм формирования случайных чисел станет известен нарушителю. Поэтому в системах защиты информации предпочтительно использовать аппаратные генераторы случайных чисел.

Важно при создании ГСЧ использовать источник случайного процесса с высокой энтропией. Известно, что максимальной энтропией при прочих равных условиях обладает так называемый «белый» шум.

Для получения «белого» шума в разработанном ГСЧ использован тепловой шум диода. После усиления шумового сигнала он преобразовывался в цифровую форму с помощью восьмибитового АЦП, выполненного на базе микроконтроллера AT90USB1286. Оцифрованный сигнал передавался по шине USB на персональный компьютер. С помощью программного пакета HEX Editor выполнена оценка плотности распределения вероятностей оцифрованного сигнала по его реализации длительностью 30 мин (6400000 выборок). Получена гистограмма этой оценки. Установлено, что сформированный цифровой «белый» шум имеет распределение вероятностей, близкое к гауссовому.

Конечной целью работы было создание ГСЧ с равномерным распределением цифрового сигнала в диапазоне чисел от 0 до 255. для этого из восьмибитовой выборки цифрового «белого» шума брался один младший разряд. Из полученных n младших разрядов формировалось n-битное значение случайной величины. Получено распределение случайных чисел сформированных из младших разрядов 8-ми разрядных выборок оцифрованного «белого» шума.

Для получения более равномерного распределения случайных величин был разработан специальный алгоритм. Суть алгоритма: из восьмибитовой выборки оцифрованного «белого» шума берётся один младший разряд. Полученные n младшие разряды суммируются по модулю 2. Из вычисленных k значений формировалось k-битное значение случайной величины. По полученным графикам можно судить о степени равномерности распределения случайных чисел. Стоит отметить, что данный алгоритм заметно улучшает распределение, но при этом снижает скорость генерирования последовательности случайных чисел.

Разработанный ГСЧ планируется использовать при создании синтезаторов речеподобных сигналов для систем защиты речевой информации.

АНАЛИЗ КРИТЕРИЕВ ДЕТЕКТИРОВАНИЯ РЕЧИ

ДМ.А. БОРИСЕВИЧ, Г.В. ДАВЫДОВ

Детектор речи предназначен для разделения речи и не речевых сигналов (например, звуковых вызовов факсов, модемов и телефонов, музыки, атмосферных звуковых помех, шума транспорта, длительных пауз в речевых сообщениях и других акустических сигналов, не являющихся речевыми). Детектор речи является необходимым устройством для многих современных устройств телекоммуникаций и средств защиты информации для отделения речи от пауз и сжатия сигналов путём удаления не речевых участков, удаления окружающих шумов во время пауз

при передаче речи по каналам коммуникаций, контроля время разговора без оператора в устройствах коммуникаций и других приложениях.

В работе рассмотрены следующие критерии детектирования речи: критерий мощности сигнала, критерий количества пересечений с нулем, критерий динамики изменения мощности сигнала, критерий особенностей речевого сигнала в спектральной области, критерий стационарности, критерий по шлейфу сигнала. Для каждого критерия описан алгоритм применения критерия с возможными параметрами реализации. Детально рассмотрен критерий по шлейфу сигнала, позволяющий детектировать сигналы типа речь, музыка, транспортный шум.

Детектор речи может быть оптимизирован по точности, скорости выполнения задачи, или в некоторой степени компромисса между ними. Наиболее часто детекторы речи требуют больших вычислительных мощностей вследствие использования для анализа большого числа признаков с применением комплексных вычислений. Показано, что использование ограниченного числа критериев детектирования речи и простейших методов обработки позволяют использовать такие алгоритмы детектирования в микропроцессорных устройствах при работе в реальном режиме времени.

ДЕТЕКТИРОВАНИЕ РЕЧИ РУССКОЯЗЫЧНОГО ДИКТОРА-БИЛИНГВА

Е.О. БАРАНОВСКИЙ

Современные условия жизни общества сопряжены со значительной миграцией населения, в связи с чем много людей пользуются в общении двумя и более языками. Способность владения двумя и более языками называется билингвизмом. Билингвизм является предметом изучения различных наук, каждая из которых рассматривает билингвизм в своей трактовке. В произношении билингвов присутствует явление интерференции (отрицательное влияние одного языка на другой), которое является предметом исследования для систем детектирования речевых сигналов.

Детектирование речи является важной частью современных приложений по обработке речевых сигналов. Алгоритмы детектирование речи используется в системах кодирования и распознавания речи, а также в системах повышения ее качества. Алгоритмы детектирования часто являются наиболее критической частью таких систем, и определяют качество всей системы в целом.

В основе большинства методов обработки речи лежит предположение о том, что свойства речевого сигнала с течением времени медленно изменяются. Это предположение приводит к методам кратковременного анализа, в которых сегменты речевого сигнала выделяются и обрабатываются так, как если бы они были короткими участками отдельных звуков с отличающимися свойствами.

Методика детектирования основана на вычислении мел-частотных кепстральных коэффициентов слов русского языка. В ходе работы были проанализированы слова русского языка, которые произносились различными дикторами. Одним из дикторов был носитель русского языка. В качестве второго диктора выступал диктор-билингв (русскоязычный диктор арабского происхождения). Результаты соответствия вычисляются при помощи алгоритма динамического программирования.

Для того чтобы получить векторы признаков одинаковой длины, нужно сегментировать речевой сигнал на равные части, а затем выполнять преобразования внутри каждого сегмента. Обычно сегменты выбирают таким образом, чтобы они

перекрывались либо наполовину, либо на 2/3. Перекрытие используется для предотвращения потери информации о сигнале на границе.

Для вычисления мел-частотных кестральных коэффициентов, на вход алгоритма подаётся последовательность отсчётов участка сигнала, исследуемого на данной итерации. К данной последовательности применяется весовая функция и затем дискретное преобразование Фурье. Весовая функция используется для уменьшения искажений в Фурье анализе, вызванных конечностью выборки. В качестве весовой функции используется окно Хэммига.

Полученное представление сигнала в частотной области разбивают на диапазоны с помощью банка треугольных фильтров. Границы фильтров рассчитывают в шкале мел. Данная шкала является результатом исследований по способности человеческого уха к восприятию звуков на различных частотах. Перевод в мел-частотную область осуществляется по формуле $B(f)=1127\ln(1+f/700)$.

Количество мел-частотных кепстральных коэффициентов определяется количеством треугольных фильтров. Фильтры применяются к квадратам модулей коэффициентов преобразования Фурье. Полученные значения логарифмируются. Заключительным этапом в вычислении мел-частотных кепстральных коэффициентов является дискретное косинусное преобразование.

ТЕСТИРОВАНИЕ НА ПРОСТОТУ БОЛЬШИХ ЧИСЕЛ СПЕЦИАЛЬНОГО ВИДА

А.В. ИВАШКЕВИЧ, Е.Д. СТРОЙНИКОВА

С целью создания генератора псевдопростых чисел были реализованы следующие тесты проверки чисел на простоту: Ферма, Миллера–Рабина, Соловея–Штрассена, Лукаса, BPSW. Первые три указанных теста являются вероятностными. Они позволяют очень эффективно отбраковать составные числа, однако не в состоянии строго доказать простоту числа, а лишь позволяют говорить, что число p не является составным с некоторой вероятностью. Наиболее эффективным из этих трех алгоритмов является тест Миллера–Рабина.

Верхняя граница ошибки на одной итерации для теста Миллера–Рабина в 2 раза меньше аналогичной для теста Соловея–Штрассена и в 4 раза — верхней границы ошибки для теста Ферма. Если на одной итерации вероятность ошибочного решения в тесте не превышает 1/4, то на двух итерациях — 1/16, на трех — 1/64. для того чтобы вероятность ошибки не превышала 0,0001, требуется всего 7 итераций, что в 2 раза меньше, чем для теста Соловея–Штрассена.

На основании вышеуказанных алгоритмов был разработан программный модуль генерации простых чисел заданной длины. Для его создания была использованна среда Microsoft Visual Studio 2010 и язык программирования C#.

Основной сложностью при создании модуля генерации стала реализация алгоритмов проверки чисел на простоту.

В результате выполенной работы были получены следующие средние временные результаты генерирования псевдопростых чисел: число длиной 256 бит было сгенерированно за 1 секунду, 512 бит — за 2–3 секунды, 1024 бит — за 55 секунд, 2048 бит — за 600 секунд, 3076 бит — за 7200 секунд.

Созданный программный модуль имеет очень важное практическое применение, так как простые числа являются неотъемлемой частью криптографических алгоритмов, используемых для защиты информации.

АРХИТЕКТУРА МНОГОКАНАЛЬНЫХ КВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

К.В. МЕЛЬНИКОВ, С.Б. БИРЮЧИНСКИЙ

Одним из основных недостатков современных систем квантовой криптографии является низкая скорость передачи данных, что обусловлено как техническими ограничениями для существующих систем, так и ограничениями, вызванными применяемыми алгоритмами. Использование систем с малой скоростью передачи данных не позволяет полностью реализовать все возможные методы криптографической защиты.

Для обеспечения наивысшего уровня секретности в симметричных криптосистемах необходимо формировать последовательность криптографического ключа с длиной, равной длине передаваемого сообщения.

Поскольку скорость передачи данных в существующих системах квантовой криптографии низка, устойчивость систем к шумовым воздействиям является слабой.

Одним из способов повышения скорости передачи информации является переход к многоканальным системам. Авторами предложены варианты архитектуры различных многоканальных систем связи, использующих квантовую криптографию.

Одним из методов перехода к многоканальности в квантовых криптографических системах является одновременное использование на передающей стороне нескольких источников фотонов с различными длинами волн, передаваемых по одному и тому же каналу связи. Разделение фотонов по частоте в этом случае осуществляется классическими методами спектральной селекции. Преимуществами являются простота реализации системы.

Возможным направлением развития является использование псевдо-квантовокриптографических систем. Реализация такой системы основана на использовании традиционных каналов связи, как волоконно-оптических, так и атмосферных оптических линий связи.

Разработана оптическая схема детектирования направления поляризации фотона, позволяющая определить поляризацию единичного фотона с вероятностью выше 50%. Предложен способ повышения точности определения поляризации фотона.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ НЕДОКУМЕНТИРОВАННОГО ОТЛАДОЧНОГО РЕЖИМА ПРОЦЕССОРОВ ФИРМЫ AMD НА БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Е.Е. ОРЛОВ, О.К. БАРАНОВСКИЙ

Аппаратное обеспечение современных компьютерных систем создается путем интеграции большого числа базовых компонент (модулей). Сложность таких систем является причиной того, что выполняемые аппаратным обеспечением функции могут не соответствовать заявленным в спецификации. Эти отличия могут вноситься преднамеренно, например, недокументированные возможности, внедряемые для послепроизводственного тестирования компаниями-производителями, или для проведения вредоносной деятельности, либо быть вызванными ошибками в технологиях разработки и производства.

Характерным примером ошибки в аппаратном обеспечении может являться проблема с когерентностью L1 кэша многоядерных процессоров Intel Core 2 Duo [1].

Предложены сценарии атак отказа в обслуживании на основе управления модельно-специфическими регистрами, являющимися механизмом перевода компьютерных систем в недокументированный отладочный режим. Условием срабатывания упомянутых выше сценариев является обработка компьютером определённого числа.

Показано, что при некорректной настройке этого режима возможен управляемый сбой работы операционной системы. Предложенные сценарии были также реализованы на виртуальных машинах и продемонстрировали успешность атак.

Литература

1. Касперский К. Дефекты проектирования Intel Core 2 Duo / [Электронный ресурс]. Режим доступа: http://www.insidepro.com/kk/286/286r.shtml. Дата доступа: 05.04.2012.

МАРШРУТИЗАЦИЯ ПО ТРЕБОВАНИЮ С МНОЖЕСТВЕННЫМИ ПУТЯМИ НА ОСНОВЕ ВЕКТОРА РАССТОЯНИЙ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

А.А. ОХРИМЕНКО, С.Б. САЛОМАТИН

Ключевой особенностью беспроводных сенсорных сетей является способность ретрансляции сообщений от одного сенсорного узла к другому, что позволяет передавать информацию на значительное расстояние при малой мощности передатчиков.

При выборе алгоритма маршрутизации в беспроводных сенсорных сетях необходимо учитывать ограниченность вычислительных ресурсов сенсорных узлов и срок службы элементов питания. Одним из таких алгоритмов является протокол маршрутизации по требованию на основе вектора расстояний (AODV), который исключает периодическое обновление маршрутов и использует их только при необходимости.

Протокол AODV является эффективным с точки зрения производительности сети, однако позволяет злоумышленнику легко фальсифицировать маршрутную информацию для перенаправления трафика и запуска DoS-атак. Таким образом, для предотвращения подобного рода воздействий, существует необходимость защиты маршрутной информации от несанкционированных узлов.

Для повышения устойчивости к разрыву соединений предлагается использовать протокол маршрутизации по требованию с множественными путями на основе вектора расстояний (AOMDV), в котором маршруты рассчитываются таким образом, чтобы гарантированно отсутствовали петли маршрутизации и пересекающиеся пути.

Следует также отметить, что протокол AOMDV обеспечивает промежуточные сенсорные узлы альтернативными маршрутами, что способствует сокращению частоты обнаружения маршрутов, экономии ресурсов сенсорных узлов и уменьшению нагрузки на беспроводную сенсорную сеть.

ФОРМИРОВАНИЕ РОБАСТНОГО ПОДХОДА К УПРАВЛЕНИЮ ПРИОРИТЕТАМИ ПРИ ОБНАРУЖЕНИИ И ПРОТИВОДЕЙСТВИИ КОМПЬЮТЕРНЫХ АТАК

Д.А. КОМЛИКОВ

Сформулируем постановку задачи "инвариантного" управления приоритетами в условиях изменения характеристик задающего воздействия (формировании стратегии организации прерывания воздействий компьютерных атак (далее — КА) на объекты информационных технологий (далее — ИТ) информационных систем (далее — ИС)) с точки зрения робастного подхода.

Рассмотрим возможность получения экстраполированных оценок (оценок при рассмотрении которых система принятия решений (далее — СПР) не имеет возможности активной коррекции и вмешательства извне) законов изменения воздействия КА и внедрения враждебного кода (далее — ВК) на объекты ИТ ИС с приоритетной дисциплиной разделения временного ресурса дискриминатора. Рассмотрим структуру объектов ИТ ИС в виде парциального канала.

Основной задачей является разработка методики синтеза робастных управлений, корректирующих средние времена обслуживания и экстраполяции в зависимости от характеристик организации КА и внедрения ВК (в частном случае, величин характеризующих динамику процесса — скоростей и ускорений). Рассмотрим задачу управления защитой для не полностью определенных объектов ИТ ИС, подверженных воздействию возмущений в СПР с приоритетами и экстраполяцией как наиболее важную.

Не полностью определенный объект ИТ или объект ИТ в условиях ограниченной неопределенности можно рассматривать как семейство объектов ИТ ИС, которое определяется множествами принадлежности параметров или характеристик этого объекта ИТ, а также множествами принадлежности внешних возмущений. Таким образом, возникает задача управления не единственным объектом ИТ, а семейством или множеством объектов ИТ ИС, что необходимо при управлении средствами обнаружения и противодействия КА систем защиты информации (далее — СЗИ) ИС. Решение этой задачи при отсутствии внешних возмущений приводит к определению фиксированного управляющего средства, обеспечивающего устойчивость СПР для всего семейства объектов ИТ. Такие СПР называются робастно устойчивыми.

Актуальность придания СПР робастизирующих свойств продемонстрируем на примере неоднородности законов изменения скоростей и ускорений при моделировании воздействий КА на объекты ИТ в зависимости от их нахождения в зоне опасности, отслеживаемой фильтрами СПР для организации противодействия КА и противодействия внедрению ВК.

Исходные формулы для расчета: $\left|\dot{\varepsilon}\right| = \frac{V}{4}\sin^2\varepsilon$, $\left|\ddot{\varepsilon}\right| = \left|\dot{\varepsilon}\right|\frac{V}{4}\left|\sin 2\varepsilon\right|$.

При прогнозировании последствий КА и организации противодействия КА опишем модель для оценки влияния робастного управления на точность принятия решения для дискретного аналога СПР принятия решений с ПИ-управлением.

Пусть передаточная функция $K_{ии}(p)=K_{ии}/p$, а $\upsilon(t)$ — белый шум со спектральной плотностью N. в первом состоянии, когда ключ замкнут, уравнение СПР относительно ошибки управления

$$e^{(1)}(t) = -Ke^{(1)}(t) + \dot{x} - K_{ии}\mathrm{v}(t) \quad K = K_g K_{ии},$$

а во втором состоянии

$e^{(2)}(t) = \dot{x}, \quad \dot{x} = \text{const}.$

Составим уравнения для математических ожиданий в различных положениях ключа, для чего воспользуемся общей формой записи уравнений моментов. Так уравнения для математических ожиданий принимают вид:

$$\dot{m}^{(1)}(t) = -Km^{(1)}(t) + \dot{x}\,p^{(1)}(t) - v^{(1)}m^{(1)}(t) + v^{(2)}m^{(2)}(t),$$

$$\dot{m}^{(2)}(t) = \dot{x}\,p^{(2)}(t) - v^{(2)}m^{(2)}(t) + v^{(1)}m^{(1)}(t).$$

После математических преобразований уравнений с учетом того, что ошибкой в режиме обслуживания не пренебрегать, и она выступает как начальное значение для режима экстраполяции, то, устремив степень устойчивости к ∞, уравнения для математических ожиданий примут следующий вид:

$$m^{(1)}(z) = 0,5z^{-1}m^{(1)}(z) + 0,5\,p^{(1)}\left(v^{(1)}, v^{(2)}\right)V_0 - v^{(1)}z^{-1}m^{(1)}(z) + v^{(2)}z^{-1}m^{(2)}(z),$$

$$m^{(2)}(z) = z^{-1}m^{(2)}(z) + p^{(2)}\left(v^{(1)}, v^{(2)}\right)V_0 - v^{(2)}z^{-1}m^{(2)}(z) + v^{(1)}z^{-1}m^{(1)}(z).$$

В результате перегруппировки и преобразований с учетом степени робастного управления α и степени задержки Z, получим конечное выражение для математического ожидания $m^{(2)}(i)$ с учетом робастного управления:

$$m^{(2)}(i) = \frac{1}{1 - v^{(2)}\left(1 - v^{(2)}\right)}\left(\frac{V_0}{v^{(1)} + v^{(2)}}\left(v^{(1)}\left(1 - 3v^{(2)}\right) + \left(A - v^{(2)}\right)\left(1 + 3v^{(1)} + A\right)\right) - \right.$$

$$-m^{(2)}(i-1)\left(A + v^{(1)} - 0,5 - v^{(2)}\left(3 - 2v^{(2)} + v^{(1)}\right)\right) - m^{(2)}(i-2)\left(A\left(1 + v^{(1)} + A\left(1 - 2v^{(2)}\right) - \right.\right.$$

$$\left.\left.-2v^{(2)}\left(1 + v^{(1)} - 0,5v^{(2)} - 0,25\right)\right)\right) - m^{(2)}(i-3)\left(v^{(2)}\left(0,5 - v^{(2)}\right) + A\left(v^{(1)} - v^{(2)} - 0,5\right)\right)\Bigg),$$

где $A = \dfrac{\left(v^{(1)} + v^{(2)}\right) - v^{(1)}\left(1 - v^{(2)}\right) - v^{(2)}\left(1 + v^{(2)}\right)}{v^{(1)} + v^{(2)}}$.

Для доказательства эффективности робастного управления проведем сравнительную оценку выражений для $m^{(2)}(i)$ с робастным управлением и без него.

Зафиксировав значения $v_0^{(1)}$; $v_0^{(2)}$ и изменяя V_0, проведем моделирование и проанализируем устойчивость СПР к внешним возмущениям. Результаты моделирования подтверждают, что так же как и в СПР, где начальной ошибкой, обусловленной режимом обслуживания, пренебрегали, качество работы робастной СПР при обнаружении и противодействии КА на порядок выше чем "штатной", а робастизирующие свойства улучшают качество работы СПР при обнаружении и противодействии КА практически на два порядка.

К ВОПРОСУ АНАЛИТИЧЕСКОГО МОДЕЛИРОВАНИЯ DOS АТАК

Л.В. НОВИКОВА

Среди различного вида атак на информационные системы (ИС) особое место занимают DoS атаки. DoS атаки (Denial of Service, отказ в обслуживании) являются наиболее известной формой хакерских атак, против которых труднее всего создать стопроцентную защиту. Для организации DoS требуется минимум знаний и умений. Атака DoS делает ИС недоступной для обычного использования за счет превышения допустимых возможностей функционирования ИС.

В докладе приводятся результаты разработки и исследования моделей атак этого типа.

Процесс атаки рассматривается как случайный поток транзакций на ИС в течение времени атаки T. для исследования таких процессов обычно используются аналитические и имитационные модели массового обслуживания с блокировкой.

Обсуждаемая в докладе модель атак относится к классу аналитических моделей массового обслуживания с дискретным временем. Состояния модели рассматриваются в равноотстоящие интервалы времени Λt. Модель содержит генератор потока атак, блок моделирования глубины защиты (накопитель атак), блок моделирования защиты. В случае, когда ресурсы защиты исчерпаны, модель переходит в заблокированное состояние (накопитель атак заполнен, блок моделирования защиты занят устранением предыдущей атаки потока, ИС неработоспособна).

Для моделирования атак используется просеянный случайный поток, в котором с вероятностью π в момент модельного времени t атака происходит, и с вероятностью $1–\pi$ не происходит. Состояние потока в следующий момент наблюдения системы $t+\Lambda t$ не зависит от его состояния в момент t (поток без последействия). Глубина защиты моделируется накопителем атак, который может хранить в очереди до n атак. Параметр n будем называть глубиной защиты. Блок моделирования защиты при возникновении атаки в момент t с вероятностью ρ к моменту $t+\Lambda t$ устраняет ее, и вероятностью $1–\rho$ продолжает ее устранение. На интервале времени воздействия потока атак модель рассматривается как стационарная. В момент времени t может произойти одна атака (ординарность потока атак).

Использование моделей с блокировкой позволило определить:

– вероятность блокировки ИС (отказ в обслуживании);

– зависимость времени блокировки от эффективности (глубины) защиты;

– время нахождения ИС в заблокированном и рабочем состоянии в процессе атаки;

– вероятность нахождения ИС в рабочем (незаблокированном) состоянии в процессе атаки.

СЕГМЕНТАЦИЯ СКРЫТНЫХ ОБЪЕКТОВ ИЗОБРАЖЕНИЙ

А.И. МИТЮХИН

В ряде специальных приложениях требуется произвести оценку скорости движения скрытного объекта, направления его движения, пройденного расстояния. Предлагается сегментацию динамических изображений осуществлять на основе корреляционного подхода. Так, скорость можно оценить через промежуточное вычисление диадной корреляционной функции. Пусть имеется последовательность из K изображений $g_{x, y, t}$ с пространственными переменными (x, y) по оси x и по оси y двумерного евклидового пространства. Рассматривается подход анализа изображений на основе использования циклической группы с операцией диадного сдвига на конечных интервалах. С помощью операцией диадного сдвига формируются мажоритарные последовательности на диадной группе.

Проекции изображений каждого кадра на ось x (ось y) выразим линейной комбинацией мажоритарных последовательностей множества $\{a_i(t)\}$. В результате получается множество последовательностей $g_i=(t)$. Сдвигу изображения за временной интервал между двумя кадрами на $\tau_t=i$ пикселей по оси $x(y)$ будет соответствовать значение отсчета последовательности $g_i=(t)$. Величина сдвига $\tau_x=j$

будет пропорциональна составляющей скорости движения объекта в пикселях на кадр по оси x. Таким образом, для вычисления составляющей скорости по оси x следует найти значение τ_x. Определение сдвига сводится к сравнению последовательности $g(t)_x$ с каждой последовательностью множества $\{a_i\}$ и выбору ближайшей из них по расстоянию Хэмминга. Максимальное значение коэффициента $r_{t\,x}$ определяет величину τ_t. Следовательно, коэффициенты корреляции $\max r_{t\,x}$ формируются в точках с теми номерами t функций $g_{t,\,x}$, координаты которых пропорциональны скорости движения объекта. Аналогичные рассуждения справедливы для получения коэффициентов диадной корреляционной функции для направления y.

В работе представлены результаты анализа движения трудноразличимого (скрытного) объекта на изображениях, искаженных аддитивным шумом. Объем вычислений параметров движения можно существенно сократить, если воспользоваться структурными свойствами мажоритарных последовательностей множества $\{a_i(t)\}$ и их упорядочением определенным способом.

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ АППАРАТНЫЕ РЕАЛИЗАЦИИ ПРОЦЕССОРОВ АЛГОРИТМА ШИФРОВАНИЯ DES НА БАЗЕ ПЛИС С АРХИТЕКТУРОЙ FPGA

М.М. РОДИОНОВ, М.И. ВАШКЕВИЧ, А.А. ПЕТРОВСКИЙ,
А.В. СТАНКЕВИЧ, АЛ.А. ПЕТРОВСКИЙ, М.В. КАЧИНСКИЙ

Предлагаются два варианта аппаратной реализации процессора шифрования алгоритма DES на основе последовательной и конвейерной архитектуры. В последовательном процессоре все циклы алгоритма DES последовательно выполняются на одном вычислительном ядре (далее подход 1). За счет этого возможна экономия аппаратных ресурсов, что позволяет реализовать специализированный процессор со средней производительностью и сравнительно невысокими аппаратными затратами.

В конвейерной архитектуре каждый цикл шифрования реализуется на отдельной вычислительной ступени. Данный вариант позволяет получать выходные результаты в каждом такте работы специализированного процессора. В результате исследований реализаций конвейерного процессора на базе ПЛИС с архитектурой FPGA было установлено, что лучшие показатели производительности достигаются при использовании распределенной памяти кристалла ПЛИС (далее подход 2.1) вместо блочной памяти (далее подход 2.2) для хранения таблиц замен алгоритма DES. Также был реализован конвейерный процессор на основе известного модифицированного представления алгоритма DES (далее подход 2.3), в котором за счет математических преобразований две операции сложения по модулю два с двумя операндами заменяются на одну операцию с четырьмя операндами, что позволяет более эффективно использовать ресурсы ПЛИС.

Для кристалла xc5vlx110 были получены следующие характеристики (логические секции/максимальная тактовая частота, МГц): подход 1 — 151/200; подход 2.1 — 1063/374; подход 2.2 — 997/300, 32 блока памяти; подход 2.3 — 991/377.

Предложенные подходы могут использоваться в приложениях, требующих высокой производительности при шифровании данных.

ГИБРИДНЫЙ КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ ЗАЩИТЫ ДАННЫХ В СЕНСОРНОЙ СЕТИ

С.А. ПЛЕТНЁВ

В настоящее время одним из новых актуальных направлений в области информационных технологий является создание нового вида сетевых систем — сенсорных сетей. Сенсорная сеть — это распределенная сеть необслуживаемых миниатюрных электронных устройств (узлов сети), которые осуществляют сбор данных о параметрах внешней среды и передачу их на базовую станцию посредством ретрансляции от узла к узлу с помощью беспроводной связи. Одной из важнейших проблем данного подхода является обеспечение безопасности информации, циркулирующей в пределах сенсорных сетей с учетом ограниченных ресурсов.

Несмотря на важность передаваемой информации, обеспечение удовлетворительного уровня безопасности в сенсорных сетях никогда не было легкой задачей. Из-за того, что сенсорные сети не только подвергаются атакам злоумышленников, но также обладают многими ограничениями в ресурсах. Сенсорные узлы, исходя из архитектуры и условий применения, являются устройствами с ограниченными ресурсами. Они имеют ограниченные вычислительные, энергетические ресурсы и небольшой запас внешней памяти.

В качестве механизма информационной безопасности предлагается гибридный блочный алгоритм защиты данных, основанный на вычислении битовой последовательности OTP (one-time pad — одноразовый блокнот) в качестве одноразового секретного ключа и MAC(message authentication code — код аутентичности сообщения).

Значение MAC вычисляется с помощью криптографического блочного алгоритма SkipJack в режиме сцепления блоков шифротекста. Алгоритм вычисления MAC в режиме сцепления блоков шифротекста эффективен и быстр, и факт того что в его основе блочный шифр также минимизирует использование памяти, которая является ограниченным ресурсом в сенсорных сетях. При использовании гибридного алгоритма передаваемый пакет данных составляет 23 байта, как следствие, он не является ресурсоемким.

Данный алгоритм обеспечивает целостность, конфиденциальность и аутентичность данных и сенсора. Ключевая последовательность используется только один раз для каждого сеанса передачи данных. Криптостойкость алгоритма основана на криптостойкостях исходного мастер ключа и алгоритма при вычислении MAC.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

С.А. ПЛЕТНЁВ

Беспроводная сенсорная сеть представляет собой распределенную, самоорганизующуюся и устойчивую к отказу сеть большого числа малогабаритных (до нескольких десятков тысяч) автономных электронных узлов, способных обмениваться сообщениями и ретранслировать их по беспроводному каналу связи. Одной из важнейших проблем данной технологии является обеспечение безопасности информации.

Требования к защите информации в беспроводной сенсорной сети можно классифицировать следующим образом:

Аутентификация: Поскольку в WSN передается важная критическая информация. Получатель должен удостовериться в том, что принятая информация получена от авторизованного источника.

Целостность: Данные при передаче могут быть изменены нарушителем. Потеря или повреждение данных может также произойти из-за ненадежной коммуникационной среды. Целостность данных гарантирует, что информация не изменена при передаче.

Конфиденциальность данных: Конфиденциальность гарантирует, что содержание сообщения, которое передается, никогда не раскрывается несанкционированным объектам. Шифрование является стандартным подходом для обеспечения конфиденциальности.

Сенсорные узлы, исходя из архитектуры и условий применения, являются устройствами с ограниченными ресурсами. Они имеют ограниченные вычислительные, энергетические ресурсы и небольшой запас внешней памяти.

На данный момент существуют протоколы безопасности, которые соответствуют ограничениям WSN и обеспечивают защиту от некоторых типов угроз. Основным из них является протокол безопасности в сенсорных сетях SPINS. Протокол SPINS обеспечивает криптографическую защиту информации на прикладном уровне и состоит из протокола SNEP и μTESLA. Протокол SNEP обеспечивает конфиденциальность, целостность и аутентичность данных. Протокол μTESLA обеспечивает аутентификацию данных при широковещательной рассылке по сети.

Криптографической основой протокола SNEP является блочный шифр RC5, изобретенный Р. Ривестом в 1995 году. Данный шифр очень непритязателен с точки зрения вычислительной мощности и требуемого объема памяти и поэтому хорошо подходит для применения в сенсорных сетях.

ИСПОЛЬЗОВАНИЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ ДЛЯ ЗАЩИТЫ ЦИФРОВЫХ УСТРОЙСТВ, РЕАЛИЗУЕМЫХ НА ПЛИС

А.А. ПРОЩЕРЯКОВ, А.А. ИВАНЮК

Использование программируемых логических интегральных схем (ПЛИС) в качестве элементной базы цифрового устройства предполагает возможность внесения изменений в синтезируемый проект как на этапе описания его на HDL-языках, так и уже в реализованный проект. Данный аспект позволяет злоумышленникам внести собственные вредоносные элементы в созданный проект, внедрять так называемые аппаратные трояны (Hardware Trojans), которые могут исказить функционирование цифрового устройства либо получить доступ на аппаратном уровне к конфиденциальной информации. В связи с этим актуальной является задача проектирования цифровых устройств, которые в автономном режиме проверяли бы целостность не только обрабатываемых данных, но и своей аппаратной составляющей. Данная методика проектирования получила название Design For Trust (DFT).

В качестве одного из походов к решению задач DFT предлагается применение физически неклонируемых функций (PUF, Physical Unclonable Function), которые основаны на использовании непредсказуемых и невоспроизводимых отклонений в физической структуре интегральных схем при их изготовлении. Внедрение специализированных типов PUF позволит решить следующие задачи: идентификация цифровых устройств, идентификация ПЛИС, аутентификация

цифровых устройств при их реализации на ПЛИС, защита цифровых устройств от клонирования на идентичных ПЛИС, защита цифровых устройств от несанкционированных изменений.

ШИФРОВАНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ФАЗОВОЙ СИНХРОНИЗАЦИИ

Д.Л. ШИЛИН, С.С. БЫВШЕВ, М.В. ПОЧЕБУТ

Авторами предлагается способ шифрования данных с использованием систем фазовой синхронизации (СФС), работающих в режиме детерминированного хаоса. Данный режим работы является нерегулярным. Причина нерегулярности определяется свойством нелинейных систем экспоненциально быстро разводить первоначально близкие траектории. Поэтому не представляется возможным предсказать поведение таких систем, так как реально начальные условия можно задавать лишь с конечной точностью, а ошибки экспоненциально возрастают.

Предлагается на основе ранее разработанной имитационной модели СФС создать систему шифрования информации для передачи последней по открытым каналам связи. В качестве случайных последовательностей будут использоваться значения фазы и частоты сигнала на выходе блока фильтров модели. Будет использован симметричный алгоритм шифрования, в котором шифрование и дешифрование отличается только порядком выполнения и направлением некоторых шагов. В этом алгоритме авторами предлагается использовать один и тот же секретный ключ — физические параметры работы модели. С точки зрения простоты реализации, наиболее привлекательным является двоичное (битовое) гаммирование. Обычно, при использовании гаммирования, если гамма короче, чем открытое сообщение, она повторяется требуемое число раз. В нашем случае, в этом нет необходимости, так как возможно сгенерировать гамма последовательность необходимой длины. Этот аспект позволяет построить поточную систему шифрования данных, которая сможет передавать поток данных, каждый символ которых должен быть зашифрован и отправлен куда-либо, не дожидаясь последующих данных (обмен текстовыми и голосовыми сообщениями по сети).

При кодировании файла целиком (без учета структуры), снижается криптостойкость шифра. Это объясняется тем, что многие файлы помимо основных данных, хранят однородные данные о формате. Поэтому для некоторых форматов файлов целесообразно шифровать только основные данные.

СИСТЕМА КОНТРОЛЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ БУРОВОЙ УСТАНОВКИ

М.В. ПОЧЕБУТ, Ю.В. ВОРОБЬЕВА

Для обеспечения операций бурения используются дизельные двигатели большой мощности. Ежедневно мастер готовит отчет о работе технологического оборудования на буровой установке и по телефону докладывает информацию в диспетчерскую службу бурового предприятия. Такой контроль сложно назвать надежным, так как присутствует человеческий фактор, влияющий на достоверность передаваемой информации.

Целью данного проекта является проектирование системы по обеспечению оперативного мониторинга и контроль в режиме ON-LINE работы, к примеру, всех

дизельных двигателей на буровой, что в свою очередь позволяет прямо и косвенно контролировать технологические процессы бурения, формировать ежедневные отчеты о работе дизельных двигателей на буровой и расходе дизельного топлива без участия мастеров.

Для контроля оборотов двигателя на этих дизелях используются электрические тахометры. Удаленный мониторинг работы дизельного двигателя производится по данным полученным с тахометра. Для измерения сигналов тахометра и передачи данных используется контроллер UAB TELTONIKA FM4200. Он содержит аналоговые входы для измерения напряжения тахометров дизельных двигателей, напряжения в электросети буровой установки (контроль дизель электростанции) и GPRS канал для передачи данных.

FM4200 это терминал с GPS и GSM соединением, который способен распознавать координаты и передавать их используя ресурсы GSM сетей. Прибор имеет входные и выходные параметры, которые позволяют следить и управлять другими приборами объекта.

Использование микроконтроллера более надежно, так как процесс полностью автоматизирован, производится экономия материальных средств за счет сокращения рабочих кадров, существует доступ к данным в любой момент времени, данные передаваемые по GRPS каналу доступны только администратору, не играет роли человеческий фактор, тем самым сводится к нулю риск кражи топлива, риск получения ложных данных, процесс может контролироваться удаленно, а также контроллер отличается низким энергопотреблением.

СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ УСТРОЙСТВ ФАПЧ

Д.Л. ШИЛИН, М.В. ПОЧЕБУТ

Разработанная система представляет собой симметрично-поточную криптосистему, в которой шифрование проводится над каждым байтом исходного текста с использованием гаммирования. Источником гамма-последовательности является система фазовой автоподстройки частоты, работающая в режиме детерминированного хаоса. Безопасность системы полностью зависит от свойств генератора потока ключей. Если он реализуется на конечном автомате, последовательность со временем повторится. Практически все генераторы псевдослучайных последовательностей за исключением одноразовых блокнотов являются периодическими. Поэтому, поток ключей должен иметь более длинный период, чем количество битов, выдаваемых между сменой ключей. Генератор должен выдавать одну и ту же гамма-последовательность и для шифрования, и для дешифрирования. Поэтому важным моментом является однократное использование гамма-последовательности, следовательно, необходима синхронизация передающего и принимающего устройств. Для этих целей предлагается использовать самосинхронизирующееся потоковое шифрование. Так как внутреннее состояние генератора потока ключей является функцией предыдущих N битов шифротекста, то расшифрующий генератор потока ключей, приняв N битов, автоматически синхронизируется с шифрующим генератором. Последовательности чисел, получаемые при помощи генератора на основе устройства фазовой автоподстройки частоты, работающем в режиме детерминированного хаоса, были протестированы на случайность.

Были использованы статистические NIST, DIEHARD. Также тестирование проводилось по критериям сериальной корреляции, частот, интервалов, серий.

В исследовании использовались выборки объемом до 400000 бит. При рассмотрении массива ключей большего объема наблюдалась периодичность выпадения значений.

БЕЗОПАСНОЕ ПРЕРЫВАНИЕ ПРОЦЕДУР МЕТОДА ДИНАМИЧЕСКОГО ПРОГРАММИРОВАНИЯ

М.П. РЕВОТЮК, М.К. КАРОЛИ

Процедуры метода динамического программирования, базирующиеся на использовании принципа последовательной декомпозиции задачи, пригодны для естественного распараллеливания на вычислительных сетях. Управление потоками порождаемых подзадач при нерегламентированном режиме доступности рабочих станций на сети общего назначения порождают необходимость надежного решения проблемы грануляции и синхронизации подзадач с гарантией решения исходной задачи. Предмет рассмотрения — способ представления в произвольный момент состояния процесса решения задачи с целью последующего восстановления состояния и продолжения процесса решения на любом доступном узле сети.

Ключевой элемент инварианта представления состояния процесса решения задачи определяется алгоритмом порождения дерева вариантов. Такой алгоритм часто допускает свободу перечисления ветвей дерева, что предлагается использовать для встраивания процедур сохранения и восстановления состояния. Например, цель решения известной задачи коммивояжера — поиск гамильтонова цикла минимальной длины. Рекурсия обхода дерева подзадач здесь реализуется генератором перестановок с мемоизацией состояния.

Предлагается вариант генерации перестановок с минимальным изменением. Набор переменных состояния процесса ветвления, следуя схеме динамического программирования, определяется вектором текущей перестановки. Установлено, что ветвление на любом уровне возможно с сохранением порядка следования элементов перестановок. Глубина ветвления не превосходит значения, поэтому активные ветви дерева порождаемы из вектора состояния генератора перестановок. Отсюда следует, что для возобновления поиска решения после прерывания требуется память объемом, включающая вектор перестановки лучшего гамильтонова цикла, вектор представления вершин пути от корня дерева до листьев и вектор позиций ветвей дерева.

БЕЗОПАСНОЕ ПРЕРЫВАНИЕ ПРОЦЕДУР МЕТОДА ВЕТВЕЙ И ГРАНИЦ

М.П. РЕВОТЮК, П.М. БАТУРА, Р. ХОРМОЗИ

Предмет рассмотрения — способ компактного представления в произвольный момент состояния задачи, решаемой методом ветвей и границ с распараллеливанием, для последующего восстановления состояния и продолжения процесса решения на любом доступном узле вычислительной сети.

В любой момент времени на дереве вариантов можно выделить путь от его корня к листу. Это путь обычно представлен неявно стеком локальных переменных рекурсивно вызываемых функций анализа отдельного узла. Возможность выделения пути от его корня дерева к листу в произвольный момент прерывания появится лишь после дополнения переменных состояния указателем на их предыдущий экземпляр. Предлагается такое дополнение оформить объектом класса в рамках объектных технологий, автоматизируя функциональное замыкание

интервала перехода между смежными уровнями дерева вариантов. Локальный фрагмент переменных состояния включаются в список конструктором такого класса непосредственно после выделения памяти. Исключение из списка производится деструктором перед освобождением памяти.

Переход между уровнями ветвления дополняется операциями в рассматриваемом классе для синхронной обработки прерываний. Альтернативы ветвления представимы инкрементом вектора состояния на предыдущем уровне. Возврат процесса в предшествующее состояние реализуется операцией декремента. Сохранение состояния процесса решения реализуется сканированием списка и выводом, например, в файловый поток. Это удобно синхронизировать с моментом обработки листа дерева вариантов.

Таким образом, состояние процесса решения оказывается представленным удобным для его миграции и дальнейшего распараллеливания системно-независимым и проблемно-ориентированным способом. Иллюстрация применения предлагаемой технологии проводится на примере задачи коммивояжера.

БЕЗОПАСНОЕ ОБСЛУЖИВАНИЕ ПОТОКОВ ЗАПРОСОВ ПРОЦЕДУРАМИ ОБЛАЧНЫХ СЕРВИСОВ

М.П. РЕВОТЮК, В.В. ЗОБОВ

Решение многих задач информационно-справочного характера или координации взаимодействия дискретных систем формально связано с систематическим поиском путей на графах и выборкой результатов поиска. Несложно показать, что в случае интенсивного изменения графа по причине полиномиальной сложности алгоритма поиска путей предпочтительной оказывается организация поиска непосредственно после получения запроса вместо выборки строк априорно подготовленной матрицы с результатами выборки. В результате реактивность сервиса обслуживания запросов должна улучшиться, однако возникает проблема обеспечения конфиденциальности — стандартный механизм олицетворения при доступе к результатам выборки становится узким местом.

Предмет обсуждения — схема обслуживания запросов процедурами облачных сервисов без буферизации результатов выборки, когда отсутствие корреляции между переменными представления фаз обслуживания клиента в области ввода-вывода интерфейсов сервиса гарантирует требуемый уровень конфиденциальности.

Основа предлагаемой схемы обслуживания — распараллеливание волновых процедур поиска леса путей среди элементов пула рабочих потоков сервиса. Каждый рабочий поток должен императивно выполнять планирование перехода из текущей вершины графа до всех смежных выходных вершин и прерывать процесс при достижении целевой вершины. Результат поиска должен сохраняться в локальной памяти потока, защита которой обеспечивается общесистемными механизмами.

Таким образом, состояние процесса решения недоступно для наблюдения потоками, связанными с субъектами обслуживания. Дополнительное преимущество рассмотренной схемы — сокращение вычислительной сложности синхронизации событий процесса поиска путем сокращения холостых просмотров горизонта планирования.

ПРОГРАММНЫЕ СРЕДСТВА СИНТЕЗА РЕЧИ

И.В. САВЧЕНКО

На данный момент существуют различные программные средства синтез речи. Данные программные средства используют различные подходы для генерации речевого сигнала. Для разработки программного средства генерации речеподобных помех, необходима интеграция с модулем, позволяющим непосредственно генерировать речь на основании текста. Рассмотрим различные существующие программные средства предоставляющие возможность интеграции.

Festival — обобщенная многоязычная система синтеза речи. Она предлагает полную систему синтеза речи с различными API, а также среду для разработки и исследования методов синтеза речи. Система написана на C++ с командным интерпретатором для общей настройки и расширения. Достоинствами данного программного средства являются: поддержка нескольких языков, свободная лицензия, наличие специального API, дополнительные утилиты для работы с системой. К недостаткам можно отнести сложность конфигурации системы под конкретную задачу и ее платформазависимость.

VoiceXML (Voice eXtensible Markup Language) — один из открытых стандартов W3C, который представляет собой интерпретатор, преобразующий текстовую фразу в синтезированную речь. Стандарт предназначен для разработки интерактивных голосовых приложений. VoiceXML имеет теги, являющиеся командами для голосового браузера, который синтезирует, распознает речь, предоставляет диалоговое управление. Достоинствами данного стандарта являются: простота и удобство в использовании, поддержка технологии крупными компаниями, наличие различных реализаций стандарта, использование XML языка разметки, кросплатформенная реализация. Главными недостатками стандарта являются отсутствие единого главного стандарта и тонкой настройки системы для конкретной задачи.

eSpeak — это компактный свободный программный синтезатор речи, поддерживающий Speech Synthesis Markup Language — SSML. Версии eSpeak существуют под такие операционные системы, как Microsoft Windows, Mac OS X, Linux, RISC OS, Android, Maemo, а также доступен его исходный код на языке C++ Windows Mobile. Слова входного текста для синтезирования в данной программе проходят два этапа обработки. На первом этапе слово в буквенном представлении преобразуется в последовательность фонем. На втором этапе на основе полученной последовательности генерируется звуковой сигнал. eSpeak является open source проектом, благодаря этому, некоторые разработчики интегрировали его в свои продукты. К достоинствам данного синтезатора речи относятся: поддержка большого числа языков, открытый исходный код, кросплатформенность, наличие дополнений и специальных услуг, широкие возможности для тонкой настройки, использование эффективных алгоритмов синтеза речи. К недостаткам можно отнести необходимость перекомпиляции программы для каждой отдельно взятой платформы.

Таким образом наиболее подходящими для интеграции являются программные средства, имеющие открытый исходный код либо предоставляющие специальное API.

Литература

1. Лобанов Б.М., Цирульник Л.И. Компьютерный синтез и клонирование речи. Минск, 2008. 316 с.
2. Сорокин В.Н. Синтез речи. М., 1992. 392 с.
3. Манахов П. Обзор мобильных Text-To-Speech движков / [Электронный ресурс]. Режим доступа: http://habrahabr.ru/post/102199/. Дата доступа: 19.05.2012.

ПОДДЕРЖКА DIGITAL RIGHTS MANAGEMENT В МОБИЛЬНЫХ УСТРОЙСТВАХ НА БАЗЕ ANDROID

П.В. САВЧЕНКО, Е.Р. ПЕЛЬКИН

Возросшая популярность мобильных устройств под управлением системы Андроид, ставит перед пользователем компьютерной техники новые проблемы. Одна из них, для многих достаточно важная, это защита информации на мобильных устройствах под управлением Андроид.

Большинство DRM решений построены по единой архитектуре. Защищаемый контент предварительно шифруется DRM модулем шифрации (как правило, применяется AES-128), а модуль управления лицензиями выдает ключи пользователям на просмотр контента (как правило создается на базе Java сервера приложений). Такая реализация позволяет эффективно разделить этапы обработки контента, доставки контента и управления разрешениями на использование.

В случае Android системы защиты контента приложение берет на себя лишь дешифрацию данных получаемых по HTTP Live Streaming протоколу при помощи заранее указанного ключа дешифрации. В качестве алгоритма используется стандартный AES-128. в этом случае разработчику приложения нужно реализовать на серверной части механизм сохранения ключей шифрации и очень аккуратной их выдачи, а на клиентской части обеспечить качественный прием этих ключей с минимальным риском для перехвата (например, обеспечить jailbreak detection в приложении).

При доставке ключей в приложение для защиты ключей предлагается использовать HTTPS. При этом остается риск перехвата ключа, в тех случаях если произвели взлом устройства (Jailbreak) или каким-то образом сэмулировали на PC данное устройство. Существенно снизить этот риск, можно лишь при написании своего приложения, реализовав дополнительные проверки.

НЕРАВНАЯ ЗАЩИТА ДАННЫХ ПРИ ПОМОЩИ НЕРАВНОМЕРНОГО ДВУМЕРНОГО КОДИРОВАНИИ ИНФОРМАЦИИ

НЕСТОР АЛЬФРЕДО САЛАС ВАЛОР

Известны многие алгоритмы декодирования двумерного неравномерного кодирования информации. Одним из них является алгоритм на основе нахождения на предварительном этапе обработки кодеком данных всевозможных комбинаций размещения ошибок определенной кратности ti в сжатой форме. Все эти образы ошибок формируют общую библиотеку образов ошибок и для каждого образа формируются правила идентификации ошибок соответствующей кратности. Известна библиотека образов ошибок для неравномерного совместного способа кодирования информации. Однако, данный способ кодирования и декодирования информации неэффективен и сложен в реализации при коррекции многократных ошибок.

Для устранения данных недостатков предложен метод формирования библиотеки образов ошибок на основе двумерного равномерного кодирования информации. Установлено, что при данном способе кодирования и декодирования общее число образов трехкратных и четырехкратных ошибок уменьшается примерно на 32% и 18% соответственно по сравнению с использованием библиотеки образов ошибок при неравномерном совместном кодировании и декодировании информации. Уменьшение общего числа образов обеспечиваются за счет исключения из

библиотеки образов ошибок таких размещений ошибок по зонам, которые превышают корректирующую способность кодов в данной зоны.

МЕХАНИЗМ ПРОВОДИМОСТИ МДМ-СТРУКТУР НА ОСНОВЕ АНОДНЫХ ОКСИДНЫХ ПЛЕНОК, СОДЕРЖАЩИХ ИТТРИЙ

С.М. САЦУК, М.М. ПИНАЕВА

МДМ-структуры находят широкое применение при создании различных компонентов для систем защиты информации.

В данной работе представлены результаты исследований нанотонких анодных оксидных пленок, содержащих иттрий, сформированных при напряжении 160 В. в качестве верхней обкладки использовался алюминий или тантал. Часть МДМ-структур подвергалась термообработке при температуре 673 К в течение 3 ч.

Анализ вольт-амперных характеристик МДМ-структур позволяет выделить на них два основных участка: омический (проводимость не зависит от напряженности электрического поля) и неомический. Омический участок, где рост тока пропорционален росту напряжения, наблюдается как при положительно, так и отрицательно смещенной структуре. Напряжение, соответствующее переходу от омического участка к неомическому, зависит от режима формирования нанотонкой анодной оксидной пленки. Отжиг также влияет на напряжение перехода, которое уменьшается с 27 до 22 В. Такому уменьшению напряжения перехода соответствует снижение проводимости структур в 12 раз. Материал верхнего электрода (алюминий или тантал) не влияет на характер зависимостей ток-напряжение.

Анализ литературных данных, касающихся основных механизмов проводимости на постоянном токе МДМ-структур, позволяет выделить три возможных механизма, ответственных за перенос носителей заряда в исследуемых МДМ-структурах: ток, ограниченный пространственным зарядом, эмиссия Пула-Френкеля и Шоттки.

Четко выраженные линейные участи на вольт-амперных характеристиках, их незначительная температурная зависимость и отсутствие влияния материала верхнего электрода всех структур, дают основания считать, что процессы переноса носителей заряда в исследуемых структурах объясняются действием объемных, а не приэлектродных эффектов.

СВОЙСТВА АНОДНЫХ ПЛЕНОК НА АЛЮМИНИИ СОДЕРЖАЩИХ РЕДКОЗЕМЕЛЬНЫЕ МЕТАЛЛЫ

С.М. САЦУК

Свойства анодных оксидных пленок в существенной степени влияет на поглощающую способность диэлектрика в различном диапазоне частот.

Для определения оптимальных условий формирования бездефектных анодных оксидных пленок на алюминии, содержащих иттрий, были проведены исследования их морфологии и профиля распределения анионов электролита.

Морфологический анализ пленок, полученных при напряжении формовки до 160 В показал, что они не содержат дефектов в виде сквозных пор или трещин, а их поверхность имеет вид, характерный для плотных пленок. На анодных оксидных пленках, сформированных при 160 В поры обнаруживаются в очень малых

количествах и располагаются исключительно по границам зерен, где находятся области кристаллизации аморфной анодной оксидной пленки. Увеличение формирующего напряжения более 160 В приводит к возрастанию числа пор, увеличению их диаметра, а при 220 В наблюдаемая поверхность имеет сходство с поверхностью пористых оксидных пленок. Полученные данные позволяют скорректировать максимальное напряжение формовки для получения бездефектного диэлектрика, содержащего редкоземельные металлы.

Анализ профиля распределения элементов анионов электролита в анодных оксидных пленках, содержащих иттрий, полученных при напряжении формовки 70 В и при различных pH, свидетельствует, что pH электролита практически не оказывает влияния на характер распределения P^{31} в анодной оксидной пленке. Наибольшее количество P^{31} фиксируется на поверхности пленки, далее оно несколько снижается и остается практически постоянным, на расстоянии, соответствующем 30% толщины оксида. Максимальное содержание Y^{89} при всех исследованных значениях pH фиксируется на поверхности пленок, а затем убывает, достигая минимума на глубине около 100 нм. Подобный характер распределения наблюдается в оксидных пленках с редкоземельными металлами, введенными методом термодиффузии и характеризует замещение алюминия иттрием в оксиде сложного состава.

ШИФРОВАНИЕ ДАННЫХ НА ОСНОВЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ СИСТЕМ И ОТОБРАЖЕНИЙ

А.В. СИДОРЕНКО, К.С. МУЛЯРЧИК

Одним из перспективных направлений в современной криптографии является разработка и исследование алгоритмов шифрования на основе динамического хаоса. Динамический хаос и криптография имеют ряд общих фундаментальных свойств, среди которых чувствительность к начальным условиям и апериодичность траекторий в фазовом пространстве динамических систем, что позволяет реализовать такие свойства криптографических систем как запутывание и рассеяние.

Нами разработан алгоритм шифрования, основанный на использовании дискретных хаотических отображений, сети Фейстеля в качестве базового преобразования и четырех режимов работы алгоритма — ECB, CBC, CFB, OFB. Использование сети Фейстеля в алгоритме шифрования позволяет применять одно базовое преобразование для зашифрования и расшифрования, что повышает скорость работы алгоритма, снижает структурную сложность, а, следовательно, и потребность в вычислительных ресурсах.

В базовом преобразовании в качестве нелинейной функции используется дискретное хаотическое отображение. При этом выбор хаотического отображения приобретает принципиальное значение, что обусловлено необходимостью целочисленного представления информации.

Для анализа алгоритмов шифрования на основе динамического хаоса используются специализированные методы: метод задержанной координаты и метод построения фазовых диаграмм. Так, для зашифрованной последовательности вычисляются значения корреляционной размерности и энтропии Колмогорова. Данные параметры позволяют в динамике оценить область локализации и степень расходимости фазовых траекторий в пространстве и определить минимально необходимое число итераций базового преобразования, которое обеспечивает криптостойкость алгоритма.

СТРУКТУРНО-ИНФОРМАЦИОННЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ СЛОЖНЫХ СИСТЕМ

Л.С. СТРИГАЛЕВ

В современных условиях резко возросла актуальность создания высокоэффективных систем и средств безопасности. Необходим анализ и обновление традиционной парадигмы безопасности. Безопасность — неотъемлемое эмерджентное свойство сложной системы; это свойство структуры системы в ее четверке: система, структура, цель, технология [1]. Чем выше качество безопасности, тем более устойчива структура системы. В структуре системы заложена ее цель, порождающая технологию системы; угрозу представляет все то, что способно причинить вред структуре системы. Безопасность, как и у живых организмов, должна охватывать все структурные уровни.

У человека, например, сеть «датчиков» контролирует все жизненно важные органы, которые имеют многочисленные проекции (на коже такие проекции используются в акупунктуре и акупрессуре). Дополнительная, интеллектуальная безопасность человека, связана с тремя уровнями целеполагания: генетическим, неосознанным (условный и каузальный рефлексы; ментальность, привычка) и осознанным. Заметим, что именно неосознанному уровню в значительной степени обязаны, техногенные катастрофы.

В заключение отметим, что важен не только «охват» структуры защищаемой системы «нервной сетью», но и обеспечение заданного качества функционирования такой сети. В этой связи необходимы соответствующие методы и средства оценки качества информационного метаболизма. Ограничения на объем тезисов не позволяют детализировать данный аспект, который является достаточно хорошо проработанным в рамках информационного подхода применительно к системам обнаружения объектов.

Литература

1. Стригалев Л.С. // Экономическое развитие общества: инновации, информатизация, системный подход: Материалы Междунар. научно-экономической конф. 22–23 апреля 2008 г. Минск, 2008 С. 257–226.

КРИТЕРИИ ОЦЕНКИ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Л.С. СТРИГАЛЕВ

Оценка качества средств защиты информации занимает далеко не последнее место в проблемной среде индустрии компьютерной безопасности. Такие оценки необходимы при разработке и оптимизации средств защиты информации, а также при выборе средств защиты для реализации политики безопасности.

Стандарты в области компьютерной безопасности отображают вопросы методологии, менеджмента, включая управление и контроль рисков, но не содержат критерии оценки качества средств безопасности. Последнее обстоятельство способствует маркетинговым играм. Например, как отмечается в ряде источников, манипулируя критериями и условиями проведения эксперимента можно практически любой антивирус представить как наилучший. Подобное возможно для всех средств и систем, работа которых связана с двумя видами ошибок: ложное обнаружение и пропуск объекта. Более того иногда количественные оценки результатов машинных и даже натурных экспериментов могут превышать предельные возможности исследуемых систем (результат «подгонки» под требования ТЗ при отсутствии оценки предельных возможностей системы).

Для разрешения обсуждаемой проблематики представляется целесообразным использовать информационные меры, в частности, дивергенцию Кульбака-Лейблера, которая представляет собой математическое ожидание логарифма отношения правдоподобия и обладает свойством аддитивности. Данное свойство позволяет, например, в области систем обнаружения оценивать предельные возможности средств обнаружения, а также путем введения информационных КПД оценивать потери информации при ее поэтапной обработке (включая оценку качества работы человека-оператора) и осуществлять оптимизацию, как в цепи поэтапной обработки информации, так и системы обнаружения в целом.

АНАЛИЗ ПРОСТОЕВ СЕРВЕРА INTEL SERVER BOARD S5520UR ПО ПРИЧИНАМ ИХ ВОЗНИКНОВЕНИЯ

В.И. ПАЧИНИН, Т.Г. ТАБОЛИЧ, Д.В. ШЕРЕМЕТ

Отказы программно-аппаратной части является одной из важнейших техногенных угроз информационной безопасности сервера [1]. Парированием этой угрозы могут быть наблюдения за работой сервера во время эксплуатации [2-5]. Результаты наблюдений не только помогают [2–4] уменьшить простои сервера и потери во время простоев обрабатываемой сервером информации, но и дают возможность количественно оценить показатели надёжности сервера и уровень потерь информации во время отказов [2, 5]. Однако фактические данные об отказах серверов практически не публикуются, поэтому в [6] проанализированы результаты наблюдений в течение 2,1 года за надёжностью высокопроизводительного сервера Intel Server Board S5520UR (процессор Intel Xeon CPU E5620 x2, RAM 26 Gb, HDD 2x2 Тб). Коэффициент готовности (КГ) этого сервера (без разделения отказов на конструктивные, производственные и эксплуатационные) составил 0,999406, коэффициент технического использования (КТИ) 0,999340, процент потерь информации (ПИ) за счёт простоев 0,066%.

Если проанализировать простои сервера и разделить их по причине возникновения, то два простоя можно отнести к эксплуатационным. Таким образом, повышая качество эксплуатации, этих отказов можно было бы избежать. Простой в связи с обновлением версии операционной системы также относится к эксплуатационным отказам. Избежать данного вида отказов не возможно по причине неосуществимости ликвидации существующего объективно морального старения программного обеспечения. Оставшиеся простои (замена планки памяти 4 Гб Memory Module Kit на планку большего объёма и замена винчестера на винчестер большего объёма с целью увеличения дискового пространства сервера) также невозможно отнести к конструктивным или производственным отказам — замена комплектующих во время эксплуатации не требовалась бы, при условии приобретения более дорогостоящего сервера с планкой и винчестером большего объёма.

Таким образом, фактическая безотказность (средняя наработка на отказ относительно отказов, которых нельзя было избежать) сервера Intel Server Board S5520UR оказалась не ниже 18 тысяч часов, фактический КТИ не ниже 0,9999445, а фактический процент ПИ не более 0,00445 %.

Литература

1. Гайдук В.Ю., Пачинин В.И., Сечко Г.В., Таболич Т.Г. // Материалы 13-й МНТК «Современные средства связи» 7–9 октября 2008 г., Минск. Минск: ВГКС, 2008. С. 194.

2. Бахтизин В.В., Николаенко Е.В., Сечко Г.В., Таболич Т.Г. Модели отказов и наблюдения за отказами: лаб. практикум по курсу «Надёжность программного обеспечения (НПО)» для студ.

спец. «Программное обеспечение информационных технологий» веч. Формы обуч.: Минск: БГУИР, 2011. 37 с.
3. Николаенко В.Л., Пачинин В.И., Сечко Г.В., Таболич Т.Г. // Материалы 15-й МНТК «Современные средства связи», 28–30 сентября 2010 г., Минск, Респ. Беларусь / редкол.: А.О.Зеневич и [др.] Минск: ВГКС, 2010. С. 149.
4. Калачёв И.А., Марков М.С., Сечко Г.В. Шеремет Д.В. // Технические средства защиты информации: Тезисы докл. 8-й Белор.-российск. НТК. Браслав, 24–28 мая 2010 г. Минск: БГУИР, 2010. С. 97.
5. Блинцов А.Е., Моженкова Е.В., Соловьянчик А.Н., и др. // Материалы 16-й МНТК «Комплексная защита информации». 17–20 мая 2011 г., Гродно. Минск: БелГИСС, 2011. С. 174–176.
6. Зенин К.Н., Марченко Е.Л., Пашкевич М.Н., и др. // Тез. докл. 48-й научной конференции аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии / под ред. В.Л. Николаенко, Г.В. Сечко. Минск: ИИТ БГУИР, 2012. С. 31.

АРХИВАТОР С ДОПОЛНИТЕЛЬНЫМИ ОПЦИЯМИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

А.А. ГИВОЙНО, Е.В. НИКОЛАЕНКО, Г.В. СЕЧКО

Основным преимуществом архиваторов является значительное уменьшение требуемого для хранения информации места на диске (до 90%), а также резкое сокращение времени на передачу и удешевление передачи архива по электронной почте по сравнению с незаархивированной информацией. Представленный в докладе архиватор NPack [1] помимо общепринятых функций обладает рядом дополнительных преимуществ в части защиты информации, выделяющих его из ряда стандартных. Такими преимуществами являются:

1. Возможность скрывать архив в любой другой файл, не повреждая его содержимого и работоспособности. Практика использования архива показала, что достаточно популярной является возможность скрыть заархивированную информацию в картинке. Архиватор самостоятельно преобразует изображение без существенной потери качества и скрывает в файле архивную информацию дополнительно так, что сложно отличить простое изображение от изображения-архива.

2. Использование по усмотрению пользователя отдельной программы для получения доступа к архиву через распознавание биометрики глаза. Применение такой дополнительной опции обеспечивает высокую степень защиты архива от взлома.

3. Устойчивость архивов, полученных с помощью NPack, к вирусным атакам [2] при привлекательной ценовой конкурентоспособности архива. Понятно, что в условиях пиратского распространения копий популярных архиваторов стоимость последних нулевая. Однако по состоянию на май 2012 г. реальная стоимость архиваторов [1] составляет (примерно): WinZip 16 Multilanguage (электронная версия) Standard — $25, WinZip Courier 3.0 — $20, WinRAR 4 Standard — $29, WinPRS 1.02 — $5.1, Microinvest Архиватор Pro 3.01.012 — $78.64, ASPack — $44,55. Рассчитанная стоимость представленного архиватора как программы общего назначения составляет $4,9 за копию

Отдельно стоит отметить, что несмотря на насыщенность допустимых операций, современный интерфейс предоставляет интуитивно понятную структуру для комфортного использования программного средства без подготовки.

Литература
1. Гивойно А.А., Куницкий А.Л. // Тез. докл. 48-й научной конференции аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии / под ред. В.Л. Николаенко и Г.В. Сечко. Минск: ИИТ БГУИР, 2012. С. 30.
2. Гивойно А.А., Николаенко В.Л., Сечко Г.В, Таболич Т.Г. // Материалы 16-й МНТК «Современные средства связи» 27–29 сентября 2011 г., Минск, Респ. Беларусь / редкол.: А.О.Зеневич и [др.] Минск: УО ВГКС, 2011. С. 90.

ПОСТАНОВКА ЗАДАЧИ СОСТАВЛЕНИЯ ПРОФИЛЯ ЗАЩИТЫ БАЗ ДАННЫХ СИСТЕМ КОМПЬЮТЕРНОЙ ДИАГНОСТИКИ АВТОТЕХНИКИ

М.В. МИХАЛЬЦОВ, В.И. ПАЧИНИН, Т.Г. ТАБОЛИЧ

Одним из способов снижения трудоёмкости ремонта автотехники является применение современных систем компьютерной диагностики [1]. Современная система компьютерной диагностики автотехники (СКДА) имеет сложную аппаратную часть и не менее сложное программное обеспечение (ПО). ПО СКДА включает собственно программу диагностики и автомобильную базу данных с собственной системой управления. Программа, установленная на компьютере, посылает через ком-порт (или USB-порт) сигналы от автосканера в адаптер, который в свою очередь транслирует их на контроллер в автомобиле. Контроллер посылает ответные сигналы (данные), которые программа получает и, сравнивая их с данными автомобильной базы данных, интерпретирует (визуализирует) их. Обмен управляющими сигналами и данными происходит согласно определенному протоколу. Описанная выше сложность СКДА делает систему как информационный объект уязвимой со стороны естественных воздействий среды и непреднамеренных воздействий со стороны человека. Возникает проблема обеспечения информационной безопасности (ИБ) СКДА. Результаты решения данной проблемы не приведены в современной литературе по обеспечению информационной безопасности, нет достаточного количества публикаций и практикоориентированного анализа по исследуемой тематике.

В докладе решение проблемы обеспечения ИБ СКДА предлагается начать с составления профиля защиты (ПЗ) базы данных (БД) СКДА. ПЗ в данном случае представляет собой [2] независимый от реализации типовой набор требований безопасности для совокупности БД СКДА, отвечающий соответствующим целям безопасности СКДА. Разрабатываемый ПЗ предназначен для многократного использования и будет определять требования безопасности БД СКДА, включая функциональные требования и требования доверия, в отношении которых установлено, что они являются достаточными и эффективными для достижения установленных целей безопасности. ПЗ будет использован как стандартизованный набор требований с целью повышения обоснованности задания требований безопасности БД СКДА, оценки безопасности и возможности проведения сравнительного анализа уровня безопасности различных БД СКДА достаточного уровня опубликованости

Первые результаты работ по созданию ПЗ БД СКДА рассмотрены в [3], где кратко проанализированы основные угрозы информационной безопасности БД СКДА.

Литература
1. Михальцов М.В., Пачинин В.Н, Сечко Г.В, Таболич Т.Г. // Материалы 16-й МНТК «Современные средства связи» 27–29 сентября 2011 г., Минск, Респ. Беларусь / редкол.: А.О.Зеневич и [др.] Минск: УО ВГКС, 2011. С. 91.

2. Голиков В.Ф., Черная И.И., Зельманский О.Б. Методологические основы информационной безопасности: учеб-метод. пособие. Минск, БГУИР, 2010. 67 с.
3. Михальцов М.В. // Тез. докл. 48-й научной конференции аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии / под ред. В.Л. Николаенко и Г.В. Сечко. Минск: ИИТ БГУИР, 2012. С. 34.

ЗАЩИТА ДАННЫХ ПРИ ПОСЛЕДОВАТЕЛЬНОЙ НОРМЕННОЙ ОБРАБОТКЕ ИНФОРМАЦИИ

ХОАНГ НГОК ЗЫОНГ

Для защиты информации от искажений, возникающих в канале связи, широко применяется помехоустойчивое кодирование. Известно, что с увеличением кратности ошибок возникает «проблема селектора». Для снижения влияния проблемы селектора в [1, 2] предложено норменное кодирование. Однако при увеличении кратности корректируемых ошибок, а также длинны кодов, вычислительная сложность реализации декодеров резко растет.

В данной работе рассматривается поход к сжатию множества норм табличным методом образующих норменных циклотомических классов, сущность которого заключается в использовании величины переходов из одного образующего циклотомического класса в другой. В результате этого, можно использовать только одну образующую норму для коррекции ошибок. Величина перехода из одного в другой циклотомический класс может быть представлена в виде таблицы. Рассматривает пример БЧХ-кода n=31, t=3, для которого существует 145 образующих векторов ошибок, с 29 образующими норменных циклотомических классов (в каждом классе 5 образующих векторов ошибок). Пусть $(N_1^{обр}, N_2^{обр}, N_3^{обр})$ образующие норменных классов. Чтобы перейти из одного $(N_{1,1}^{обр}, N_{1,2}^{обр}, N_{1,3}^{обр})$ в другой $(N_{2,1}^{обр}, N_{2,2}^{обр}, N_{2,3}^{обр})$ используются величину Δ_1, Δ_2, Δ_3, которые находятся из условий $N_{2,1}^{обр} = N_{1,1}^{обр} + \Delta_1; N_{2,2}^{обр} = N_{2,1}^{обр} + \Delta_2; N_{2,3}^{обр} = N_{1,3}^{обр} + \Delta_3$, для этого нужно 29 Δ_1, Δ_2, Δ_3.

Литература

1. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М., 2004.
2. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.

ПАКЕТНАЯ ФИЛЬТРАЦИЯ ТРАФИКА В БЕСПРОВОДНЫХ ЯЧЕИСТЫХ СЕТЯХ НА ОСНОВЕ РАСПРЕДЕЛЕННОГО МЕЖСЕТЕВОГО ЭКРАНА

А.А. ЮРЕВИЧ, В.Ю. ЦВЕТКОВ, А.С. АЛЬ-АЛЕМ

В компьютерных сетях применяются системы защиты на основе межсетевых экранов. Системы защиты осуществляют блокировку атак, предотвращают «фоновый» трафик, ограничивают доступ в сеть извне, контролируют трафик внутри сети и регистрируют сетевую активность. Ключевыми узлами беспроводных ячеистых сетей являются беспроводные маршрутизаторы с невысокой вычислительной мощностью. Это затрудняет реализацию на их базе пакетных фильтров и сетевых экранов. Предлагается метод построения распределенного межсетевого экрана, узлами которого являются беспроводные ячеистые маршрутизаторы с операционной системой Linux/UNIX. Суть метода состоит

в применении прикладного TCP/IP сервера для управления набором правил пакетного фильтра (в GNU/Linux используется iptables) на маршрутизаторах. Для запуска приложения TCP/IP сервера при появлении трафика на детерминированных портах предлагается использовать суперсервер xinetd (extended Internet daemon). Метод позволяет централизованно и быстро вносить изменения в правила пакетных фильтров на все маршрутизаторы в сети. Использование распределенного межсетевого экрана обеспечивает низкую уязвимость к DoS-атакам, отсутствие единой точки отказа, высокую пропускную способность сети и делает возможным применение локальных и глобальных политик.

АНАЛИЗ БОРТОВЫХ СИСТЕМ ВИДЕОФИКСАЦИИ ДЛЯ ОХРАНЫ РАСПРЕДЕЛЕННЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

А.А. ЖУРАВЛЕВ, В.Ю. ЦВЕТКОВ

Произведен анализ существующих систем видеофиксации, предназначенных для беспилотных летательных аппаратов (БПЛА) и обеспечивающих мониторинг территорий и распределенных объектов с целью выявления незаконной деятельности вблизи критически важных объектов. Выявлены основные параметры систем видеофиксации, определяющие выбор метода эффективного кодирования для сжатия видеоданных, фиксируемых на борту БПЛА. Установлено, что при выборе метода видеокодирования необходимо учитывать угол наклона камеры, аберрации оптической системы, а также разрешающую способность матрицы видеокамеры. Последний параметр особенно важен, так как определяет качество воспроизведения видеоданных после декодирования. Увеличение размера матрицы позволяет повысить качество воспроизведения видеоданных, но только при увеличении скорости передачи. Если полоса канала ограничена, увеличение размера матрицы ведет к необходимости повышения коэффициента сжатия видеоданных, что вызывает снижение качества их воспроизведения. С другой стороны, использование оптического увеличения для повышения детальности формируемых на борту БПЛА видеоданных приводит к уменьшению площади перекрытия соседних кадров и снижению эффективности методов сжатия, основанных на блочной компенсации движения.

АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ

Ю.А. СЕЛИВАНОВА, В.Ю. ЦВЕТКОВ

Проведен анализ защищенности сервисов в коммуникационных системах Microsoft Lync Server 2010, Skype и ooVoo. Установлено, что данные системы используют следующие технологии информационной безопасности. В Microsoft Lync Server 2010 для аутентификации пользователей и серверов используются протоколы TLS и MTLS с криптографическими алгоритмами RSA-RC4-128-SHA. Пользователи локальной сети аутентифицируются средствами протокола Kerberos, а внешние — с использованием TLS-DSK или NTLMv2. SIP-каналы шифруются средствами TLS. Трафик аудио и видео защищается протоколом SRTP с применением AES-128. Трафик веб-конференций шифруется в HTTPS-канале. в Skype для аутентификации пользователей используется протокол TLS, для шифрования и защиты целостности

– AES-256 блочный шифр, криптографические стандарты открытого ключа RSA, ISO 9796-2 система подписи, SHA-1 систему хэширования и RC4 шифрование потока. В ooVoo аутентификация пользователей осуществляется по защищенному каналу TLS (RSA-RC4-128-MD5), аудио и видео трафик передается в открытом виде. Таким образом, Microsoft Lync Server 2010 и Skype используют схожие технологии информационной безопасности и предоставляют более защищенные сервисы по отношению к ooVoo.

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДОВ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

С.Б. САЛОМАТИН, В.В. ПАНЬКОВА

Кодовые структуры, обладающие стойкостью к раскрытию, используют как компоненты систем защиты информации. Одним из эффективных средств защиты от ошибок и преднамеренных воздействий является комплексная кодовая зашита. Объектом исследования являлись алгебро-геометрические коды Эрмита, мощность которых превосходит аналогичный показатель кодов эллиптических кривых.

Основными критериями, предъявляемыми к разработке и исследованию эффективности криптоалгоритмов, являются такие показатели, как нелинейность преобразований, сбалансированность криптографической функции, линейная сложность шифрующей последовательности. Автокорреляционная функция (АКФ) предоставляет возможность описания критериев безопасности через оценку вероятностных параметров.

Криптографический анализ проведён на примере алгебро-геометрического кода (32, 64), заданного кривой Эрмита в поле GF(16). Оценка АКФ указывает на близость исследуемых последовательностей к случайным. Значения компонент спектра Уолша-Адамара эквивалентных сопряжённых последовательностей кодированных векторов отражают уровень нелинейности (от 106 до 104 при верхней границе 120), что указывает на высокую степень удалённости последовательностей от линейных, а значит, высокую степень устойчивости к линейному криптоанализу. Значения нулевых компонент спектров имеют отклонения от нуля, что указывает на определенную несбалансированность структуры кода. Уровень линейной сложности шифрующих последовательностей оценён с помощью алгоритма Берлекемпа-Месси и составляет от 120 до 124, т.е. криптосистемы, использующие подобные последовательности, устойчивы к вскрытию, и криптоаналитик не может предсказать ни следующий, ни предыдущий бит последовательности.

МОНИТОРИНГ СИСТЕМЫ БЕЗОПАСНОСТИ СЕТИ 2G/3G (UMTS)

Д.Н. ПИСКУН

Системы связи UMTS требуют осуществления глобального роуминга, высокой скорости передачи информации и оказания электронных услуг различного вида. Все эти функции должны быть поддержаны системой защиты информации, одной из опций которой является анализ состояний мобильных станций и сетевой структуры.

Целью данной работы является разработка моделей и алгоритмов анализа состояния системы связи в режиме мониторинга зон покрытия, а также написание программного обеспечения системы защиты информации.

Архитектура системы безопасности сетей связи 3G (UMTS) представляет собой многоуровневую структуру. Одной из неотъемлемых функций архитектуры является поддержка требований по наблюдаемости и конфигурируемости системы защиты информации на основе анализа состояний мобильный станций, оконечных мобильных устройств, каналов передачи, сетевой инфраструктуры. Априорное знание этих состояний, в сочетании с точными географическими параметрами (широта, высота, долгота), позволяют оценить степень конфиденциальности и произвести оценку целостности всей инфраструктуры сети. Перспективным инструментом анализа в этом отношении являются методы основанные на фрактальных вейвлетных моделях.

В данной работе предполагается использование программно-аппаратного комплекса базирующегося на высокотехнологичном радиоизмерительном оборудовании — модульной измерительной системе компании National Instruments, основанной на открытом промышленном стандарте PXI. для использования своих модульных измерительных систем, компания National Instruments предлагает использовать среду графического программирования NI LabVIEW. в состав NI LabVIEW входят специализированные модули для имитации и записи реального сигнала UMTS и измерения различных технических параметров сигнала.

КОДОВАЯ КОРРЕКЦИЯ СМЕЩЕНИЯ В ГЕНЕРАТОРАХ СЛУЧАЙНЫХ ЧИСЕЛ

С.Б. САЛОМАТИН, Т.А. АНДРИАНОВА

Основными элементами в инфраструктуре формирования ключевого пространства является генераторы случайных чисел. Одним из недостатков генераторов такого рода является возможность появления постоянного смещения e в распределениях случайных последовательностей чисел.

Для предотвращения появления смещения можно использовать метод кодовой коррекции работы генератора случайных чисел. Суть метода состоит в дополнительном кодировании данных, формируемых генератором случайных чисел.

Кодовые корректоры смещения можно разделить на два вида: линейные и нелинейные.

Линейный кодовый корректор отображает n бит входных данных в m бит выхода с величиной смещения $e/2$. Смещение любой ненулевой комбинации выходных бит будет не больше $e^d/2$, где d — минимальное кодовое расстояние линейного кода, задаваемого порождающей матрицей G.

Действие линейного корректора удобно описать с помощью (n, m, t)-устойчивой функции. Под (n, m, t)-устойчивой функцией будем понимать функцию, отображающую n битов входа в m битов выхода таким образом, что если t входных битов имеют фиксированные значения, то не происходит никаких изменений на выходе.

Нелинейный корректор отображает n бит в m бит. При этом ненулевая линейная комбинация выхода определяется как вектор булевой функции. Величина смещения может быть вычислена с помощью таблицы истинности. Используя преобразования Уолша, можно оценить смещение с помощью функции веса кода.

В качестве примера рассматривается применение кода БЧХ с параметрами (256, 21, 111) и дуального кода (256, 234, 6) с порождающим полиномом $h(x)$, имеющего степень 21 Вектор из 255 символов представляется в полиномиальном виде $m(x)$. Далее выполняется кодирование $m(x) \bmod h(x)$. При этом происходит

отображение элементов поля F_2^{255} в поле F_2^{21}. При входном смещении равном 0,25 теоретическая оценка смещения выхода не превосходит 2^{-111}. Энтропия выхода близка к 21.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ОБЛАЧНЫХ СЕРВИСОВ

П.В. ШЕЛЕСТОВИЧ

С ростом популярности облачных сервисов для определенных видов вычислений все острее встает вопрос обеспечения безопасности данных в «облаке» и их постоянной доступности. Например, пользователи мобильных устройств регулярно синхронизируют свои данные с персональными компьютерами посредством облачных служб, то выступает потенциальной угрозой для важных рабочих данных.

Были проведены исследования мероприятий по обеспечению безопасности облачных вычислений. Эта задача лежит как на операторе облака, так и на пользователе. Создание условий для функционирования средств защиты информации в первую очередь подразумевает формирование доверенной среды. Для облачной платформы это означает тотальную организацию процессов развертывания и корректного завершения доверенных контейнеров (виртуальных машин или приложений) внутри. Внутри доверенной среды такие сервисы защиты информации, как подпись, аутентификация, идентификация и другие, также становятся облачными сервисами, доступными всем доверенным пользователям на общих основаниях. Перенос основных сервисов защиты информации в облачную среду снимает с участника сложную инфраструктурную часть средств защиты информации и предъявляет практически единственное требование к пользователю среды облачных вычислений — доверенность среды компьютера (устройства, терминала), который подключается к облаку.

Полученные результаты исследований выявили: использование облачной безопасности для защиты информации имеет смысл и результат. Таким образом, облачная безопасность больше всего подходит именно для пользователей, которые с ее помощью могут обезопасить свою деятельность куда более действенно и актуально, нежели локальными решениями.

СЕКЦИЯ 4. ЭЛЕМЕНТЫ И КОМПОНЕНТЫ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

ОЦЕНКА ВЛИЯНИЯ МОЩНОСТИ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ НА ХАРАКТЕРИСТИКИ ОСЛАБЛЕНИЯ ЗАЩИТНЫХ ЭКРАНОВ

О.В. БОЙПРАВ, М.Р. НЕАМАХ

Нормируемым параметром электромагнитного излучения (ЭМИ) диапазона сверхвысоких частот (СВЧ) является плотность потока энергии, мВт/см^2. Большинство методик, существующих в настоящее время, позволяет исследовать эффективность конструкций, экранирующих ЭМИ, путем измерения их коэффициентов отражения и передачи по напряженности, дБ. Данные параметры не поддаются нормированию, значит, по ним нельзя судить о пригодности выбранного материала для использования в целях защиты информации от утечки по электромагнитным каналам. Цель настоящей работы состояла в разработке методики оценки ослабления мощности сверхвысокочастотных ЭМИ экранирующими конструкциями.

Для проведения измерений в рамках методики были выбраны генератор ЭМИ диапазона 0,01…18 ГГц, передающая и приемная антенны, измеритель мощности (ИМ) РМ 0,01–39,5. С использованием данных устройств собрана измерительная система. Генератор встроен в конструктив персонального компьютера, с которого осуществляется запуск специализированного программного обеспечения для управления значениями частоты и амплитуды формируемого ЭМИ. Измерения проводились в три этапа. На первом этапе осуществлялась калибровка измерительной системы, в процессе которой определялись уровни мощности ЭМИ генератора в диапазоне 0,8…18 ГГц, соответствующие уровням мощности ЭМИ на приемной антенне 1…5 мВт с шагом 1 мВт. При этом между передающей и приемной антеннами образец не устанавливался. На втором этапе между антеннами размещался исследуемый образец, после чего на каждой из частот, для которой была проведена калибровка, с помощью генератора поочередно формировалось ЭМИ с мощностями, определенными на первом этапе, и снимались показания ИМ РМ 0,01–39,5. Разработанная методика была апробирована при оценке эффективностей экранирования ЭМИ конструкциями, изготовленными с использованием углеродсодержащих и металлосодержащих порошков.

ТЕПЛООБМЕННЫЙ АППАРАТ КОНТАКТНОГО ТИПА ДЛЯ СИСТЕМ СНИЖЕНИЯ ТЕПЛОВОЙ ЗАМЕТНОСТИ ОБЪЕКТОВ

АБДУЛЬКАБЕР ХАМЗА АБДУЛЬКАДЕР, Т.В. БОРБОТЬКО, АКСОЙ СИНАН

Возникновение теплового канала утечки информации обусловлено различием в температурах между объектом наблюдения и фоном, на котором расположен объект. Снижение тепловой заметности, как правило, реализуется за счет передачи тепла от защищаемого объекта конденсированному веществу определенной теплоемкости. Наибольшей эффективностью обладают системы с принудительным жидкостным охлаждением. Однако существенным их недостатком является применение пластинчатых теплообменных аппаратов, которые демаскируют объект

за счет высокого теплового контраста теплообменника, обнаружение которого будет обусловлено не только температурой его поверхности, но значительной площадью.

Разработан теплообменный аппарат контактного типа, понижение температуры хладагента в котором реализуется за счет его охлаждения термоэлектрическими модулями Пельтье. Исследуемый макетный образец такого теплообменного аппарата рассчитан на работу с 10 л хладагента, который из него подавался насосом в трубопровод теплового экрана, выполненный на основе дюралюминия. Тепловой экран непосредственно контактировал источником ИК-излучения нагретого до температуры 150°С. Установлено, что при скорости движения хладагента 0,1 м/с и начальной его температуре 17°С температура жидкости на выходе теплообменного аппарата составила 23°С после 2 ч функционирования системы охлаждения. Показано, что увеличение времени функционирования системы не приводит к дальнейшему повышению температуры хладагента на выходе теплообменного аппарата. Для получения необходимого значения температуры жидкости на выходе теплообменного аппарата необходимо увеличить холодопроизводительность системы его охлаждения.

МЕТОДИКА ПРОГНОЗИРОВАНИЯ НАДЁЖНОСТИ ЭЛЕКТРОННЫХ УСТРОЙСТВ ДЛЯ СИСТЕМЫ АРИОН

С.М. БОРОВИКОВ, Е.Н. ШНЕЙДЕРОВ,
В.Е. МАТЮШКОВ, И.Н. ЦЫРЕЛЬЧУК, Р.П. ГРИШЕЛЬ

Оценка показателей надёжности электронных устройств на этапе проектирования аппаратуры является актуальной задачей. Она даёт ответ на вопрос о целесообразности дальнейших затрат, необходимых на отработку технологии и производство устройств.

В недалёком прошлом проектные и промышленные предприятия Республики Беларусь испытывали трудности при расчёте показателей надёжности электронных устройств из-за неполноты данных о показателях надёжности элементов производства стран СНГ, ограниченности данных об элементах зарубежного производства, входящих в состав электронных устройств, а также из-за отсутствия адаптированной к этим случаям системы автоматизированного расчёта показателей надёжности устройств. Поэтому актуальным являлось создание отечественной системы автоматизированного расчёта, которая, с одной стороны — позволило бы существенно сократить время для поиска справочной информации о надёжности элементов и время решения задачи по оценке надёжности электронных устройств в целом, с другой стороны — повысила бы престиж республики как страны, являющейся одним из лидеров широкого внедрения информационных технологий в проектирование электронной аппаратуры. Такая система была разработана в БГУИР в рамках выполнения инновационного проекта ГКНТ и получила название системы АРИОН.

Система АРИОН (аббревиатура наименования «система автоматизированного расчёта и обеспечения надёжности электронных устройств») была разработана как белорусский вариант подобных российских систем АСОНИКА, АСРН, зарубежных систем RELEX, Cadence Reliability, ALD Group, Item Toolkit, Blocksim и др., представляет собой высокотехнологичный программный комплекс для ЭВМ, предназначенный для автоматизированного расчёта показателей надёжности электронных устройств, имеет некоторые функции, не реализованные в зарубежных системах.

Рассматриваются предпосылки, положенные в основу разработки методики прогнозирования надёжности электронных устройств. Методика использована при создании системы АРИОН, предназначенной для автоматизированного расчёта надёжности. Предлагаются модели прогнозирования, позволяющие определить эксплуатационную интенсивность отказов элементов производства стран СНГ. На основе анализа зарубежных (Россия, США, Китай) справочников и стандартов по прогнозированию надёжности электронной аппаратуры предложена новая классификация наземной аппаратуры по условиям её эксплуатации. Эта классификация заложена в расчётный модуль системы АРИОН. для различных классов и групп элементов с учётом новой классификации получены усреднённые значения поправочного коэффициента, учитывающего жёсткость условий эксплуатации.

ИСПОЛЬЗОВАНИЕ НАПРЯЖЕНИЯ КОЛЛЕКТОР–ЭМИТТЕР В КАЧЕСТВЕ ИМИТАЦИОННОГО ФАКТОРА ДЛЯ ПРОГНОЗИРОВАНИЯ ПОСТЕПЕННЫХ ОТКАЗОВ БИПОЛЯРНЫХ ТРАНЗИСТОРОВ

А.И. БЕРЕСНЕВИЧ

В работах ряда исследователей было показано, что по реакции биполярных транзисторов (БТ) на имитационное воздействие можно прогнозировать значение функционального параметра и, следовательно, наличие или отсутствие постепенного отказа для заданной будущей наработки. В качестве имитационного фактора было предложено использовать ток коллектора. При этом надо различать понятия «рабочий ток коллектора» и «имитационный ток коллектора». Практика показала, что в ряде случаев имитационное значение тока коллектора для заданной будущей наработки может выйти за пределы предельно допустимого значения тока, указываемого в технической документации на БТ Поэтому актуальным является поиск других альтернативных имитационных факторов.

Автором предлагается в качестве нового имитационного фактора использовать напряжение, прикладываемое к p-n-переходам БТ. Обоснованием возможности его использования является то, что между изменениями функциональных параметров биполярных транзисторов, обусловленных длительной наработкой, с одной стороны, и напряжениями, прикладываемыми к p-n-переходам, с другой, существует статистическая аналогия. Поэтому представляется, по значению функционального параметра ($U_{КЭнас}$, $h_{21Э}$ и прочие), измеренного при определенном значении напряжения коллектор–эмиттер $U_{КЭ}$, сделать прогноз параметра для заданной наработки t и заключение о возможном постепенном отказе БТ (конкретного экземпляра).

Показано, что между отклонениями функционального параметра БТ, вызываемыми изменением напряжения коллектор–эмиттер, и деградацией функционального параметра при длительной наработке транзисторов имеет место тесная линейная корреляционная связь. Наличие тесной корреляции является доказательством возможности использования напряжения коллектор–эмиттер в качестве имитационного фактора.

МАТЕРИАЛЫ ДЛЯ ЭКРАНОВ ЭМИ НА ОСНОВЕ ВОЛОКНИСТЫХ МАТРИЦ

М. АЛЬ-МАХДИ, Г.А. ВЛАСОВА, Н.В. НАСОНОВА, Л.М. ЛЫНЬКОВ

В качестве основы для синтеза материалов для экранов ЭМИ на основе волокнистых матриц использовались волокна и трикотажное полотно из полиакрилонитрила. Процесс синтеза основывается на химической сорбции, позволяющей, проводящей последовательность химических реакций, получать материалы с заданными свойствами. Подготовку полиакрилонитрильных волокон и трикотажных полотен на их основе проводили путем обработки их гидроксиламином.

С помощью описанной методики были синтезированы тонкие трикотажные прокладки, содержащие дисперсный Ni и Co, и различающиеся по размерам частиц, электропроводности и магнитным свойствам. Исследования экранирующих свойств проводили в диапазоне частот 1,5–37 ГГц. Для проведения измерений образцов материалов использовалась линейка векторных анализаторов цепей.

Показано, что оптимальная конструкция содержит три слоя: согласующий, рабочий и вспомогательный. В качестве согласующего слоя выступает композитный материал с мелкодисперсным кобальтом, имеющим входное сопротивление, наиболее близкое к сопротивлению воздуха. Рабочий слой с частицами никеля рассеивает прошедшую энергию излучения, а вспомогательный — отражает часть, увеличивая эффективность конструкции.

Измерения электромагнитных свойств, показали, что в области частот 17–37 ГГц увеличивается абсолютная величина коэффициента передачи, а значение коэффициента отражения не превышает уровень –15 дБ.

МОДЕЛИРОВАНИЕ СОПРОТИВЛЕНИЙ ИСТОК-СТОК ОТКРЫТЫХ МОЩНЫХ МОП-ТРАНЗИСТОРОВ

Б.С. КОЛОСНИЦЫН, М.Д. БУШКОВСКИЙ

Конструкции мощных транзисторов можно условно разбить на два основных класса: двухмерные и трехмерные. В двухмерных приборах (горизонтальные МОП-транзисторы с двойной диффузией на n- и на p- подложках ГДМОП$_{n\text{-}(p\text{-})}$) сток и исток располагаются в боковом (горизонтальном) направлении. Такие приборы аналогичны стандартным МОП-транзисторам с протяженной высокорезистивной областью стока, что необходимо для работы в высоковольтном режиме.

В трехмерных приборах дрейфовая область стока расположена вертикально; электрод стока размещен на нижней стороне пластины МОП-транзистора с V-канавкой VМОП, вертикальный транзистор с двойной диффузией ВДМОП.

Сопротивление прибора в проводящем состоянии является крайне важным параметром для работы транзистора, так как определяет величину рассеяния энергии. Оно включает в себя несколько составляющих, в том числе сопротивление канала и сопротивления дрейфовых обогащенной и необогащенной областей n^--тока.

В транзисторах с двойной диффузией (ГДМОМ, ВДМОП) длина канала определяется последовательной диффузией через одно и то же окно в SiO_2 бора и фосфора (или мышьяка). Из-за двухмерных процессов, происходящих при диффузии, уменьшается длина канала $L_k = 0{,}85\ (x_p – x_{n+})$, где x_p и x_{n+} — глубины залегания p-области подложки и n^+-области истока соответственно.

В VМОП и UМОП-транзисторах каналы образуются вертикальным диффузионным профилем за счет анизотропного травления V-канавки под углом

54,74° к поверхности. В результате при тех же самых технологических параметрах диффузии длина канала в этих транзисторах $L_k = (x_p – x_n)/\sin 54{,}74°$ в полтора раза больше, чем длина горизонтального канала в ДМОП-структурах.

Сопротивление обогащенной n^--области дрейфа моделируется сопротивлением канала МОП-транзистора, работающего в режиме обеднения, а сопротивление необогащенной области — резистором с параллельно подключенным объемом n^--тока.

ИК-ФИЛЬТРЫ НА ОСНОВЕ МЕМБРАН ПОРИСТОГО ОКСИДА АЛЮМИНИЯ ДЛЯ ДЕТЕКТОРОВ БАНКНОТ

И.А. ВРУБЛЕВСКИЙ, К.В. ЧЕРНЯКОВА, Д.В. ГОРБАЧЕВ, А.П. КАЗАНЦЕВ

Количество поддельных банкнот и их качество с каждым годом растут, поэтому распознать поддельную банкноту визуально или с помощью ультрафиолетового детектора все сложнее. В настоящее время банки и крупные магазины все чаще используют для проверки денежных знаков ИК-детекторы. Одним из ключевых элементов этих детекторов является фильтр, отсекающий видимый свет и пропускающий излучение инфракрасного диапазона. В настоящее время в качестве фильтров используют материалы кремний (прозрачен при $\lambda>1{,}0$ мкм), германий ($\lambda>1{,}8$ мкм), халькогенидные стекла (прозрачны в диапазоне длин волн 0,3–2,5 мкм). Эти материалы имеют высокую стоимость и, поэтому актуальными становятся разработка и внедрение новых недорогих материалов, прозрачных в ИК-области.

Анодный оксид алюминия обладает высокой твердостью, термической и химической стабильностью. В данной работе предложено использовать в качестве ИК-фильтров мембраны пористого оксида алюминия, полученные электрохимическим окислением алюминия в электролитах на основе органических кислот. Изготовленные мембраны пористого оксида алюминия серо-желтого цвета. Установлено, что мембрана толщиной 100 мкм полностью блокирует прохождение видимого света, излучаемого светодиодным источником белого цвета. Исследованы спектры ИК-пропускания мембран пористого оксида алюминия в области среднего ИК-диапазона (2,5–20 мкм). Эти исследования показали, что пропускание мембран составляет 85–100 %, таким образом, анодный оксид алюминия может быть использован в качестве ИК-фильтра для детекторов банкнот.

НАНОКОМПОЗИТНЫЕ ПЛЕНКИ АНОДНОГО ОКСИДА АЛЮМИНИЯ С КОБАЛЬТОВЫМИ НАНОПРОВОЛОКАМИ ДЛЯ ЭКРАНИРОВАНИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

АХМЕД АЛИ АБДУЛЛАХ АЛЬ-ДИЛАМИ, И.А. ВРУБЛЕВСКИЙ,
К.В. ЧЕРНЯКОВА, Г.А. ПУХИР

Пленки пористого оксида алюминия, полученные электрохимическим окислением алюминия, имеют упорядоченную пористую структуру, которую можно контролировать подбором режимов анодирования, например, напряжения и (или) времени. Возможность варьирования параметров структуры анодных пленок таких, как диаметр пор и межпористое расстояние позволяет использовать нанопористый оксид алюминия в качестве матриц для получения массивов анизотропных наночастиц, повторяющих форму матрицы.

Одно из возможных применений магнитных кобальтовых нанопроволок, электрохимически выращенных внутри пор анодного оксида алюминия — защита

электронных устройств, мобильных телефонов и компьютеров от электромагнитного излучения (ЭМИ).

В качестве магнитных нанокомпозитов в работе были получены нитевидные наночастицы кобальта в матрице пористого Al_2O_3. Слой пористого оксида алюминия толщиной 50 мкм формировали в 4-м % водном растворе щавелевой кислоты на сплаве АМГ–3. Кобальтовые нанопроволки внутри пор пористого оксида алюминия получали методом электрохимического осаждения. Взаимодействие полученных нанокомпозитных пленок с СВЧ-излучением в диапазоне частот 8–12 ГГц изучали стандартным способом с использованием волновода, между фланцами которого помещали исследуемый образец. По данным измерений, средняя величина ослабления ЭМИ в указанном спектральном диапазоне была равна 40 дБ.

МОДЕЛИРОВАНИЕ РАДИОПОГЛОЩАЮЩИХ СВОЙСТВ МНОГОСЛОЙНЫХ КОНСТРУКЦИЙ ЭКРАНОВ ЭМИ

И.А. ГРАБАРЬ, Н.В. НАСОНОВА

При разработке материалов для радиоэлектроники интерес представляют слоистые структуры, полученные чередованием слоев на основе проводников и диэлектриков. Такие среды могут рассматриваться как новый тип искусственных материалов со своими физическими свойствами.

Основным недостатком большинства поглощающих ЭМИ материалов и конструкций является узкополосность. для повышения эффективности поглощения ЭМИ и расширения рабочего диапазона частот была предложена многослойная конструкция экрана ЭМИ, представляющая собой комбинацию диэлектрических слоев на основе влагосодержащих композиционных материалов с различной величиной диэлектрической проницаемости и слоя с высокой проводимостью для отражения электромагнитного излучения. Электромагнитные свойства композиционных слоев определяются составом и содержанием раствора, а также параметрами пористой структуры матрицы.

Программа моделирования “CST Microwave Studio” использовалась для расчета эффективной площади рассеяния (ЭПР) многослойных конструкций экранов. Требуемая величина влагосодержания композиционных слоев определялась, исходя из толщины пористой основы, рабочей длины волны и оптимизировалась для получения минимального коэффициента отражения многослойной конструкции экрана ЭМИ размером 50×50 см в диапазоне частот 1−20 ГГц. По результатам исследования на частоте 20 ГГц снижение ЭПР с помощью многослойной конструкции экрана ЭМИ составило 9,52 дБ, а на частоте 7 ГГц — на 28,48 дБ.

Таким образом, применение многослойной конструкции экрана ЭМИ, в которой параметры каждого слоя оптимизированы под частоты заданного диапазона позволяет снизить ЭПР на 9,5–28,48 дБ.

ПРИМЕНЕНИЕ КЛИСТРОНОВ-ГЕНЕРАТОРОВ РАЗЛИЧНЫХ КОНСТРУКЦИЙ

А.Б. ГУРИНОВИЧ, И.В. ЛУЩИЦКАЯ

Рассмотрены особенности моделирования и применения для двух- и трехкаскадных клистронов-генераторов. Простейшие двух- и трехкаскадная конструкции генератора, работающего по схеме клистрона с обратной связью, в котором роль как модулятора, так и отбирателя играют резонансные канавки. Электродинамическая система предлагаемой конструкции соответствует пространственно развитой структуре сильноточного релятивистского пучка. Показано, что даже при частичной оптимизации в двухкаскадной конструкции возможен мягкий режим генерации с КПД до 20%, что не уступает классическому карсинотрону. Также показано, что в трехкаскадной конструкции возможен режим генерации с КПД до 31%, что приближается к лучшим вариантам черенковских генераторов.

Проведенные исследования свидетельствуют о достаточно высокой эффективности релятивистских клистронов-генераторов сверхбольшой мощности, сопоставимой с эффективностью лучших вариантов черенковских генераторов такой же мощности. В исследовании показано, что клистрон-генератор имеет ряд преимуществ перед черенковским генератором:

– конструкция клистрона-генератора значительно проще и технологичней;

– в клистроне-генераторе одночастотная резонансная система, что обеспечивает отсутствие паразитных колебаний и неустойчивостей, что характерно для приборов с бегущей волной;

– для клистрона-генератора характерен мягкий режим самовозбуждения;

– конструкция клистрона-генератора имеет большее число параметров оптимизации, чем конструкция черенковского генератора, что предопределят лучшие перспективы для повышения эффективности этого генератора.

Найденные различные варианты для клистронов-генераторов обоих видов, которые с большой эффективностью могут быть использованы в большом количестве приборов, использующих подобные устройства.

ПОЛУЧЕНИЕ ФУНКЦИОНАЛЬНЫХ ПОКРЫТИЙ МЕТОДОМ МАГНИТОЭЛЕКТРОЛИЗА

М.С. ГУРСКИЙ

В настоящее время для получения функциональных покрытий с заданными свойствами, а также элементов и компонентов систем защиты информации широко используют электролитические методы осаждения различных металлов. При этом одной из основных проблем является формирование покрытий высокого качества, обладающих мелкокристаллической структурой, с определенными механическими и электрофизическими свойствами, которые в значительной степени определяются условиями электрокристаллизации. Одним из методов, позволяющим решить некоторые из указанных задач, является метод магнитоэлектролиза, т.е. метод электроосаждения функциональных покрытий при воздействии слабых магнитных полей (СМП).

Установлено, что проведение процесса электроосаждения при наложении постоянного магнитного поля напряженностью до $3 \cdot 10^5$ А/м приводит к изменению свойств как электролитов, так и формируемых покрытий. Результаты

экспериментальных данных и расчетов показывают, что при электроосаждении в СМП снижается энергия зародышеобразования, увеличивается скорость образования зародышей и уменьшается их объем. Благодаря уменьшению диффузионных ограничений происходит ускоренный рост толщины металлической пленки при высокой равномерности, при этом процесс нанесения можно интенсифицировать в 2–4 раза за счет увеличения диапазона рабочих плотностей тока. Такие условия электрокристаллизации приводят к тому, что образуется мелкозернистая, плотноупакованная, практически беспористая с определенной направленностью структура, обладающая улучшенными физико-механическими свойствами.

Полученные результаты положены в основу разработки технологических процессов создания защитных покрытий, мембранных узлов акустических преобразователей и других компонентов систем защиты информации.

МОДЕЛИРОВАНИЕ ОБРАЗОВАНИЯ КРАТЕРОВ НА ПОВЕРХНОСТИ МЕТАЛЛА ПРИ ВОЗДЕЙСТВИИ ПЛАЗМЕННЫХ ПОТОКОВ

Т.И. МАКОВСКАЯ, А.Л. ДАНИЛЮК

Облучение различных материалов интенсивными пучками заряженных частиц или плазменными потоками применяется в технологических целях для получения наноструктурированных поверхностных слоев. Формируемые при этом дефекты кристаллической решетки, образующиеся наноструктурированные пленки, кратеры изменяют прочностные свойства, износостойкость, а также могут быть использованы, в частности, для создания устройств очитки воды от органических загрязнений.

Кратеры образуются в результате комплекса сложных физических процессов. Их исследования важны не только для управления технологическим процессом при плазменной обработке материалов, но и представляют общефизический интерес. В данной работе приводятся результаты моделирования кратерообразования на поверхности металла при воздействии компрессионного плазменного потока, а также закономерности формирования профилей кратеров и полей напряжений.

Моделирование кратерообразование на поверхности металла проведено в зависимости от вида начального возмущения, величины проплавленного поверхностного слоя, величины ускорения поверхности, волнового числа, времени действия импульса ускорения, интервала времени от момента окончания импульса ускорения до кристаллизации жидкой фазы. Рассчитаны функция роста кратера, а также профили кратеров при различных плазменных режимах.

С помощью вычислительного эксперимента определены размеры и форма кратеров. Рассчитаны поля упругих напряжений, возникающих при формировании кратеров. Установлено, что в процессе формирования кратера под его поверхностью возбуждаются поля напряжений, ответственные за структурные изменения в металле.

ИНФОРМАЦИОННАЯ ЗАЩИЩЕННОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ЭКСПРЕССНОЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОТИВОМИКРОБНЫХ ПРЕПАРАТОВ

М.В. ПАРКУН, А.И. ДРАПЕЗА, В.А. ЛОБАН, Г.А. СКОРОХОД, Ю.М. СУДНИК

Экспрессная оценка эффективности противомикробных препаратов является одной из проблем экспериментальной и практической микробиологии. Для решения этой проблемы необходим поиск универсальных и объективных критериев определения жизнеспособности инактивированных микроорганизмов, которые отражали бы характер их повреждения в популяции. Современные подходы к объективной идентификации поврежденных микроорганизмов по категориям их жизнеспособности требуют значительных материальных, временных и интеллектуальных затрат.

Эффективное решение данной проблемы лежит в области создания аппаратно-программных средств получения и обработки многопараметрической информации, с помощью которой физиологическое состояния микроорганизмов, подвергнутых инактивирующему воздействию, может быть отражено более объективно с помощью фазового портрета.

В тоже время перспектива коммерциализации такого рода систем требует и решения вопросов по их информационной защищенности от несанкционированного воспроизводства. При создании автоматизированных систем негосударственного типа требования по их информационной защите, а также выбору для этого необходимых средств, определяются собственником автоматизированной системы, а не нормативно-правовыми документами.

Для защиты информации в разрабатываемой нами системе используется принцип ограниченного доступа к аппаратным и программным ее ресурсам. Это обеспечивается как использованием технологических особенностей изготовления датчиков, так и алгоритмами выделения и предварительной обработки информационных сигналов с помощью программно защищенных микроконтроллеров.

ЭКРАНИРУЮЩИЕ ЭЛЕКТРОМАГНИТНОЕ ИЗЛУЧЕНИЕ ЦЕМЕНТНЫЕ МАТЕРИАЛЫ

М.Ш. МАХМУД, Н.Х.М. АЛАЛЛАК, Е.А. КРИШТОПОВА

Использование экранирующих электромагнитное излечение (ЭМИ) строительных материалов позволяет защитить информацию от утечки через побочные электромагнитные излучения и наводки, а также создать экологически благоприятные условий труда для персонала.

На этапе строительства зданий предлагается использовать цементные растворы с проводящими наполнителями, а также наполнителями, удерживающими капиллярную воду от испарения. В качестве первого наполнителя в настоящей работе использовался минерал шунгит в порошкообразном состоянии с размером фракции до 20 мкм, содержащий 68% кварца, 29% глобулярного углерода, а также оксиды щелочноземельных металлов, связанную воду и органические вещества. В качестве добавки, удерживающей в материале воду в затвердевшем цементном растворе, использовался хлорид кальция.

Были изготовлены образцы экранов ЭМИ, содержащие 40% шунгита, 40% стандартной цементной смеси и 20% хлорида кальция. Жидкая смесь наносилась

на трикотажную основу слоем 5 мм и выдерживалась до полного затвердевания. Способность образца подавлять ЭМИ оценивалась по экспериментально полученным на измерительном комплексе SNA 0,01–18, значениям коэффициентов передачи (S_{21}) и отражения (S_{11}) в диапазоне частот 2–18 ГГц.

Установлено, что образцы ослабляют ЭМИ диапазона 2–18 ГГц на значение от 10 до 30 дБ при значении коэффициента отражения (S_{11}) от –2 до –5 дБ. Для снижения уровня вторично отраженной энергии электромагнитного поля рекомендуется добавить к образцу еще один слой из диэлектрического материала для итогового снижения коэффициента отражения.

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ УДАЛЕННОГО МОНИТОРИНГА ПАРАМЕТРОВ ЭЛЕКТРОСЕТЕЙ

В.П. ЛУГОВСКИЙ

Защита информации от несанкционированного доступа в системах удаленного мониторинга параметров электросетей должна обеспечиваться комплексом технических, организационных и программно-алгоритмических мер. Технические меры должны предусматривать: а) размещение мастера-устройства системы удаленного мониторинга в защищенном помещении; б) опломбирование локальных устройств. Организационные меры должны обеспечивать выполнение работ по эксплуатации и обслуживанию системы удаленного мониторинга персоналом только в пределах своей компетенции, оговоренной нормативно-технической документацией. Программно-алгоритмические средства защиты должны реализовать: а) гарантированное разграничение доступа пользователей и программ пользователей к информации системы удаленного мониторинга; б) обнаружение и регистрацию попыток нарушения разграничения доступа в журнале событий; в) автоматизированную идентификацию персонала при обращении к ресурсам системы; г) регистрацию входа (выхода) в систему, обращений к ресурсам и фактов попыток нарушения доступа в журнале системных событий; д) запрет на несанкционированное изменение конфигурации системы; е) обеспечивать конфиденциальность переданной информации по сети электропитания.

ОПТИМИЗАЦИЯ СТРУКТУРЫ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ЭЛЕКТРОЭНЕРГИИ

В.П. ЛУГОВСКИЙ

Информационно-измерительные системы показателей качества электроэнергии обеспечивают контроль работоспособности и мониторинг состояния как самих электросетей, так и подсоединенного оборудования. При использовании структурированной модели декомпозиции для решения задачи оптимизации структуры информационно-измерительные система разделяется на подсистемы, состоящие из локальных устройств с выделением мастер-устройства, которое имеет возможность работать как в режиме координатора, так и повторителя сигналов. Предложенный способ разбиения учитывается в математической постановке задачи, и предназначен для избавления от большой разреженности матриц, описывающих соединение локальных устройств системы. Для каждой полученной подсистемы возможно отдельное решение задачи оптимизации, что гарантирует отсутствие необходимости многократного возвращения к решению этих подзадач. При

определении расположения (подключения) локальных устройств в соответствии с требованиями структурированных кабельных систем (электросетей) можно воспользоваться адаптированным методом построения минимального дерева.

ВЗАИМОЗАМЕНЯЕМОСТЬ КОМПОНЕНТОВ КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ ЗАЩИТНЫХ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ СВЧ-ДИАПАЗОНА

М.Ш. МАХМУД, Г.А. ПУХИР

Изготовление композиционных материалов экранов электромагнитного излучения (ЭМИ) требует наличия определенных компонентов защитной системы и технологии их обработки для получения ожидаемых результатов экранирования. В условиях оптимизации данного процесса актуальной проблемой является поиск взаимозаменяемых компонентов, позволяющих в кратчайшее время и с минимальными затратами получить композиционный материал защитного экрана ЭМИ с заданным уровнем эффективности по таким показателям, как отражающая способность и поглощение.

В настоящей работе был проведен сравнительный анализ экранирующих свойств образцов экранов на основе углеродосодержащих порошков в гипсовом связующем с добавлением водного раствора солей щелочноземельных металлов и ферритового порошка. Согласно результатам измерений, как для образцов, в которых не содержатся частицы магнитных порошков, но содержится большее количество солевого раствора по объему составляющих композита, так и для образцов с меньшим содержанием солевого раствора и наличием ферритового порошка, величина ослабления в диапазоне 8–12 ГГц составляет порядка 30 дБ. Коэффициент отражения для всех типов образцов составляет порядка –5 дБ. Экранирующие характеристики стабильны и имеют идентичную форму во всем исследуемом частотном диапазоне.

Полученные результаты можно аргументировать ранее установленным свойствам щелочноземельных металлов на примере кальция увеличивать намагниченность частиц различных материалов за счет усиления обменных процессов между ионами металлов, приводящих к переориентации спинов. Это дает возможность использовать данное свойство при выборе компонентов экранов ЭМИ на основе различных композиционных материалов.

ОПТИЧЕСКИЕ СВОЙСТВА ШУНГИТСОДЕРЖАЩИХ МАТЕРИАЛОВ

М.Ш. МАХМУД М.М. АВСИ, М.А. АЛЬ-ХИЗАИ, А.М. ПРУДНИК, Л.М. ЛЫНЬКОВ

Свойства композиционных материалов определяются не только по свойствам компонентов, но и их взаимодействием. Их компоненты должны быть хорошо совместимы и при этом не должны растворяться или иным способом поглощать друг друга.

При разработке и изготовлении композиционных материалов, а также при создании конструкций на их основе приходится учитывать влияние внешних условий, например, температура, высокая влажность. Необходимо учитывать и ряд специфических свойств композиционных материалов. Так, учет ползучести, которая является характерным свойством многих композиционных материалов, заставляет проектировщиков отказываться от целого ряда традиционных решений.

Для изготовления экспериментальных образцов композиционных материалов использовался шунгит и связующее вещество — прозрачный силикон, стойкий к воздействию температур в диапазоне –40÷+150°С, позволяющий получать гибкие материалы.

Образец из шунгита отражает большую долю падающего светового потока, что подтверждается увеличением значения СКЯ до 0,02…0,05 для всех углов падения света и визирования, за исключением угла визирования 70° при угле падения света 40° (поляризация 0° и 45°) и угле падения света 50°, при которых СКЯ составляет 0,04–0,05. Отражение светового потока от поверхности образца из шунгита обусловлено двумя факторами: геометрическими неровностями поверхности образца, вызванными порошкообразной формой исходного материала, и химическими неоднородностями каждой из частиц, представляющей собой вкрапления кварца в углеродную матрицу. Вследствие наличия в шунгите включений α-кварца значение степени поляризации по сравнению с активированным углем незначительно снижается до 0,05–0,45, что свидетельствует о зеркальной составляющей в отражении светового потока.

ФОТОПРИЕМНОЕ УСТРОЙСТВО МОДУЛЯ АВТОМАТИЧЕСКОЙ ЮСТИРОВКИ ПРИЕМОПЕРЕДАТЧИКА СИСТЕМЫ АТМОСФЕРНОЙ ОПТИЧЕСКОЙ СВЯЗИ

К.В. МЕЛЬНИКОВ, С.Б. БИРЮЧИНСКИЙ

Одним из главных преимуществ систем передачи информации по оптическим атмосферным линиям связи (АОЛС) является повышенная скрытность, обусловленная исчезающе малой величиной уровня боковых лепестков диаграммы направленности оптических антенных систем.

Для систем связи, включающих в себя возимые либо стационарные базовые станции с известными координатами и передвижные маломощные приемопередающие узлы сети, актуальной является проблема точной настройки АОЛС. для решения данной проблемы предложено использовать мощный импульсный лазер на стороне базовой станции и отдельное фотоприемное устройство (ФПУ) на приемной стороне с квадрантным либо сегментным фотодетектором на базе лавинного фотодиода (ЛФД) для определения направления максимальной интенсивности принятого сигнала в азимутальной и угломестной плоскостях с последующей регулировкой положения приемопередающей оптики в пространстве.

В данном случае дополнительной проблемой является обеспечение совпадения оптических осей приемных объективов канала юстировки и канала приема данных и телескопа передающего канала оптической системы.

Представлена схема оптической антенной системы, базирующаяся на схеме двойного зеркала Манжена, позволяющая решить вышеуказанную проблему соосности каналов.

Проведены теоретические исследования оптимизации параметров ФПУ по чувствительности в зависимости от величины коэффициента лавинного умножения фотодетектора (ЛФД) и шумовых параметров входного каскада, построенного по схеме трансимпедансного усилителя, на основании которых предложена методика оптимизации фотоприемного устройства.

Представлены характеристики разработанного на базе вышеуказанной методики оптимизации ФПУ с рабочим диапазоном длин волн 1,0–1,6 мкм.

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ПЕРЕНОСА ЭЛЕКТРОНОВ В ГЕТЕРОСТРУКТУРАХ $GaAs–Al_xGa_{1–x}As$

В.Н. МИЩЕНКО

Исследование электронного транспорта в полевых транзисторах с соединением $GaAs–Al_xGa_{1–x}As$, формирующих двумерный электронный газ с высокой подвижностью, вызывает особый интерес, который связан с возможностью создания на основе этих приборов приемников, генераторов и ряда других телекоммуникационных устройств. Разработана программа моделирования переноса электронов в гетероструктурном приборе на основе соединения $GaAs–Al_xGa_{1–x}As$, используя процедуру решения уравнений Шредингера и Пуассона. Основной особенностью этой программы является наличие итерационной процедуры совместного решения уравнений Шредингера и Пуассона. Используя процедуру метода Монте-Карло, были исследованы процессы переноса электронов в различных областях прибора, содержащего соединения $GaAs–Al_xGa_{1–x}As$. Определены основные выходные параметры транзисторов при величине молярной доли Al x=0,3 и различных температурах. Использование исследованных структур позволяет создавать, при соответствующем выборе размеров рабочей области, транзисторы, работающие в высокочастотной части диапазона КВЧ.

МОДИФИЦИРОВАННАЯ УСТАНОВКА ДЛЯ ОПРЕДЕЛЕНИЯ АКУСТИЧЕСКИХ ХАРАКТЕРИСТИК ЗВУКОИЗОЛИРУЮЩИХ ПАНЕЛЕЙ

С.Н. ПЕТРОВ, А.М. ЭПЕМУ, А.М. ПРУДНИК, Т.В. БОРБОТЬКО

На сегодняшний день сертифицированные лаборатории проводят измерения звукоизоляции строительных конструкций в больших звукомерных камерах с общим объемом свыше 120 м^3 и площадью исследуемых образцов порядка 8 м^2. Малогабаритные установки с объемом в несколько кубических метров позволяют провести экспресс-оценку звукоизоляции образцов. В данном случае некоторое снижение точности получаемых результатов измерений компенсируется скоростью проведения измерений и малыми размерами необходимых для измерения образцов. Такой подход может быть приемлем в тех случаях, когда необходимо отобрать из ряда образцов несколько, обладающих наилучшими характеристиками.

Измерительная установка, предназначенная для измерения звукоизоляции плоских образцов, выполнена в виде двух камер цилиндрической формы, установленных соосно на металлической станине. В одной камере (неподвижной) установлен микрофон, в другой (подвижной) — динамик. Звукоизоляция образца определялась как разность уровня звукового давления при прямом прохождении звука и уровня звукового давления при прохождении звука через исследуемый образец. Внутренний объем установки составляет 0,07 м^3. Частотный диапазон проводимых измерений — от 200 до 8 000 Гц. Тип генерируемого сигнала — белый шум.

Для снижения косвенной передачи звука в камеру низкого уровня через металлическую станину, внутренняя и внешняя поверхности установки (включая камеры и станину) облицованы вибропоглотителем STP Bimast-Bomb. Станина установлена на виброизолирующие опоры. Для достижения равномерной АЧХ излучательной системы был выбран тип акустического оформления закрытый ящик. Объем камеры был выбран таким образом, чтобы резонансная частота системы находилась за границами частотного диапазона измерений.

ЗВУКОИЗОЛИРУЮЩИЕ СВОЙСТВА ПАНЕЛЕЙ ЭЛЕКТРОМАГНИТНО-АКУСТИЧЕСКОЙ ЗАЩИТЫ

С.Н. ПЕТРОВ, М.А. ГОТОВКО, А.М. ЭПЕМУ, А.М. ПРУДНИК

Комбинированные панели электромагнитно-акустической защиты предназначены для защиты информации от утечки по техническим (электромагнитному и акустическому) каналам. Панель включает в себя несколько слоев стекломагнезита, битумной мастики с высоким содержанием углерода и алюминиевой фольги. Комбинированная панель толщиной не более 16 мм обеспечивает ослабление электромагнитных волн не менее чем на 25 дБ в диапазоне 0,009–120 ГГц, ослабление акустических волн не менее чем на 20 дБ в диапазоне 160–8000 Гц.

Построение интегрированных защитных помещений обычно состоит из поэтапного монтажа на ограждающих конструкциях помещения экранов электромагнитного излучения и звукоизолятора. Такой подход имеет следующие недостатки, во-первых, значительное время проведения работ, во-вторых, большое число монтажных соединений, со временем приводящих к снижению защитных свойств всей конструкции.

Применение комбинированных панелей для построения специальных помещений позволяет снизить время монтажа за счет того что в одном материале объединены свойства как звукоизолятора, так и поглотителя электромагнитного излучения. Исследование звукоизоляции конструкции в местах крепления к металлическому каркасу (соединительных швах) показало лишь незначительное снижение звукоизоляции по сравнению с цельной панелью. Все это говорит о перспективности построения защищенных помещений из унифицированных модульных элементов на базе комбинированных защитных панелей.

ЭКРАНИРУЮЩИЕ СВОЙСТВА КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ НА ОСНОВЕ СИНТЕТИЧЕСКОГО ПОЛИМЕРА

ХУССЕЙН МОХАМЕД АЛЬЛЯБАД, ЯХИЯ ТАХА АЛЬ-АДЕМИ, Т.А. ПУЛКО

Характерным свойством пространственно сшитых полимерных гидрогелей является способность к ограниченному набуханию в воде и других полярных жидкостях, обратному процессу уменьшения объема гелей с выделением ранее сорбированной жидкости под действием изменений во внешней среде (pH, температура и др.).

Исследовались образцы экранирующих материалов на основе водосодержащего полимерного гидрогеля и гранулированного силикагеля, с последующим формированием композиционной структуры синтетическим полимером с низкой молекулярной массой, характеризующимся высокими связующими свойствами и эффективной полимеризацией. Для исследования экранирующих характеристик разработанных образцов композиционных материалов использовались панорамные измерители КСВН и ослабления. Измерения проводились в диапазоне частот 8,0–11,5 ГГц после проведения стандартных калибровок на прохождение и отражение.

В исследованных диапазонах частот исследуемые образцы толщиной 0,5 мм создают ослабление ЭМИ порядка 6,4–7,9 дБ. Потери энергии ЭМИ в образцах композиционных материалов, связаны с диэлектрическими потерями, обусловленными присутствием кремния и небольшого количества связанной воды, сорбированной в пористой структуре полимерного гидрогеля. Коэффициент

отражения ЭМИ образцов находится в пределах –8,6÷–10,8 дБ в диапазоне частот 8,0–11,5 ГГц.

Установлена эффективность экранирования в диапазоне частот 8,0–11,5 ГГц и исследуемыми образцами композиционных материалов на основе полимерных гидрогелей в синтетическом полимерном связующем, с добавлением гранулированного силикагеля, что позволило повысить конструктивно-технологические и эксплуатационные параметры разработанных образцов поглотителей ЭМИ для экранированных помещений.

КОМПОЗИЦИОННЫЕ ВЛАГОСОДЕРЖАЩИЕ МАТЕРИАЛЫ ДЛЯ ЭЛЕМЕНТОВ ЗАЩИТЫ ЧЕЛОВЕКА В СВЧ-ДИАПАЗОНЕ

ЯХИЯ ТАХА АЛЬ-АДЕМИ

Защита организма человека от действия электромагнитных излучений предполагает снижение их интенсивности до уровней, не превышающих предельно допустимые. Защита обеспечивается выбором конкретных методов и средств, учетом их экономических показателей, простотой и надежностью эксплуатации. Индивидуальные средства защиты предназначены для предотвращения воздействия на организм человека ЭМИ с уровнями, превышающими предельно допустимые, когда применение иных способов и средств невозможно или нецелесообразно. Они могут обеспечить общую защиту, либо локальную защиту тела.

Для защиты человека от ЭМИ СВЧ-диапазона разработаны образцы композиционных влагосодержащих материалов на основе капиллярно-пористого материала, пропитанных раствором соли щелочноземельного металла равновесной концентрации, с покрытием поверхности образцов раствором гидрофильного полимера. Для исследования экранирующих характеристик разработанных образцов композиционных материалов использовались панорамные измерители КСВН и ослабления в диапазоне частот 8,0–11,5 ГГц после проведения стандартных калибровок на прохождение и отражение. Измерение комплексного сопротивления в диапазоне частот 25 Гц–1 ГГц осуществлялось методом наложения стандартных пластинчатых металлических электродов размером 60×30 мм. Образцы композиционных влагосодержащих материалов толщиной 3 мм обеспечивают ослабление ЭМИ порядка 7,2–7,9 дБ при коэффициенте отражения –3,8 дБ в диапазоне частот 8,0–11,5 ГГц. Комплексное сопротивление образцов материалов находится в пределах 0,22–3 кОм и в выбранном диапазоне частот соответствует заданному параметру тканей человека (±0,25 кОм).

Разработанные композиционные влагосодержащие материалы, в соответствии с полученными характеристиками, могут использоваться для имитации кожных и подкожных покровов тела человека при проведении медицинских исследований в СВЧ-диапазоне, для создания материалов, имитирующих электромагнитные характеристики биологических объектов, а также для производства недорогих экранирующих материалов с улучшенной стабильностью свойств, которые позволят эффективно защищать электронное оборудование и в целом организм человека от вредных воздействий ЭМИ.

ПОЛИМЕРНЫЕ ВОДОСОДЕРЖАЩИЕ МАТЕРИАЛЫ ДЛЯ СРЕДСТВ ЭКРАНИРОВАНИЯ

Ю.В. СМИРНОВ, Т.А. ПУЛКО

Изучение деталей процессов набухания дисперсных гидрогелей в воде и других полярных жидкостях, а также процессов адсорбции ими паров растворителей различной природы имеет исключительно важное значение при создании водосодержащих экранирующих материалов со стабильными свойствами. Для повышения стабильности водосодержащих материалов предложено использование полимерного комплекса на основе гидрогеля в составе синтетического полимера с добавлением поливинилового спирта, которые отличаются высокими абсорбирующими свойствами. В результате получен гибкий полимерный водосодержащий материал с неоднородной структурой и неравномерным распределением водных растворов по объёму материала. Эффективность экранирования исследуемых материалов в диапазоне СВЧ характеризуется коэффициентом ослабления энергии ЭМИ и коэффициентом отражения электромагнитных волн от экрана. Измерения проводились после проведения стандартных калибровок в диапазоне частот 8,0–11,5 ГГц.

Разработанные образцы материалов толщиной 0,3 мм обеспечивают ослабление ЭМИ порядка 2,8–3,9 дБ, при коэффициенте отражения ЭМИ в пределах –8,6÷–10,8 дБ. Исследования показали, что образцы водосодержащих полимерных материалов в диапазоне частот 8,0–11,5 ГГц обеспечивают эффективность экранирования, вследствие диэлектрических потерь, обусловленных стабильным уровнем водосодержания образцов. Следовательно, предложенная методика стабилизации уровня влагосодержания материалов путём инкапсулирования водных растворов в объёме полимерных гидрогелей, обеспечивает эффективность экранирования элементов конструкций экранов ЭМИ на основе капиллярно-пористых материалов в течение длительного периода эксплуатации

ИМИТАТОРЫ РАДИОПОГЛОЩАЮЩИХ СВОЙСТВ БИОЛОГИЧЕСКИХ ТКАНЕЙ

ЯХИЯ ТАХА АЛЬ-АДАМИ, Т.А. ПУЛКО, М.В. ДАВЫДОВ

Для защиты биологических тканей и в целом организма человека от воздействия СВЧ-излучений и имитации биологической ткани при проведении медико-биологических экспериментов предлагаются принципиально новые защитные средства, ослабляющие ЭМИ СВЧ диапазона и экологически совместимые с человеческим организмом.

Исследовались образцы композиционных материалов на основе волокнистого материала, пропитанных раствором натриевой соли соляной кислоты различной концентрации. Для оценки импедансных свойств композиционных влагосодержащих структур проводилось измерение комплексного сопротивления в диапазоне частот 25 Гц–1 МГц, методом наложения стандартных пластинчатых металлических электродов размером 60×30 мм. Для исследования экранирующих характеристик разработанных образцов композиционных материалов использовались панорамные измерители КСВН и ослабления в диапазоне частот 8,0–11,5 ГГц после проведения стандартных калибровок на прохождение и отражение.

Комплексное сопротивление образцов, пропитанных раствором 20% масс. Концентрации находится в пределах 0,37–4,45 кОм, что соответствует комплексному сопротивлению кожных покровов человека (±0,25 кОм). В исследованных диапазонах частот образцы композиционных материалов толщиной 3 мм обеспечивают ослабление ЭМИ порядка 11,5–15,5 дБ при коэффициенте отражения ЭМИ образцов находится в пределах –3,4÷–5,1 дБ в диапазоне частот 8,0–11,5 ГГц.

Электрические свойства и диэлектрическая проницаемость полученных образцов обладают дисперсией, связанной с состоянием заряженных частиц при действии электромагнитных полей различной частоты, что указывает на различие механизмов поляризации материала в разных частотных диапазонах, в которых запаздывание ориентационной поляризации различных волокнистых структур и макромолекул относительно изменения электромагнитных полей минимально. Это позволяет использовать их для имитации кожных и подкожных покровов тела человека, и защиты от воздействия ЭМИ СВЧ диапазона.

КОНСТРУКТИВНО-ТЕХНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ТЕПЛОВЫХ ПИРОПРИЕМНИКОВ

В.А. СТОЛЕР, Д.В. СТОЛЕР

В приборах наблюдения и системах охраны объектов народного хозяйства все чаще используется одна из таких групп тепловых приемников, как пироэлектрические, принцип действия которых основан на использовании пироэлектрического эффекта, заключающегося в изменении поляризации сегнетоэлектрика во времени при воздействии на него потока излучения. Пироэлектрические приемники обладают рядом достоинств: хорошее быстродействие при высокой пороговой чувствительности; большое значение коэффициента преобразования; большой динамический диапазон.

В зависимости от назначения пироприемников основной акцент при выборе сегнетоэлектрика ставится или на комплекс его физических свойств для достижения заданных эксплуатационных характеристик, или на конструктивно-технологические возможности материалов для варьирования их геометрическими размерами и формой.

Применяются несколько вариантов конструкции: продольного типа, когда направление потока излучения параллельно пироэлектрическому току в кристалле; поперечного типа, когда направление потока излучения перпендикулярно пиротоку в кристалле. Для исключения влияния фонового излучения и больших перепадов температуры окружающей среды и получения знакопеременного выходного напряжения при перемещении сфокусированного изображения объекта по поверхности пироприемника применяют четное количество кристаллов, соединенных последовательно с чередующейся полярностью.

Из известных монокристаллических сегнетоэлектриков таких как танталат лития, ниобат бария-стронция вызывает интерес триглицинсульфат и его изоморфы, на основе которых получаются неплохие пироэлектрические приемники излучения [1]. Исследование характеристик и структуры кристаллов, точки фазового перехода, коэффициента теплового расширения триглицинсульфата говорит о его перспективности.

Литература

1. Столер В.А., Столер Д.В. // Сборник тез. докл. VIII Белорусско-российской НТК «Технические средства защиты информации», 24–28 мая 2010 г., Браслав. Минск: БГУИР, 2010, С. 79–80.

РАССЕИВАЮЩИЕ ПОКРЫТИЯ ОПТИЧЕСКОГО ДИАПАЗОНА НА ОСНОВЕ ОРГАНИЧЕСКИХ КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ

Л.М. ЛЫНЬКОВ, Т.В. БОРБОТЬКО, Д.В. СТОЛЕР

Композиционные материалы могут применяться для формирования оптических рассеивающих покрытий с требуемыми значениями спектрально-поляризационных характеристик, которые могут варьироваться в зависимости от концентрации и размеров частиц порошкообразного наполнителя.

Были исследованы зависимости спектрально-поляризационных характеристик композиционных материалов от различных концентраций органического наполнителя, в качестве которого были использованы порошкообразные хна и лавр. Для создания композиции использовался прозрачный силикон. Образцы изготавливались с объемным содержанием порошкообразного наполнителя 20% и 30%.

Исследование материалов выполнялось в видимом и ближнем инфракрасном диапазонах длин волн 400…2400 нм. Для этой цели был использован спектрорадиометр ПСР-02. Угол падения коллимированного пучка света на исследуемый объект составлял 45°, а углы наблюдения — от 5° до 65°. в поляризационной насадке использовалось три положения оси поляроида относительно вертикальной плоскости: 0°, 45° и 90°. Полученные данные использовались для вычисления спектрального коэффициента яркости (СКЯ) и степени поляризации.

В результате было установлено, что СКЯ порошкообразных лавра и хны имеет сходство с СКЯ растительности. Полученные композиты диффузно рассеивают электромагнитное излучение видимого и ближнего инфракрасного диапазонов длин волн. Изменение объемного содержания порошкообразного материала в композите с 20% до 30% позволяет управляемо изменять СКЯ и степень поляризации излучения, отраженного и рассеянного этими композитными материалами. Увеличение объемного содержания порошкообразных лавра и хны в композите более 30% является не целесообразным, так как снижаются прочностные характеристики материала.

МИКРОМИНИАТЮРНОЕ РАДИОПРИЕМНОЕ УСТРОЙСТВО НА УГЛЕРОДНЫХ НАНОТРУБКАХ

А.С. ТЫМОЩИК, Е.С. ТАМАШЕВИЧ, А.Г. ЧЕРНЫХ, М.А. КОРНИЦКИЙ

Интерес, проявляемый к разработке микроминиатюрных радиоприемных устройств, не утихает по сей день. Так, группа разработчиков Центра интегрированных наномеханических систем Университета Калифорнии выступила с предложением по использованию углеродной нанотрубки в качестве ключевого элемента радиоприемного устройства. В предлагаемой конструкции нанотрубка выполняет одновременно роль антенны, узкополосного фильтра и демодулятора радиосигнала. Несмотря на превосходные физические и электрические характеристики нанотрубок, технологический барьер манипулирования одиночными нанотрубками вызывает наибольшие опасения. Одним из методов манипулирования одиночными нанотрубками является их физическое перемещение в желаемую позицию метод с помощью зонда атомно-силового микроскопа. Электроннолучевая литография помогает сделать контакт к таким нанотрубкам.

к сожалению, данная комбинация методов не обладает масштабируемостью для массового применения.

Нами предложена технология встраивания как отдельных, так и группы углеродных нанотрубок в приборные структуры и конструкция радиоприемного устройства на их основе. Предлагаемая технология встраивания нанотрубок использует разновидность электрофореза, широко используемого при работе с биологическими объектами и позволяющего как перемещать отдельные частицы, так и производить их разделение по свойствам. С помощью вышеуказанного метода получены экспериментальные тестовые образцы отдельных структур радиоприемного устройства.

ИНВАРИАНТНАЯ К ПАРАЛЛАКСУ ПАРАМЕТРИЗАЦИЯ РЕПЕРОВ ДЛЯ ЭФФЕКТИВНОГО КОДИРОВАНИЯ МНОГОРАКУРСНЫХ ИЗОБРАЖЕНИЙ В СИСТЕМЕ ВИДЕОМОНИТОРИНГА

О.ДЖ. АЛЬ-ФУРАЙДЖИ, К.Т. АЛЬ-ШАМЕРИ, А.С. АЛЬ-АЛЕМ, В.Ю. ЦВЕТКОВ

Проведен анализ эффективности методов локализации и параметризации реперов на изображениях для эффективного кодирования видеоинформации с устранением межракурсной избыточности в системе распределенного видеомониторинга. Установлено, что известные методы SIFT и SURF не обеспечивают локализацию и параметризацию реперов в реальном масштабе времени. Это обусловлено использованием большого числа разномасштабных аппроксимированных образов исходных изображений для поиска реперов и формирования их идентификаторов, что обеспечивает инвариантность результатов поиска соответствия с использованием данных идентификаторов, однако достигается за счет высокой вычислительной сложности. Кроме того, идентификаторы, формируемые с помощью SIFT и SURF, характеризуют распределение градиента яркости в окрестности реперов без учета локальной структуры изображений, что не обеспечивает инвариантность идентификации к параллаксу и снижает эффективность использования данных методов для поиска соответствия при многоракурсном эффективном кодировании изображений. Для устранения данных недостатков разработан метод локализации и параметризации реперов, основанный на поиске пар соответствующих друг другу угловых контурных реперов на смежных уровнях аппроксимированного кратномасштабного представления изображения и параметризации окрестности этих реперов с использованием распределения вероятностей угловых расстояний между равноудаленными от реперов контурными точками для смежных углов, образованных контурами в окрестностях реперов. Установлено, что в сравнении с SIFT и SURF, данный метод обеспечивает идентификацию реперов инвариантно к параллаксу и снижение вычислительной сложности их локализации примерно в 100 и 10 раз соответственно.

СЕКЦИЯ 5. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ХОЗЯЙСТВЕННЫХ ОБЪЕКТОВ

ЗАКОНЫ РАСПРЕДЕЛЕНИЯ ДАЛЬНОСТИ ДЕЙСТВИЯ УСТРОЙСТВ ОБНАРУЖЕНИЯ ПРОСТРАНСТВЕННЫХ ОХРАННЫХ СИСТЕМ

В.И. ВОЛОВАЧ

Законом распределения дальности действия называется соотношение, устанавливающее связь между возможными значениями дальности действия охранной системы и соответствующими вероятностями обнаружения объекта. Как правило, интегральная кривая, характеризующая зависимость вероятности обнаружения от дальности действия, стремится к нулю на максимальных дальностях, и к единице на минимальных дальностях обнаружения объекта.

Если рассматривать обнаружение объектов как случайный процесс, осуществляемый в достаточно однородных «типичных» условиях, то распределение дальностей обнаружения подчиняется тому или иному закону распределения. При типизации условий ограничивается влияние некоторых доминирующих факторов на процесс обнаружения. У каждой отдельной категории «типичных» условий имеются возможности для реализации того или иного закона распределения, когда получение определенного значения дальности действия радиотехнического устройства, как случайной величины, обусловливается воздействием большого числа незначительных по силе своего влияния факторов.

При расчете ожидаемой дальности действия радиотехнических устройств охраны необходимо использовать вероятностно-статистические методы, при которых обнаружение объектов на той или иной дальности оценивается с помощью статистически обоснованной вероятности получения указанной дальности.

В результате исследований были получены законы распределения дальности действия охранных систем применительно к двигающемуся протяженному объекту в зависимости от скорости его движения, характера отражающей поверхности, условий работы радиотехнических устройств обнаружения, с учетом статистических характеристик отраженных сигналов, а также формы диаграммы направленности устройств обнаружения.

К ВОПРОСУ ОПРЕДЕЛЕНИЯ НАКАПЛИВАЮЩЕЙСЯ ВЕРОЯТНОСТИ ОБНАРУЖЕНИЯ В ЗОНЕ КОНТРОЛЯ ПРОСТРАНСТВЕННЫХ ОХРАННЫХ СИСТЕМ

В.И. ВОЛОВАЧ

В зависимости от особенностей охранных систем и способов их использования обследование пространства в процессе проведения поиска может быть непрерывным во времени и оцениваться мгновенной вероятностью g обнаружения объекта на данной дальности путем одного мгновенного наблюдения, или состоять из отдельных мгновенных актов, при котором критерием для оценки эффективности является мгновенная вероятность γdt обнаружения.

Эффективность обнаружения охранной системой объекта за то или иное время может быть оценена с помощью накапливающихся (нарастающих) вероятностей

обнаружения объекта, определяемых для различных условий наблюдения и для различного характера поведения объекта, прежде всего, скорости его движения. Отметим, что для быстро движущихся объектов можно считать, что за время их движения в зоне контроля охранной системы, ограниченной предельной дальностью обнаружения, не происходит существенного изменения физических условий наблюдения и, соответственно, названных мгновенных вероятностей обнаружения.

Для прямого нахождения накапливающейся вероятности обнаружения $P(t)$ необходимо найти, прежде всего, аналитические зависимости закона установления приборного контакта охранных систем при изменении расстояния между объектом и устройством обнаружения в двухмерной и трехмерной системе координат.

В докладе показано, что при известных законах распределения дальности действия устройств охраны оценка ожидаемой вероятности установления приборного контакта сводится к нахождению $P(t)$ на основе функции мгновенной вероятности обнаружения $\gamma=\gamma(t)$, определяемой с учетом характеристик этих законов и характера движения объекта.

РАЗРАБОТКА АППАРАТНО-ПРОГРАММНОГО ВИДЕОТЕПЛОВОГО КОМПЛЕКСА ДИСТАНЦИОННОГО ОБНАРУЖЕНИЯ ПОЖАРОВ

Л.В. КАТКОВСКИЙ, С.Ю. ВОРОБЬЕВ, Р.П. БОГУШ, Н.В. БРОВКО

Разрабатываемый аппаратно-программный комплекс представляет собой автономную оптоэлектронную систему видеонаблюдения, снабженную ИК-датчиками, применяемыми для параллельной (одновременной) регистрации видеоизображения и таких факторов пожара как превышение инфракрасного излучения (превышения температуры) над фоновым, и может быть использовано на промышленных предприятиях, объектах транспортной инфраструктуры, лесном и сельском хозяйстве, логистических объектах, топливно-энергетическом комплексе для раннего обнаружения пожара.

Видеотепловой комплекс состоит из цветной цифровой видеокамеры, одноэлементных (либо, в варианте исполнения, малоформатных матриц с небольшим числом элементов) приемников излучения среднего и теплового ИК-диапазонов, с полями зрения соответствующими полю зрения видеокамеры, блоков питания, управления и обработки, помещенных в общий корпус. ПО обработки данных совместно использует цветовые (RGB) данные, сигналы ИК-каналов и движение (пространственно-временные изменения) для классификации областей пожара и не-пожара в последовательности кадров в реальном масштабе времени.

ИСПОЛЬЗОВАНИЕ ТЕОРИИ ИГР ПРИ МИНИМИЗАЦИИ РИСКОВ В БАНКОВСКИХ СИСТЕМАХ

Е.В. ВАЛАХАНОВИЧ

Одной из важнейших задач защиты информационных ресурсов в банковских системах является минимизация рисков. Под риском понимаются возможные потери вследствие воздействия угроз через уязвимые места системы. Риск реализуется через ущерб, который можно измерить. Ущерб наступает, если реализуется риск, вследствие уязвимости объекта к неблагоприятным воздействиям.

Использование натурного эксперимента для оценки рисков и их минимизации трудно осуществимо из-за колоссальных материальных затрат, высокой трудоемкости, и невозможности охвата всех возможных сочетаний воздействующих угроз и возможных режимов функционирования банковских систем.

В связи с этим для оценки рисков в банковских системах целесообразно применять математическое моделирование, которое позволяет решать задачи, включающие элементы непрерывного и дискретного действия с учетом факторов случайного воздействия.

Из математических методов оценки рисков наиболее предпочтительными представляются методы, основанные на базе теории игр. В работе для оценки банковских систем использованы антагонистические игры в нормальной форме, отличие которых от остальных игр в том, что в них нет никаких переговоров между игроками: если один выигрывает, то другой проигрывает.

В общем случае модель игры представляет собой конечную игру, в которой игрок A (банк) имеет m стратегий, а игрок в (злоумышленник) имеет n стратегий. Такая игра называется игрой $m \times n$. Стратегии, соответственно, обозначаются: A_1, A_2, …, A_m — для игрока A; B_1, B_2, …, B_n — для игрока B. Нормальная форма конечной антагонистической игры сводится к некоторой матрице игры размером $m \times n$, где m — число строк матрицы, равное числу стратегий игрока A; n — число столбцов матрицы, равное числу стратегий игрока B. Выигрыш — если игрок A выбирает i-ю стратегию, а игрок B выбирает j-ю стратегию — представляет собой элемент a_{ij} в i-й строке и j-м столбце матрицы.

Если игра состоит только из личных ходов, то выбор стратегий A_i и B_j игроками однозначно определяет исход игры — выигрыш a_{ij} игрока A. Если игра содержит кроме личных ходов и случайные ходы, то выигрыш при паре стратегий A_i и B_j есть величина случайная, зависящая от исходов всех случайных ходов. В этом случае естественной оценкой возможного выигрыша является математическое ожидание случайного выигрыша.

Ставится задача: определить наилучшую среди стратегий $A_1, A_2, \ldots, A_m$ игрока A. Последовательно анализируется каждая из них от A_1 до A_m. Выбирая A_i, нужно учитывать, что противник ответит на нее той из стратегий B_j, для которой выигрыш игрока A минимален. В каждой строке матрицы находится минимальный элемент a_i. Затем среди чисел a_1, a_2, …a_m выбирается максимальное число.

Если игрок A будет придерживаться описанной выше стратегии, то при любом поведении игрока B игроку A гарантирован выигрыш, не меньший α. Эта величина α называется нижней ценой игры, максиминным выигрышем или максимином. Соответствующая стратегия называется максиминной стратегией. Аналогично рассматривается минимальный проигрыш игрока B, т.е. верхняя цена игры. Ей соответствует минимаксная стратегия игры.

Выбранный метод позволяет игрокам применять принцип осторожности, диктующий им выбор соответствующих стратегий (максиминной и минимаксной) и являющийся в теории игр основным принципом — принципом минимакса. Основной сложностью в ходе применения данного метода является определение размерности матрицы при моделировании случайных ходов игроков.

Таким образом, методы теории игр могут рассматриваться как математический инструмент для анализа ситуаций, характеризующихся конфликтом сторон и неопределенностью.

Литература

1. Оуэн Г. Теория игр. М., 1971.
2. Краснов М.Л., Киселев А.И., Макаренко Г.И. и др. Вся высшая математика. М., 2002.
3. Бандурин А.В., Чуб Б.А. «Стратегический менеджмент организации» М., 2005.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ АУДИТОВ СИСТЕМ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В.В. МАЛИКОВ, И.В. БЕНЕДИКТОВИЧ, С.А. ЧУРЮКАНОВ

Согласно п. 14 Концепции национальной безопасности Республики Беларусь обеспечение надежности и устойчивости функционирования критически важных объектов информатизации (КВОИ) является одним из основных национальных интересов в информационной сфере Республики Беларусь.

Проблема безопасности КВОИ заключается в следующем: создатель объекта и его составляющих, в том числе средств автоматизации, стремиться к обеспечению наибольшей эффективности объекта. Однако, ввиду наличия угроз информационной безопасности КВОИ, разработчик систем защиты независимо от его решений вынужден снижать эффективность объекта. Для того чтобы степень снижения эффективности лежала в рамках допустимых значений, целесообразно выполнение следующих мероприятий: внедрение новых систем защиты и модернизация существующих должна быть экономически целесообразной, что требует разработки методик оценки их эффективности.

В целях определения соответствия функциональных характеристик КВОИ требованиям, установленным эксплуатационной документацией на КВОИ и техническими нормативными правовыми актами необходимо проведение внутренних и внешних аудитов систем защиты.

Концептуальные основы организации и проведения аудитов систем комплексной безопасности КВОИ включают:

– методику оценки эффективности проектируемых и эксплуатируемых систем защиты КВОИ;

– методику повышения эффективности эксплуатируемых систем защиты КВОИ;

– методику автоматизации подходов по эффективной эксплуатации и модернизации систем защиты КВОИ.

Для методического обеспечения указанных выше концептуальных основ дополнительно необходима разработка:

– целевых критериев эффективности систем защиты КВОИ путем выделения группы критически важных показателей и определения эффективных значений их параметров.

– краткого каталога требований на основные структурные уровни системы защиты КВОИ, основанного на тематических классификационных шаблонах составных компонентов системы безопасности.

Предлагаемые концептуальные основы организации и проведения аудитов систем комплексной безопасности КВОИ позволят решить ряд задач в рамках Концепции национальной безопасности Республики Беларусь, что обеспечит комплексную безопасность КВОИ на качественно новом научно-теоретическом и практическом уровне.

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ФАЗОВОГО МЕТОДА ДЛЯ ОБНАРУЖЕНИЯ СМЕЩЕНИЯ ОБЪЕКТОВ В РЕЗУЛЬТАТЕ АНАЛИЗА ИЗОБРАЖЕНИЙ

А.С. МАМЕДОВ

Обнаружение объектов, исследование их характеристик и свойств, основываясь на результатах анализа изображений, подразумевает учет некоторых особенностей. Решая вопрос обнаружения, нельзя забывать о том, что смещение объектов может осуществляться с такими незначительными скоростями, которые, в силу специфики структуры цифровых изображений, зафиксировать в полной мере будет трудно, не говоря уже об определении значения характеристик изучаемого объекта. В этой ситуации процедура анализа может оказаться недостаточно достоверной, т.е. привести к полной несостоятельности самой методики и, соответственно, полученных результатов.

В связи с отмеченными особенностями, возникает задача применения высокопрецизионного метода обнаружения смещения объектов в результате анализа их изображений. Не секрет, что в области цифровой обработки изображений весьма успешно себя зарекомендовал Фурье-анализ. Данный инструмент исследования подразумевает рассмотрение изображения с другой точки зрения. А именно, каждый элемент (пиксель) изображения характеризуется двумя параметрами: частотой и фазой. С этой позиции необходимо определить, какой из этих параметров содержит более существенную информацию о структуре изображения. Основываясь на результатах проведенных экспериментов, можно заключить, что фаза Фурье-преобразования является носителем существенной информации об изображении. В случае отсутствия данных о фазе изображения, будет невозможно определить расположение и особенности изучаемого объекта. Учитывая не уровень яркости, а фазу сигнала, можно избежать зависимости от освещенности. Применяя фазовый метод анализа смещения на изображениях, учитывается как координатная, так и временная составляющие, в результате чего, определяется такие характеристики объекта, как частота и скорость.

Таким образом, определение фазового градиента (например, с помощью квадратурного фильтра) позволит получить гораздо более точную оценку наличия смещения объекта при анализе его изображений.

МЕТОДИКА ОЦЕНКИ ДОСТОВЕРНОСТИ СКРЫТИЯ НАЗЕМНЫХ ОБЪЕКТОВ В ОПТИЧЕСКОМ ДИАПАЗОНЕ ДЛИН ВОЛН

В.В. МИРОНЧИК

При защите информации от наблюдения в оптическом диапазоне необходимо учитывать факторы, влияющие на вероятность обнаружения (распознавания) объектов наблюдения и ухудшающие точность измерения видовых демаскирующих признаков. Эффективность поиска объектов наблюдения зависит от: яркости объекта; контраста объект-фон; угловых размеров объекта; угловых размеров поля обзора; времени наблюдения объекта; скорости движения объекта.

Контрастность объекта с окружающим фоном является необходимым условием выделения демаскирующих признаков объекта и его распознавания.

Для оценки достоверности скрытия наземных объектов в оптическом диапазоне длин волн была разработана следующая методика, которая состоит из следующих этапов:

1. Измерения на гониометрической установке, которые включают в себя калибровку гониометрической установки с помощью молочного стекла МС-20 и измерения характеристик образцов, предназначенных для маскировки объектов.

2. Получение спектральной плотности энергетической яркости

3. Вычисление спектрального коэффициента яркости

4. Расчёт значения контраста по коэффициенту спектральной яркости K_R

5. Оценка достоверности скрытия объектов, которая заключается в анализе значения контраста по коэффициенту яркости объект-фон.

Для достоверного скрытия объекта необходимо, чтобы контраст по коэффициенту яркости объект–фон не превышал 0,2, тогда объект и фон мало отличаются по яркости.

МОДЕРНИЗАЦИЯ СВЧ-ИЗВЕЩАТЕЛЕЙ ДЛЯ ОДНОВРЕМЕННОГО ОБНАРУЖЕНИЯ НАЗЕМНОЙ И ПОДЗЕМНОЙ АКТИВНОСТИ

Е.А. МИХНО, И.Н. ЦЫРЕЛЬЧУК

Радиоволновые извещатели систем периметральной охраны на основе СВЧ-датчиков представляют собой охранные устройства, в работе которых используется сверхвысокочастотное излучение. Использование энергии СВЧ в системах периметральной охраны делает теоретически возможным одним устройством контролировать сразу две уязвимые зоны: наземную и подземную.

Частое комбинирование систем охраны с использованием СВЧ-датчиков и вибрационно-сейсмических устройств даёт предпосылки для модернизации разработок на основе сверхвысокочастотного излучения для одновременного решения двух задач. Специфические свойства СВЧ-излучения [1] и использование его в датчиках движения даёт основания полагать, что при их модификации возможно обнаружение активности в некоторой неглубокой подземной области, достаточной для обнаружения подкопа, то есть нести в себе некоторые функции радиолокационных устройств подповерхностного зондирования.

Глубина расположения вычисляется при известных ширине спектра сигнала и частоте модуляции — определяется частота биения [2], что можно использовать для более конкретного определения координат проникающего объекта. Одним из главных недостатков извещателей на основе зондирующего СВЧ-излучения предполагается малая зона покрытия, что потребует установления большого количества датчиков.

Более детальное изучение развития СВЧ-извещателей для обнаружения подземной активности должно показать достоинства и недостатки описанного комбинирования, а также экономическую обоснованность производства систем такого типа. В докладе рассмотрены достоинства и недостатки, которые предполагаются при создании и эксплуатации СВЧ-датчиков на основе зондирующего излучения для одновременной охраны периметра и подземной области, предложены оптимальные варианты исполнения извещателей на основе существующих моделей.

Литература

1. Кураев А.А., Байбурин В.Б., Ильин Е.М. Математическое моделирование и методы оптимального проектирования СВЧ приборов. Минск, 1990.

2. Финкельштейн М.И. и др. Подповерхностная радиолокация. М., 1994.

ВОПРОСЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

О.К. БАРАНОВСКИЙ

Нормальная эксплуатация объектов информатизации, обеспечивающих функционирование опасных или социально значимых производств, а также реализующих значимые для государства и общества функции (объекты критической инфраструктуры — ОКИ), поддерживается с применением систем безопасности. Системы безопасности ОКИ обязательно включают меры по физической защите. В свою очередь системы физической защиты (СФЗ) предусматривают применение технических мер и средств защиты информации, обеспечивающих конфиденциальность информации о составе и функционировании СФЗ, целостность и доступность технологической информации, нарушение которых может привести к снижению эффективности функционирования (выводу из строя) системы физической защиты (ее отдельных элементов).

Безопасное управление средствами или системами физической защиты включает:

– защиту от несанкционированного доступа к оборудованию и информации в соответствии с требованиями нормативных документов по защите информации;

– хранение и выдачу информации о функционировании системы физической защиты (в том числе документирование всех действий оператора), попытках ее преодоления и несанкционированных действиях;

– тестирование и контроль наличия неисправностей оборудования без нарушения его работоспособности (отдельных элементов);

– дублирование и резервирование оборудования.

Учет требований и реализация мер технической защиты информации и оборудования СФЗ на стадиях ее проектирования и разработки позволяет существенно снизить риски безопасности ОКИ при их эксплуатации.

СПЕКТРАЛЬНЫЕ ЗАВИСИМОСТИ СТЕПЕНИ ЛИНЕЙНОЙ ПОЛЯРИЗАЦИИ ОБЪЕКТОВ С СЕТОЧНЫМ ПОКРЫТИЕМ ПРИ РАЗЛИЧНЫХ ФАЗОВЫХ УГЛАХ

ДЖАМАЛЬ СААД ОМЕР, И.М. ЦИКМАН, Ю.В. БЕЛЯЕВ

Дальнейшее развитие современных средств и методов оптической диагностики требует определения параметров оптического поля объекта и окружающего его фона в широкой (видимой и инфракрасной) области спектра. Такими важнейшими параметрами, наряду со спектрально-энергетическими характеристиками, являются спектральные зависимости степени линейной поляризации отраженного солнечного излучения. В изменяющихся условиях наружного наблюдения большое значение имеют угловые зависимости перечисленных параметров излучения, их значения для разных фазовых углов (углов между потоком падающего солнечного излучения и направлением визирования).

При снижении заметности скрываемых объектов в видимой области спектра широко применяются различные маскировочные сетки. Однако влияние сеток на поляризационные характеристики отраженного излучения и их спектрально-угловые зависимости слабо изучены. В данной работе исследовалось влияние сеток различного состава с различным шагом ячейки на угловые характеристики поляризационных параметров оптического поля некоторых материалов. Измерения

проводились на гониометрической установке с помощью спектрорадиометра ПСР-02, оснащенного поляризационной насадкой. Спектральная зависимость степени линейной поляризации образцов для разных фазовых углов получена в диапазоне 0,38–2,3 мкм.

Анализ полученных зависимостей для образцов показал, что экранирующие свойства и снижение степени линейной поляризации значительнее у сеток с меньшим размером ячейки и возрастает с увеличением угла наблюдения. Сетки, изготовленные из одинакового материала, но имеющие различную окраску отличаются по спектрально-поляризационной зависимости. Полосы поглощения красителя, по-видимому, вносят свой вклад в различие хода спектральной зависимости степени линейной поляризации.

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ФИНАНСОВОЙ ОТЧЕТНОСТИ: ТРЕБОВАНИЯ К РАСКРЫТИЮ ИНФОРМАЦИИ

Е.С. РОМАНОВА, В.В. САВОЩИК

4 мая 1998 г. постановлением Совета Министров Республики Беларусь № 694 была принята Государственная программа перехода на международные стандарты бухгалтерского учета, регламентирующая переход всех хозяйствующих субъектов на МСФО в Республике Беларусь к 1 января 2008 г. Сегодня, как и 15 лет назад, говорить о фактическом применении международных стандартов белорусскими предприятиями, все еще не приходится. Основная причина этого — существенные различия между белорусской системой бухгалтерского учета и МСФО, в числе которых и требования к раскрытию информации, содержащейся в финансовой отчетности.

Бухгалтерская отчетность белорусских организаций в соответствии с Законом Республики Беларусь "О бухгалтерском учете и отчетности" должна обеспечивать достоверное и полное представление только об имущественном и финансовом положении организации, о финансовых результатах ее деятельности.

Отчетность по МСФО более публична и информативна. В ней должен быть раскрыт значительно больший объем информации о деятельности организации. Причем таким образом, чтобы заострить внимание пользователей на всех деталях ее работы. Такая детализация, по мнению белорусских бухгалтеров, неоправданна, не соответствует требованиям конфиденциальности и, соответственно, повышает предпринимательский риск. Преодоление противоречия между прозрачностью и конфиденциальностью возможно только в случае осознания выгодности прозрачной отчетности, в первую очередь, самими ее составителями. Финансовая отчетность МСФО позволяет более подробно оценить структуру риск-менеджмента, проанализировать количественные и качественные параметры рисков, которым подвержен хозяйственный субъект. В итоге грамотный пользователь (и, в первую очередь, управляющий или инвестор) может увидеть не только каким будет финансовый результат или капитал компании сейчас, но и оценить перспективы его развития. А снижение неопределенности, как известно, уменьшает любой риск.

РОБОТИЗАЦИЯ СРЕДСТВ УПРАВЛЕНИЯ СЛОЖНЫХ ВОЕННО-ТЕХНИЧЕСКИХ СИСТЕМ В КОНТЕКСТЕ ЗАЩИТЫ ИНФОРМАЦИИ

И.Г. ДЕНИСЕНКО, А.А. ОЛЬХОВИК

Изменилось содержание современной информационной и вооруженной борьбы в воздушно-космической и наземной сфере, что требует пересмотра принципов построения перспективных систем вооружения и систем управления ими в целях повышения их эффективности, устойчивости и быстродействия. Актуальным направлением совершенствования сложных военно-технических систем представляется роботизация элементов её системы управления на основе разработки, производства и внедрения специальных робототехнических устройств (ситуаторов управления) предназначенных для автоматического решения сложных ситуационных задач, требующих мгновенного принятия решений, доведения их до исполнителей и последующей реализации. Система управления — совокупность функционально взаимосвязанных органов управления, пунктов управления, средств связи, АСУ и роботов интеллектуальной поддержки — ситуаторов. Ситуатор — робот-управленец, (программа) предназначен для повышения информационно-психологической устойчивости управленческого персонала за счет возможной интеллектуальной поддержки принимаемых решений, автоматического выбора наиболее целесообразного решения в условиях крайне ограниченного располагаемого времени, автоматической постановки боевых и других задач подчиненным системам и подразделениям. Ситуаторы должны быть в каждом управляемом и обеспечивающем подразделении и мгновенно использоваться при пропадании связи с вышестоящим пунктом управления, пунктами управления взаимодействующих и обеспечивающих сил и средств, появлении информации о внезапном вооруженном нападении, хакерской атаке, изменении других элементов оперативно-тактической и тактической воздушно-космической и наземной обстановки, требующих реакции системы управления.

СИСТЕМА ОБНАРУЖЕНИЯ ВОЗДУШНОГО ВТОРЖЕНИЯ НА БАЗЕ ЭЛЕКТРОСТАТИЧЕСКИХ ДАТЧИКОВ

А.Ф. МЕЛЕЦ, Д.С. НЕФЕДОВ

Защита важных объектов хозяйственной деятельности, таких как АЭС, ГЭС, ТЭЦ, заводы и др., от возможных действий диверсионных групп или террористических банд-формирований не возможна без применения современных технических средств охраны. Если раньше такие средства обеспечивали обнаружение и определение местоположения наземных нарушителей, то теперь с появлением малоразмерной беспилотной авиации, совершенствованием вертолетной техники, актуальной стала задача обнаружения угроз воздушного вторжения [1]. Особенностями тактико-технических характеристик летательных аппаратов (ЛА), используемых для осуществления воздушного вторжения, являются малые размеры и предельно-малые высоты полета от 2–10 до 200 м.

Наиболее эффективное обнаружение таких ЛА обеспечивают многодатчиковые системы пассивной локации на базе разведывательно-сигнализационных приборов (датчиков). Основными преимуществами пассивных систем является высокая скрытность, малые габариты и вес, низкая стоимость, простота размещения на местности.

В докладе представлен анализ современных датчиков обнаружения маловысотных ЛА, построенных на различных физических принципах, на основании которого обоснована перспективность применения электростатических датчиков для создания системы обнаружения воздушного вторжения. Излагаются основные результаты теоретических и экспериментальных работ в области создания электростатической многодатчиковой системы обнаружения маловысотных ЛА, проведенных авторами в последнее время.

Литература

1. Щербаков Г.Н., Шлыков Ю.А. // Специальная техника. 2008. № 1. С. 17–22.

ДЕТЕКТОР ДЛЯ СИСТЕМ ДОЗИМЕТРИЧЕСКОГО КОНТРОЛЯ НА РАДИАЦИОННО-ОПАСНЫХ ОБЪЕКТАХ

Н.И. МУХУРОВ, ЯСИН МОХСИН ВАХИОХ, А.М. ПРУДНИК

Для контроля радиационной обстановки в охранных и санитарно-защитных зонах создаваемых вокруг искусственных источников радиоактивных излучений (атомных станций, предприятий атомной промышленности, научно-исследовательских институтов и др.), а также для контроля уровня гамма-излучений, обнаружения радиоактивных материалов и контроля транспортных средств, осуществляющих перевозку радиоактивных веществ, предлагается применение детектора ионизирующего излучения.

Решение задачи повышения чувствительности, стабильности и расширение рабочего диапазона детектора при минимальных массогабаритных характеристиках достигается следующим образом. Детектор, содержащий подложку с фотолюминесцирующим под действием ионизирующего излучения веществом и фотоприемник, подложка выполняется из анодного оксида алюминия (прозрачного в оптическом диапазоне), содержит периодическую систему отверстий, перпендикулярных обеим поверхностям подложки и заполненных композитом из наноструктурированных соединений, чувствительным к ионизирующим излучениям в широком диапазоне энергий, причем диаметр отверстий больше диаметра частиц соединений в 3 и более раз.

Предложенный способ обеспечивает повышение чувствительности, стабильности и расширение рабочего диапазона за счет увеличения объема композита из частиц фотолюминесцирующих соединений, чувствительных к ионизирующим излучениям в широком диапазоне энергий, определяемых их наноструктурированием, толщиной диэлектрической подложки и площадью периодической системы микроотверстий в ней, применением высокотемпературной алюмооксидной керамики, незначительно изменяющей свои характеристики при высоких уровнях ионизирующего излучения и температур окружающей среды.

СЕКЦИЯ 6. ПОДГОТОВКА КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОСОБЕННОСТИ ОБУЧЕНИЯ СТУДЕНТОВ НА АНГЛИЙСКОМ ЯЗЫКЕ

А.А. БУДЬКО

Обучение студентов и магистрантов на английском языке в Белорусском государственном университете информатики и радиоэлектроники осуществляется уже три года и за это время накопился некоторый опыт работы с таким контингентом студентов. Используя это, а также учитывая опыт предыдущий аналогичной работы, в докладе предлагается обсудить следующие особенности:

– английский язык студентов обучающихся в англоязычных группах, не является родным. Это накладывает серьезные ограничения на восприятие в первую очередь речевой информации.

– английский язык не является родным также для преподавателей, работающих в англоязычных группах. Но, если преподаватели владеют английским (американским) языком, то английский язык студентов в большинстве случаев другой, а уровень владения языком у разных студентов может сильно отличаться.

– рассмотренные обстоятельства необходимо учитывать при проведении занятий в таких группах, а также при подготовке раздаточных материалов (конспекты лекций, лабораторные практикумы, индивидуальных заданий и заданий на курсовое проектирование).

– при сложившихся особенностях работы в англоязычных группах в докладе предлагается обсудить внедрение элементов рейтинговой системы обучения для повышения эффективности учебного процесса.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНЫХ ОБЪЕКТОВ И СИСТЕМ ПО ДИСЦИПЛИНЕ «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОЕКТИРОВАНИЯ ЭЛЕКТРОННЫХ СИСТЕМ БЕЗОПАСНОСТИ»

С.М. БОРОВИКОВ, Е.Н. ШНЕЙДЕРОВ, А.И. БЕРЕСНЕВИЧ,
И.Н. ЦЫРЕЛЬЧУК, В.Е. МАТЮШКОВ

С сентября 2011 г. в Белорусском государственном университете информатики и радиоэлектроники открыта подготовка по новой специальности «Электронные системы безопасности». Специальная подготовка по этой специальности начинается с учебной дисциплины «Теоретические основы проектирования электронных систем безопасности» (ТОПЭСБ).

Цель дисциплины — формирование теоретических знаний и практических умений, необходимых для проектирования и оценки эффективности функционирования электронных систем безопасности (ЭСБ) объектов: предприятий, организаций, персонала, транспорта, физических лиц.

Разработка по дисциплине «ТОПЭСБ» компьютерных лабораторных работ (лабораторного комплекса) с использованием виртуальных объектов и виртуальных компонентов ЭСБ является актуальной. Эффект от внедрения разрабатываемого лабораторного комплекса обусловлен следующим:

1) экономией финансовых средств в виду того, что отпадает необходимость в покупке дорогостоящих компонентов реальных электронных систем безопасности, в частности датчиков и исполнительных устройств большой номенклатуры;

2) отсутствием необходимости технологической подготовки, предшествующей выполнению лабораторных работ, а также текущего и, как правило, дорогостоящего ремонта лабораторного оборудования (технические средства являются виртуальными, кроме самих компьютеров);

3) глубоким осмысливанием основных положений учебной дисциплины, так как компьютерная реализация ЭСБ позволяет быстро «проиграть» большое число вариантов системы и выбрать лучший из них.

Перед написанием компьютерных программ к лабораторным работам были разработаны сценарии, включающие этапы по созданию виртуальных объектов и виртуальных составных частей ЭСБ. Также были определены конкретные действия студента при выполнении ими лабораторных работ.

Разработанный практикум включает шесть компьютерных лабораторных работ. При написании программ к лабораторным работам использовалась среда программирования Delphi.

СЦЕНАРИЙ КОМПЬЮТЕРНЫХ ЛАБОРАТОРНЫХ РАБОТ ПО ИССЛЕДОВАНИЮ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭЛЕКТРОННЫХ СИСТЕМ БЕЗОПАСНОСТИ

С.М. БОРОВИКОВ, Е.Н. ШНЕЙДЕРОВ, А.И. БЕРЕСНЕВИЧ,
Н.А. ЖАГОРА, А.А. БРУЙ

Специальная подготовка по новой специальности «Электронные системы безопасности» начинается с учебной дисциплины «Теоретические основы проектирования электронных систем безопасности» (ТОПЭСБ), которая может рассматриваться как теоретическая база подготовки инженера. Разработка по дисциплине «ТОПЭСБ» компьютерных лабораторных работ (лабораторного комплекса) с использованием виртуальных объектов и виртуальных компонентов ЭСБ является актуальной. Использование в подготовке студентов таких работ сэкономит финансовые средства, прежде всего в виду того, что отпадает необходимость в покупке дорогостоящих компонентов реальных электронных систем безопасности, в частности датчиков и исполнительных устройств большой номенклатуры.

Сценарии к «виртуальным лабораторным работам», предлагаемые для программной реализации на компьютерах, включали следующее:

формулировку цели лабораторной работы;

характеристику объекта и защищаемых ресурсов (денежные, информационные, материальные ценности, персонал и т.п.);

функциональное назначение ЭСБ и режимы её работы;

количественный критерий, используемый для оценки качества функционирования электронной системы безопасности;

задание студентам для проведения экспериментальной части работы;

действия студента в процессе выполнения лабораторной работы.

При решении поставленной задачи студенту понадобиться обращаться к справочным данным технических средств ЭСБ. для этого было предусмотрено создание специальных баз данных о датчиках и исполнительных устройствах.

Разработчики компьютерных лабораторных работ по учебной дисциплине «Теоретические основы проектирования ЭСБ» будут признательны специалистам

за критические замечания по уточнению сценариев и советы по программной реализации лабораторных работ (bsm@bsuir.by).

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕ НАДЁЖНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

В.А. ГАНЖА, О.И. ЧИЧКО

В докладе представлены соображения, мысли и примеры методики обучения защите информации как в информационных системах в общем, так и в компьютерных сетях в частности. Эти материалы апробированы авторами на протяжении ряда лет преподавания в различных вузах и перед различными слушательскими аудиториями.

В силу большой насыщенности литературой как русскоязычной, так и на английском языке по информационной безопасности и по криптографии, построение лекционной части курса, обычно, затруднений не вызывает.

Акцентируется внимание на проведении практических и лабораторных занятий. Рассматривается работа обучаемых с простейшими пакетами и утилитами, создающими хэш-функции по алгоритмам MD5, SHA1. Иллюстрируются возможности простейших пакетов стеганографии.

На занятиях проводится простейший криптоанализ со студентами, на примере взлома запароленых архивов в зависимости от длины ключа и его состава (только цифры, только буквы, и буквы и цифры). Разбираются некоторые аспекты использования пакетов PGP (платформа Microsoft Windows) и GPG (платформа Linux) для практической работы с обучаемыми.

Генерация пары ключей (публичного и приватного) для осуществления и иллюстрации метода асимметричного шифрования. Организация тренинга обучаемых по рассылке и получению электронной почты с использованием приватных и публичных ключей. Методы аутентификации сообщений, создание цифровой подписи в пакете PGP и верификация этой подписи.

Курирование и руководство самостоятельного задания обучаемых по проекту построения небольшой локальной компьютерной сети с привязкой отдельных компонентов оборудования к 7-уровневой модели OSI и реализация функций информационной безопасности конкретными уровнями этой модели.

МОБИЛЬНАЯ СИСТЕМА ЭКСПРЕСС-ОПРОСА СТУДЕНТОВ

А.А. ДЕРЮШЕВ

При преподавании студентам технических предметов большое значение имеет постоянный контроль знаний студентов. Повышение качества данного контроля и его оперативности невозможно без использования вычислительной техники, однако при увеличении числа контролируемых студентов до 100-150 (экспресс-опрос на лекции) человек делает невозможным использование персональных компьютеров. Можно использовать системы электронного голосования типа Hitachi Verdict, состоящие из базового модуля, подключаемого к компьютеру, и персональных пультов студентов. Однако данные системы, как правило, ограничиваются небольшим числом персональных пультов (16-32), а также требуют существенных затрат на свое приобретение.

В то же время, практически каждый студент имеет в своем распоряжении как минимум один сотовый телефон. Технический уровень этих телефонов различен, однако все позволяют отправлять SMS, что и послужило отправным пунктом для разработки системы.

Созданная система состоит из двух модулей. Первый модуль включает сотовый телефон преподавателя с ОС Android и разработанной программой, содержащей базу данных. Второй модуль выполнен в виде сайта и предназначен для организации удобного доступа студентов к результатам опроса. Работа системы начинается с заполнения таблицы сведений о студентах, для чего каждый из них должен прислать SMS, содержащее специальный символ, ФИО и номер группы. В таблице предусмотрены поля для трех различных телефонов для каждого студента. Заполнение таблицы происходит в автоматическом режиме; при необходимости она может быть подкорректирована вручную. Другая таблица содержит набор возможных вариантов ответов на каждый вопрос и баллы за каждый вариант ответа для данного теста. Процесс опроса заключается в демонстрации студентам мультимедиа слайдов с вопросами и вариантами ответов. Каждый вопрос предполагает возможность нескольких ответов, которые разделяются запятой. После ответа на один вопрос, студент ставит точку с запятой и отвечает на следующий. После ответа на все вопросы SMS отправляется на номер преподавателя, после чего производится его разбор с подсчетом набранных баллов. Затем информация из телефона передается в серверную базу данных.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО НАПРАВЛЕНИЮ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ

В.В. МАЛИКОВ

Для повышения эффективности самостоятельного получения новых знаний в режиме 24*7*365, предлагается построение процесса обучения на основе адаптированного алгоритма широковещания источник-получатель: multicast.

Основные этапы для эффективной адаптации алгоритма multicast к процессу обучения:

– путем проведения/участия в разноплановых on-line/off-line семинарах/конференциях, проработке типовых групп/профилей социальных сетей, форумах сформированных сообществ, выделить среди всего профессионального сообщества наиболее мотивированную его часть по определенным критериям: профессионализм, инициативность, стремление к постоянному профессиональному развитию;

– в рамках выделенного подмножества сообщества сформировать инициативную группу из представителей: регуляторов отрасти, академического образования, производителей/интеграторов современных информационных систем;

– детально изучить конкретные потребности регуляторов отрасти, академического образования, производителей/интеграторов современных информационных систем, а также других членов профессионального сообщества;

– создать единый специализированный on-line ресурс доступа к актуальной информации по современным информационным технологиям;

– анонсировать и проводить тематические off-line семинары/конференции с участием компетентных специалистов регуляторов отрасти, академического образования, производителей/интеграторов современных информационных систем, а также лидеров профессионального сообщества;

– сформировать и провести оперативное издание расширенных бумажных вестников/журналов/каталогов по результатам проведенных мероприятий и их адресную доставку представителям профессиональной отрасли, включая регуляторов отрасли;

– обеспечить конверсию посетителей off-line семинаров/конференций, на единый on-line ресурс путем размещения уникального контента по результатам проведенных мероприятий;

– обеспечить репутацию единого on-line ресурса путем проведения вебинаров, оперативного представления уникальной профессиональной информации, оперативных ответов на вопросы пользователей со стороны экспертов;

– обеспечить «вирусную» масштабируемость репутации единого on-line ресурса через социальные сети и СМИ, включая ведомственные;

– построить уникальные адресные образовательные off-line программы повышения квалификации в рамках дополнительного образования взрослых с обязательным предварительным анкетированием потребностей и последующей обратной связью от целевых потребителей образовательной услуги;

- проводить оперативный мониторинг, сбор и анализ потребностей профессионального сообщества через форумы/опросы/статистику с передачей итоговых тенденций по качеству услуг, недостатков НПА (ТНПА) регуляторам отрасли для дальнейшего реагирования.

Практическая реализация, верификация и адаптация представленного выше подхода была проведена в 2011-2012 гг. совместно с Департаментом охраны МВД, журналом «Технологии безопасности», БГУИР и другими организациями в рамках научно-практических семинаров: «Комплексная безопасность банков», «Центры обработки данных», «Безопасный город», «Видеоаналитика в системах защиты объектов различных категорий» и научно-практической конференции «Безопасность многофункциональных и спортивных объектов с массовым пребыванием людей».

РОЛЬ ЧЕЛОВЕКА В СИСТЕМЕ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ АЭС

Э.П. КРЮКОВА

При обеспечении безопасности компьютерных систем АЭС необходимо особо учитывать роль человека в использовании их уязвимостей, возможностей реализации угроз, а также ошибок.

Исследования в области живучести систем управления реакторными установками АЭС уделяют основное внимание разработке программного обеспечения для компьютерных систем, важных для безопасности: обнаружение вторжения, предотвращение вторжения, более строгие системы аутентификации, более стойкие методам шифрования и др., но недостаточно исследований посвящено человеку. Исследования и отчеты идентифицировали человеческую ошибку как причину номер один нарушений правил безопасности. Оценки их влияния, связанного с нарушением правил безопасности, составляют 63–80%.

Как только произошел отказ и началось восстановление компьютерной системы, ошибка человека может сыграть разрушительную роль при восстановлении данных. Отмечается, что 30% всех потерь данных — результат человеческой ошибки и только 15% — от злоумышленного воздействия (вирусное повреждение — 6% плюс кража с использованием компьютера — 9%). Эти ошибки могут быть активными, происходящими в ходе процесса восстановления, или скрытыми, которые следуют из предыдущего процесса архивирования или резервирования.

При анализе угроз следует также учитывать и положительное влияние действий человека при обеспечении защиты компьютерных систем АЭС. Будучи самым слабым звеном компьютерной системы, оператор или служащий может стать преградой, предотвращающей отказ системы или ее компрометацию.

В связи с этим возрастает задача повышения культуры безопасности, которая характеризует квалификационную и психологическую подготовленность работников (персонала), при которой обеспечение безопасности является приоритетной целью и внутренней потребностью каждого, приводящей к осознанию личной ответственности и к самоконтролю в процессе всех работ, влияющих на безопасность.

Система управления безопасностью на предприятии (в организации) должна использоваться для поддержки высокой культуры безопасности, для чего необходимо:

– обеспечить общее понимание ключевых аспектов культуры безопасности в пределах предприятия (организации);

– обеспечить ресурсы для поддержки отдельных членов персонала и групп в выполнении ими задач безопасно и успешно, принимая во внимание взаимодействие между отдельными лицами, технологией и организацией;

– усилить изучение и исследование отношения к проблеме безопасности на всех уровнях организации;

– обеспечить средства для непрерывного развития и повышения культуры своей безопасности.

Знания особенностей персонала и принципов обеспечения надежности человека должны использоваться для повышения качества разработки курсов обучения безопасности и осведомленности и гарантировать восстановление систем с наименьшим ущербом, имущественным и человеческой жизни.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ ПО ОСНОВАМ УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ С УКЛОНОМ В ПРАКТИКУ ЗАЩИТЫ ИНФОРМАЦИИ

Д.Н. МАРУДА, В.Л. НИКОЛАЕНКО, Г.В. СЕЧКО

Подготовка, переподготовка и повышение квалификации кадров в области защиты информации включает изучение курса «Основы управления интеллектуальной собственностью» (ОУИС) в виде отдельной дисциплины или в виде совмещения её с курсом защиты информации «Основы защиты информации и управления интеллектуальной собственностью (ОЗИиУИС)» [1]. При этом, если теоретическая часть курсов ОУИС и ОЗИиУИС представлена в литературе достаточно полно [2, 3], то поиск соответствующего материала для проведения практических занятий (ПЗ), интересного не только для обучающих, но и для обучаемых, — это довольно сложная задача. Поэтому студенты и курсанты большинства учреждений образования республики на ПЗ, посвящённых составлению и оформлению заявок на объекты промышленной собственности (ОПС), выполняют одну и ту же простейшую процедуру: примерно 80 % учебного времени изучают методическое пособие, и затем в течение примерно 10 % учебного времени (в среднем 9 мин) заполняют бланк заявки по установленной форме. Вариантов выполнения задания нет. Виды предлагаемых для включения в заявку ОПС чаще всего не совпадают с тематикой специальности, которую получают обучаемые.

Для устранения данного недостатка в [1, 4] предложено составлять на ПЗ формулу изобретения и реферат ОПС для включения в заявку. Сделанные предшественниками наработки в области составления заявки на ОПС учтены

следующим образом: для составленной студентом однозвенной формулы изобретения ему предлагается заполнить бланк заявки, подписанный заявителем, а затем для предварительно составленной им же многозвенной формулы — бланк, подписанный патентным поверенным. В докладе рассматривается практическая реализация сделанного предложения в виде готового описания ПЗ. в описании предлагается 34 варианта исходных данных для составления сначала однозвенной, затем многозвенной формулы изобретения и реферата на ОПС в области защиты информации и информационной безопасности в телекоммуникациях. Описание прошло практическую апробацию в осеннем семестре 2011 года. Готовятся аналогичные исходные данные для других специальностей и специализаций.

Литература

1. Гасенкова И.В., Лыньков Л.М., Мухуров Н.И., Сечко Г.В. // Закон и порядок: Материалы I Межд. науч.-практ. конф. (31 января 2011 года): Сборник научных трудов. М.: Спутник+, 2011. С. 107-110.
2. Лыньков Л.М., Мухуров Н.И. Лекции по курсу «Основы управления интеллектуальной собственностью» для специальностей 45 01 03 «Сети телекоммуникаций», 98 01 02 «Защита информации в телекоммуникациях». Минск: БГУИР, 2008. 173 с.
3 Герасимова Л.К. Основы управления интеллектуальной собственностью: учеб. пособие. Минск, 2011. 256 с.
4. Корсаков А.В., Маруда Д.Н., Иванова Т.Н. // Тезисы докладов 48-й научной конференции аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии / под ред. В.Л. Николаенко и Г. В. Сечко. Минск: ИИТ БГУИР, 2012. С. 30.

ОСОБЕННОСТИ ДИСЦИПЛИНЫ «ФУНКЦИОНАЛЬНЫЕ УСТРОЙСТВА И ЭЛЕКТРОПИТАНИЕ СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ» ДЛЯ СПЕЦИАЛЬНОСТИ «ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ»

Н.И. ШАТИЛО

Современные тенденции развития систем электропитания характеризуются, во-первых, возрастающим использованием цифровых способов контроля и управления, и во-вторых, широким внедрением устройств защиты от помех в связи с усложняющейся помеховой ситуацией в сетях электропитания общего пользования.

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 во второй части программы дисциплины предусмотрен специальный раздел, посвященный защите блоков питания от непреднамеренных помех. В этом разделе рассматриваются параметры стандартизованных видов помех: импульсных (микросекундных, наносекундных) и длительных (перепадов сетевого напряжения), помехоустойчивые структурные и схемотехнические решения блоков питания.

Цифровые элементы устройств электропитания особенно чувствительны к внешним импульсным помехам и, в свою очередь, являются источниками таких помех. Поэтому в дисциплине анализируются схемотехнические и конструктивные решения цифровых блоков, обеспечивающие повышенную помехоустойчивость этих блоков и минимальный уровень собственных помех.

ЭНЕРГЕТИЧЕСКИЙ ПАСПОРТ ТИПОВОЙ КВАРТИРЫ

Д.Г. САВИЦКАЯ, В.П. БУРЦЕВА

Создана компьютерная модель типовой квартиры, на основании которой изучен вопрос потребления электрической и тепловой энергии, наиболее часто используемыми бытовыми приборами.

Рассчитано количество потребляемой квартирой энергии за месяц; выявлены пути экономии тепло- и электроэнергии, а также пути удешевления оплаты квартиросъёмщиком коммунальных услуг. В ходе работы определены бытовые приборы, являющиеся основными потребителями тепло- и электроэнергии (анализ проведен на образцах отечественной бытовой техники). Составлен энергетический паспорт типовой квартиры и даны конкретные рекомендации по экономии энергии в рамках одной квартиры.

На основании составленного паспорта выработаны рекомендации по экономии энергоресурсов в масштабах региона и республики.

ДИСЦИПЛИНА «ПОЧТОВАЯ БЕЗОПАСНОСТЬ»: СУЩНОСТЬ И СОДЕРЖАНИЕ

Т.В. ЖИГАДЛО

Информационная безопасность тесно соприкасается с почтовой безопасностью, которой операторы почтовой связи уделяют сегодня существенное внимание. Такое взаимодействие обусловлено наличием значительного объема информации, передаваемой при помощи электронных средств связи, и услуг, которые невозможны без применения информационных технологий.

При подготовке специалистов для отрасли «почтовая связь» (техников и инженеров), вопросам почтовой безопасности уделяется особое внимание. Наряду со специальными дисциплинами «Информационные технологии в почтовой связи», «Компьютерные сети», где также есть разделы, посвященные информационной безопасности, дисциплина «Почтовая безопасность» отражает специфику будущей профессиональной деятельности. Данный курс включает в себя следующие разделы:

– нормативно-правовое обеспечение почтовой безопасности;
– сохранность ценностей и имущества объектов почтовой связи;
– сохранность почтовых отправлений;
– информационная безопасность.

Причем заключительная часть учебного курса предусматривает изучение общих принципов информационно-технологической безопасности, безопасной эксплуатации программного обеспечения (в том числе и специальных программ, используемых на предприятии почтовой связи), а также использование информационных технологий для контроля производственной деятельности персонала, занятого на объектах почтовой связи.

Данный курс способствует систематизации знаний учащихся и студентов по вопросам почтовой безопасности и повышению качества образовательных услуг.

ВЛИЯНИЕ СЕТИ ИНТЕРНЕТ НА ИДЕНТИФИКАЦИЮ ЛИЧНОСТИ

Е.А. КУХАРЕНКО

Социокультурная деятельность современного человека в значительной степени определяется влиянием процесса всемирной экономической, политической и культурной интеграции и унификации, т.е. глобализации. В частности общества, открытые для глобализационных веяний, подвергаются влиянию через практики потребления. Консьюмеризм во многом стал следствием социальных макроизменений, сказавшихся на распределении пространства и времени социальной жизни в контексте индивидуального самоосуществления и самоидентификации в системе социокультурных, политических, экономических отношений.

Таким образом, ключевым вопросом исследования является изучение влияния интернет пространства на формирование социальной идентификации личности (размывание и изменение идентичности под влиянием Интернет пространства).

Очевидно, что массированная виртуализация повседневности внесла свой вклад в картину повседневной жизни. Беларусь попала в двадцатку стран, где наиболее активно растет количество интернет-пользователей.

Современный человек формируется как личность в медианасыщенной среде, где любые социальные отношения связаны с интенсивным информационным обменом. Психический ресурс человека вступает в конфликт с информационной средой, поскольку доступность информации не коррелируется с физическими ограничениями психики по возможностям ее обработки.

Таким образом, в условиях разнонаправленных потоков и неопределённости социальных перспектив актуальным востребованным ресурсом становится информация в переработанном и адаптированном виде. Можно констатировать, что интернет ресурсы становятся идеальным инструментом формирования мировоззрения, готовой социальной идентичности. Они обладают мощнейшими возможностями консолидации пользователей на основе как позитивной, так и негативной идеи, которая усваивается с минимальными усилиями.

Замечено, что долговременное пользование интернет меняет (формирует) личность человека и его восприятие мира. Множественность и изменчивость идентичности в виртуальной коммуникации отражает множественность и размытость идентичности в современном обществе в целом.

Подводя итог, можно сказать:

– интернет образует особую коммуникативную среду, которая не имеет исторических аналогов;

– вербальное общение становится системообразующим признаком социальной реальности;

– поиск идентичности, коллективной или индивидуальной, приписанной или сконструированной, становится фундаментальным источником социальных значений;

– феномен идентичности образуется в непосредственной связи с коммуникацией.

КРЕАТИВНОЕ МЫШЛЕНИЕ КАК НЕОТЪЕМЛЕМЫЙ НАВЫК СОВРЕМЕННОГО СПЕЦИАЛИСТА

Е.А. КУХАРЕНКО

Сегодня специалисты в Республике Беларусь осуществляют свою деятельность в динамике многофакторных изменений социально-экономической системы. Развитие рыночной экономики, модернизация производства, появление новых наукоемких технологий приводит к изменению профессионально-квалификационной структуры спроса на рынке труда и к повышению требований работодателей к качеству персонала. Одним из ключевых вопросов менеджмента персонала для эффективного решения проблемных ситуаций является приобретение специалистами навыков креативного (творческого) мышления. Базовое образование сегодняшних специалистов, как правило, готовит их к решению типовых задач. Следствием этого является низкая интеллектуальная мобильность и отсутствие навыков, оперативно ориентироваться в динамически трансформирующейся профессиональной среде. Актуальные для сегодняшнего дня оценки возможностей персонала описываются психологическими теориями поведения, теорией мотивации и стимулов.

К решению выявленной проблемы можно подойти также, выстраивая систему менеджмента персонала в проблемном поле развития креативности. Еще в середине XX века считалось, что вопрос креативности — это вопрос дара, но не навыка. Постепенно (социальная психология, психологические теории) взгляд на креативность изменяется. Анжи Гаральски предлагает рассматривать креативность как ремесло. «Ремесло: 1) мелкое, преимущественно ручное производство товаров, требующее значительного мастерства; 2) владение искусством изготовления определенных видов вещей, наличие соответствующей профессии». (Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б.. Современный экономический словарь. М., 1999). Предлагается попытка выявления порядка действий при организации креативного подхода в решении примерной заданной проблемы. Рассмотрение креативности «в ключе ремесленничества» позволит обозначить этапы развития навыка креативного мышления следующим образом: 1) постановка задачи; 2) конкретизация цели; 3) подготовка и утверждение плана действий; 4) изучение существующей ситуации; 5) нахождение, оценка и конкретизация пути решения проблемы; 6) реализация решения; 7) исследование результатов реализации. Оптимально решить задачу обучения креативному мышлению можно, применяя современный метод активного обучения, направленный на развитие знаний, умений и навыков, а именно тренинг

Предполагается, что знание порядка действий для выстраивания креативного подхода — лишь первый этап на пути освоения креативности как навыка. Необходимы тренировки навыка и его закрепление, что убеждает нас: креативность — это инструмент, работу с которым может освоить любой заинтересованный человек и профессионал. Развитие креативного мышления как основы менеджмента персонала – это потенциал для конструирования текущих производственных ситуаций, разработки работающих моделей для повышения эффективности труда и качества современного наукоемкого производства.

НАУЧНОЕ ИЗДАНИЕ

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

ТЕЗИСЫ ДОКЛАДОВ X БЕЛОРУССКО-РОССИЙСКОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ

29–30 МАЯ 2012 Г., МИНСК

ОТВЕТСТВЕННЫЙ ЗА ВЫПУСК Л.М. ЛЫНЬКОВ
КОМПЬЮТЕРНЫЙ ДИЗАЙН И ВЁРСТКА А.М. ПРУДНИК

Подписано в печать 25.05.2012. Формат 60×84 ⅛. Бумага офсетная.
Гарнитура "Century Schoolbook". Отпечатано на ризографе. Усл. печ. л. 11,86.
Уч. изд. л. 10,1. Тираж 100 экз. Заказ 246.

Издатель и полиграфическое исполнение: учреждение образования
"Белорусский государственный университет информатики и радиоэлектроники"
Лицензия ЛИ № 02330/0494371 от 16.03.2009. Лицензия ЛП № 02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6.