ISSN 1729-7648

ДОКЛАДЫ

Белорусского Государственного Университета Информатики и Радиоэлектроники

№ 5 17 мая 2005 г.

ЭЛЕКТРОНИКА, МАТЕРИАЛЫ

ТЕХНОЛОГИИ, ИНФОРМАТИКА

ЭКОНОМИКА И УПРАВЛЕНИЕ

III Белорусско-российская научно-техническая конференция

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Минск-Нарочь 23-27 мая 2005 года

ДОКЛАДЫ

БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Выходит четыре номера в год

Научный журнал основан в 2002 году

АДРЕС РЕДАКЦИИ:

220013, Минск, ул. П. Бровки, 6, к. 327, тел. 239-84-89

doklady@bsuir.by

Учредитель: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Редактор В.И. БОРИСОВА

Компьютерный дизайн и верстка А.М. ПРУДНИК

Подписано в печать 6.05.2005. Дата выхода в свет 17.05.2005. Формат 60×84 ⅛. Гарнитура «Century Schoolbook».
Печать ризографическая. Усл. печ. л. 23,83. Уч. изд. л. 21,45. Тираж 100 экз. Заказ 83.
Индекс для ведомственной подписки 007872. Подписная цена 7 450 р.
Индекс для индивидуальной подписки 00787. Подписная цена 7 390 р.

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

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

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

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

III Белорусско-российская научно–техническая конференция

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

23 мая – 27 мая 2005
Минск — Нарочь

Материалы докладов и краткие сообщения

СОДЕРЖАНИЕ

Секция 1. Организационно-правовое и методологическое обеспечение защиты информации

- **Анищенко В.В.** Системный анализ рисков. Сущность и основные направления использования 7
- **Анищенко В.В., Криштофик А.М.** Методика разработки функциональных требований безопасности на основе системного анализа рисков 7
- **Анищенко В.В., Криштофик А.М.** Системный анализ рисков. Способы описания элементов безопасности 8
- **Криштофик А.М.** Системный анализ рисков. Определение потенциала атаки 9
- **Мартинович Т.С., Талалуева М.А., Фисенко В.К.** Направления развития Общей методологии оценки безопасности информационных технологий 9
- **Корлуженко В.А., Максимович Е.П., Фисенко В.К.** Подход к выбору требований информационной безопасности на основе кластерного анализа 10
- **Липень В.Ю., Воронецкий М.А., Липень Д.В.** Обеспечение достоверности и правомочности документов, выдаваемых с помощью автоматизированных информационных систем 11
- **Липень В.Ю., Воронецкий М.А., Демченко А.И., Липень Д.В.** Средства защиты и контроля за оборотом документов в электронной и бумажной форме 12
- **Трухан С.А.** Модель управления информационными рисками 13
- **Костров А.И., Радыно Т.В.** Юридические гарантии защиты информации 14

Секция 2. Технические средства обнаружения и подавления каналов утечки информации

- **Верлыго С.П., Потапович А.В.** Экспериментальные исследования статистических параметров речи 16
- **Главинский Б.О., Деев Н.А., Дубровский В.В., Чердынцев В.А.** Алгоритмы защиты информации в системах видеонаблюдения 16

- **Язловецкий Я.С.** Маскирование поля шифрованных данных в синхронных радиосетях с временным разделением каналов ... 17
- **Ходыко Д.Л. Саломатин С.Б.** Анализ помехозащищенности устройств навигационной информации ... 18
- **Хижняк А.В., Моисеев В.В., Шевяков А.В.** Особенности изображений и методика расчета характеристик обнаружения объектов в инфракрасном диапазоне ... 18
- **Хижняк А.В., Моисеев В.В., Шевяков А.В.** Результаты исследования временных свойств радиопоглощающих материалов в радиолокационном диапазоне ... 19
- **Ходыко Д.Л., Саломатин С.Б.** Анализ помехозащищенности устройств навигационной информации ... 20
- **Мисюкевич Н.С., Яцковский Ю.Э.** Подавление радиоканала пламенем ... 20
- **Бельский А.Я., Гусинский А.В., Дзисяк А.Б., Кострикин А.М.** Измерители флуктуаций миллиметрового диапазона длин волн ... 21
- **Свирид М.С.** Коммутационная схема построения устройства автоматической калибровки векторного анализатора цепей ... 22
- **Гурло Ю.Е.** Антенные измерения мощности излучения индустриальных радиопомех ... 22
- **Борботько Т.В., Хай Нгуен Ван** Оптические свойства гетерогенных поглотителей электромагнитного излучения ... 23
- **Лыньков Л.М., Борботько Т.В., Петров С.Н.** Методы и средства защиты от психотронных воздействий ... 24
- **Бригидин А.М.** Об одном способе определения восприимчивости генераторов СВЧ при воздействии помех 24
- **Луговский В.П., Русак И.М.** Особенности информационной защиты интеллектуальных источников электропитания компьютеров ... 25
- **Хижняк А.В., Игнатченко А.В.** Метод криптографической защиты видеоинформации в средствах обработки данных ... 26
- **Лыньков Л.М., Кузнецов С.С., Борботько Т.В.** Разработка средств имитации наземных объектов ... 27
- **Паркун В.М., Кузнецов С.С., Борботько Т.В.** Скрытие наземных объектов в широком диапазоне длин волн ... 27
- **Богуш В.А., Зубаревич О.И., Колбун Н.В., Позняк А.А.** Влияние растворных наполнителей гибких радиопоглощающих материалов на эффективность подавления электромагнитного канала утечки информации 28
- **Пулко Е.С., Богуш В.А.** Подавление побочных электромагнитных излучений композиционными экранирующими покрытиями для защиты информации в сетях связи ... 29
- **Прудник А.М., Алехина Н.Е., Смирнов Ю.В., Власова Г.А., Петров С.Н.** Комбинированные гибкие панели для Биологической защиты организма от электромагнитных и акустических воздействий ... 31
- **Воробьев В.И., Давыдов Г.В.** Установка для измерения динамических сил, развиваемых электроакустическими преобразователями устройств акустического маскирования речевых сигналов ... 32

Секция 3. Программно-аппаратные средства защиты информации в компьютерных и телекоммуникационных сетях

- **Бокунович А.В., Минченко Л.И., Харитоненков Е.В.** Применение теоремы Байеса при построении биометрической системы идентификации пользователя на базе клавиатурного почерка ... 33
- **Борискевич А.А., Лагойко А.Ю.** Защита речевых сообщений на основе псевдослучайных и однородных перестановок ... 33
- **Борискевич А.А., Меркушов А.А.** Синтез и анализ хаотических последовательностей на основе линейных и нелинейных методов ... 34
- **Гарцуев А.Л., Борзенков А.В.** Безопасное программирование на языках серверных сценариев Pearl и PHP 35
- **Величковский В.В.** Вычисление комплексного коэффициента передачи СВЧ четырехполюсника в узкой полосе частот ... 35
- **Баев В.С., Дайняк И.В.** Методы защиты SWF-файлов от декомпиляции ... 36

- **Дайняк И.В., Баев В.С., Карпович С.Е.** Защита мультимедийного контента сетевой интерактивной мультимедийной обучающей системы 36
- **Карасик Е.А.** Повышение надежности криптографической защиты с использованием временных характеристик процесса шифрования 37
- **Кузнецов А.П., Ганьшин Д.А., Русак Л.В., Седушкин А.А., Алькатауна Х.А.** Автоматизированное проектирование систем с фазовым управлением 38
- **Колешко В.М., Карякин Ю.Д.** Псевдостохастические нейронные системы обработки и защиты информации 39
- **Тыкоцкий С.А.** Идентификация автора электронного продукта 39
- **Усова М.Г., Стеринзат Д.М., Тиванова М.С.** Об организации защиты корпоративных данных 40
- **Митюхин А.И.** Обнаружение энергетически скрытного кодированного сигнала 41
- **Сиротко С.И.** Измерение временных параметров консольного ввода для задачи анализа клавиатурного почерка 41
- **Афанасенко А.Э.** Протоколы обеспечения безопасности vpn-соединения 42
- **Лазаревич В.Л.** Обеспечение защиты рабочих станций и корпоративных сетей с использованием Windows Firewall 43
- **Лазаревич Е.В.** Построение системы переподготовки кадров на базе платформы Microsoft eLearning Server 44
- **Некрасов В.С., Летохо А.С.** Программный модуль защиты информации в компьютерных сетях 44
- **Голенков В.В., Иванченко Ю.И., Деев А.Ю.** Обеспечение информационной безопасности корпоративной системы профилирующей кафедры 45
- **Гембицкий А.В., Саломатин С.Б.** Статистическое исследование псевдослучайных последовательностей на эллиптических кривых 46
- **Готовко В.А., Липницкий В.А.** Оценка мощности открытых ключей в криптосистеме Мак-Элиса-Сидельникова 46
- **Прищепа Д.С., Голиков В.Ф.** Имитация удаленных атак, направленных на отказ в обслуживании сетевых операционных систем 47
- **Величковский В.В.** Защита информации от искажений методом встречной фильтрации 50
- **Яшин К.Д., Алексейчук Л.И., Осипович В.С., Пицук С.Е.** Технические средства визуализации информации 50
- **Колбун Н.В., Фан Н. Занг, Лыньков Л.М.** Экранирующие свойства порошкообразного влагосодержащего материала на основе бентонита 51
- **Терех И.С., Турук Г.П., Рубаник А.В., Лыньков Л.М., Колбун Н.В.** Влияние импульсного электромагнитного излучения на влагосодержащие капиллярно пористые материалы. 55
- **Лыньков Л.М., Таболич Т.Г.** Отбраковочные испытания электронных пластиковых карт 57
- **Таболич Т.Г., Сечко Г.В.** Оценка интегральных показателей качества таксофонных интеллектуальных пластиковых карт 60
- **Анищенко В.В., Земцов Ю.В.** Внешний активный аудит безопасности корпоративной сети 61
- **Анищенко В.В., Земцов Ю.В.** Фильтрация ложных сигналов тревоги с помощью интеллектуального анализа данных 62
- **Дубровский В.В.** Некогерентный алгоритм обработки шумоподобного сигнала в совмещённой системе передачи информации 63
- **Конопелько В.К., Липницкий В.А.** Корректирующие возможности укороченных РС-кодов 64
- **Липницкий В.А., Костелецкий А.В.** О программной реализации криптосистемы Мак-Элиса– Сидельникова 65
- **Борискевич А.А., Ливочкин В.В., Подлуцкий А.А., Цветков В.Ю.** Генетический алгоритм маршрутизации пакетов на основе рекурсивных разверток для защиты медиатрафика 65
- **Борискевич А.А., Цветков В.Ю.** Метод шифрования речи и данных на основе рекурсивных разверток и муаровых ключей 66

- **Борискевич А.А., Ливочкин В.В., Подлуцкий А.А., Цветков В.Ю.** Адаптивно-динамический метод внесения защитных элементов в видеоизображение 67
- **Шкиленок А.В.** Применение помехоустойчивых турбо-кодов в системах связи 67
- **Ревотюк М.П., Колотыгин К.Е.** Сквозная защита персональных каналов на локальной сети 68
- **Ревотюк М.П., Бацекина Е.П.** Защита программ от авторизованных пользователей 69
- **Ревотюк М.П., Жирко Т.А., Кишкевич А.П.** Активная защита исполняемых модулей ответственных систем обработки информации 70
- **Ревотюк М.П., Хаджинова Н.В.** Защита распределенных кооперативных вычислений на локальных сетях ... 71

Секция 4. Проектирование и производство элементов и компонентов для систем защиты информации

- **Прудникова Е.Л.** Углеродные нанотрубки для сверхбыстродействующих транзисторов — элементной базы информационных систем будущего поколения 72
- **Емельянов В.А., Пономарь В.Н., Чигирь Г.Г., Ухов В.А.** Анализ элементной базы систем защиты информации в Государственном Центре "Белмикроанализ" 73
- **Емельянов В.А., Пономарь В.Н., Чигирь Г.Г.** Цифровая оптическая микроскопия в производстве элементной базы для систем защиты информации 74
- **Емельянов В.А., Пономарь В.Н., Ухов В.А., Лесникова В.П.** Анализ микроэлектронных структур с высоким пространственным разрешением 74
- **Максимович Р.Н., Попов В.А.** Электропитание мобильного комплекса контроля защищенности речевой информации 75
- **Пушкарчук В.А., Килин С.Я., Низовцев А.П., Пушкарчук А.Л., Борисенко В.Е., Филонов А.Б.** Источники одиночных фотонов для квантовой криптографии: ab initio исследование одиночных NV^--центров в наноалмазе 75
- **Циркунов Д.А., Молчан И.С., Маляревич Г.К., Гапоненко Н.В.** Скрытые люминесцирующие изображения . 76
- **Русак Л.В., Бусько В.Л.** Моделирование в среде Matlab дискретных систем с фазовым управлением 77
- **Подрябинкин Д.А., Данилюк А.Л.** Элементы квантовой логики для защиты информации 78
- **Данилюк А.Л., Титович И.Н.** Синхронизация ансамбля кубит при непрерывных квантовых измерениях 78
- **Королев А.В., Кривошеева А.В., Данилюк А.Л.** Вычислительные кластеры на основе кремния для квантовых каналов связи 79
- **Образцов Н.С., Кулешов Д.А., Пинаев А.И.** Методика повышения устойчивости работы интегральных схем к воздействию мощных электромагнитных помех 80
- **Образцов Н.С., Макаревич С.Ю., Пинаев А.И.** Схемотехнические решения импульсной защиты на МОП-транзисторах 81
- **Образцов Н.С., Мельничук В.В., Пинаев А.И.** Разработка испытательного оборудования для оценки стойкости к импульсным сигналам средств защиты информации 81
- **Гаврилович А.Б., Радыно Н.Я.** Об оптическом методе исследования шероховатых поверхностей и его приложении к определению генетической информации по поверхности биологического материала 82
- **Бересневич А.И., Боровиков С.М.** Выбор имитационных воздействий в задачах прогнозирования постепенных отказов полупроводниковых приборов 83
- **Бересневич А.И., Боровиков С.М.** Использование параметров электрического режима биполярных транзисторов в качестве имитационных факторов 83
- **Боровиков С.М., Никифоренко Л.Г.** Эффективность прогнозирования надёжности элементов методом пороговой логики 84
- **Боровиков С.М., Мандик Н.Е.** Эффективность прогнозирования постепенных отказов биполярных транзисторов методом имитационных воздействий 85
- **Унучек Д.Н., Лазарук С.К., Кацуба П.С., Румянцев А.А., Лешок А.А., Лабунов В.А.** Использование нанокристаллического кремния для создания люминесцентных надписей 85

- **Луговский В.П., Русак И.М.** Использование инжекционно-полевых транзисторных структур для активного подавления данных в сетях электропитания 86
- **Долбик А.В., Лазарук С.К., Кацуба П.С., Румянцев А.А., Лабунов В.А.** Саморазрушающиеся кремниевые чипы при попытке несанкционированного доступа к ним 87
- **Ажаронок В.В., Бордусов С.В., Вощула И.В., Филатова И.И.** Изменение оптических свойств бумаги при воздействии высокочастотного магнитного поля 87
- **Галузо В.Е.** Модель МДП-транзистора с субмикронными размерами 88

Секция 5. Защита информации в банковских технологиях

- **Маликов В.В.** Интегрированные системы технических средств охраны банковских учреждений 89
- **Поляков А.С., Самсонов В.Е.** Проблемы практического применения электронных документов и электронной цифровой подписи 90
- **Цынкевич Е.А.** Форматы электронных документов как элемент защиты в системах электронного документооборота 91
- **Полаженко С.В.** САПР для проектирования правил разграничения доступа в автоматизированных системах в процессе её проектирования и эксплуатации 92

Секция 6. Проблемы подготовки и переподготовки кадров

- **Яшин К.Д., Кузнецов В.В., Паримская Л.Е.** Лабораторный практикум "Влияние электромагнитных полей на организм человека" 93
- **Гулаков И.Р., Зеневич А.О.** Анализ квантовых оптических каналов связи 94
- **Новикова Л.М.** Подготовка студентов в Высшем государственном колледже связи по вопросам безопасности 95
- **Левкович В.Н., Саломатин С.Б., Ходасевич Р.Г.** Подготовка специалистов по радиоэлектронной защите информации 96
- **Липницкий В.А., Липницкая В.А.** О математическом обеспечении курса защиты информации 96
- **Лыньков Л.М., Соловьев В.В., Прудник А.М., Жданович С.В.** Особенности внедрения решений Бухарестской всемирной почтовой стратегии в сфере информационной безопасности 97
- **Богуш В.А., Доду А.В., Тиллаев М.З.** Система автоматизации контроля знаний учащихся по защите информации 98
- **Богуш В.А., Голиков В.Ф., Конопелько В.К., Лыньков Л.М.** Организация подготовки инженерных кадров по новой специальности "Защита информации в телекоммуникациях" 99

СЕКЦИЯ 1. ОРГАНИЗАЦИОННО-ПРАВОВОЕ И МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

СИСТЕМНЫЙ АНАЛИЗ РИСКОВ. СУЩНОСТЬ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ

В.В. АНИЩЕНКО

Нормативная база в области обеспечения безопасности информационных технологий предусматривает анализ и оценку рисков при проведении любых работ. Однако для этого не в полной мере разработаны математический и методический аппараты. В связи с этим широко используются на практике базовый и экспертный методы анализа рисков. Первый из них не предусматривает оценку рисков, второй - использует качественную или количественную оценку рисков на основании экспертных данных. Основными недостатками данных методов являются субъективность оценки и невозможность сопровождения и использования полученных результатов в процессе эксплуатации объекта информационных технологий (ОИТ). Для устранения указанных недостатков разработан системный анализ рисков.

Системный анализ рисков основан на проведении комплексного анализа всех элементов безопасности и оценка рисков на его основе. Он разработан на основе базовой модели ОИТ, модели системы защиты и их комплексных показателей, характеризующих взаимодействие объекта оценки (00) с внешней средой и негативные последствия этого взаимодействия, а также изменение свойств и характеристик 00 и последствий нарушения информационной безопасности при изменении его структуры.

Основными направлениями использования системного анализа рисков являются:

– комплексная оценка элементов безопасности;

– разработка требований безопасности и требований к стойкости средств обеспечения безопасности (СОБ);

– обоснование и выбор варианта СОБ, проведение сравнительного анализа различных вариантов СОБ;

– оценка защищенности ОИТ на всех этапах жизненного цикла;

– оценка соответствия ОИТ заданным требованиям безопасности;

– принятие решения о доработке (модернизации) СБО и выработка рекомендаций по ее проведению.

МЕТОДИКА РАЗРАБОТКИ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ НА ОСНОВЕ СИСТЕМНОГО АНАЛИЗА РИСКОВ

В.В. АНИЩЕНКО, А.М. КРИШТОФИК

Рассматриваются вопросы недостаточности общих критериев для разработки требований безопасности при проектировании профиля защиты (задания по безопасности). Для устранения недостатков предлагается методика разработки функциональных требований безопасности с использованием системного анализа рисков. Задача разработки требований

безопасности в профиле защиты (задании по безопасности) объекта информационных технологий (ОИТ) на основе системного анализа рисков проводится на основе анализа взаимодействия следующих элементов безопасности:

"угроза (действие) ⇒ ***фактор*** (уязвимость) ⇒ ***риск*** (возможность последствий) ⇒ ***требования безопасности*** (требования к контрмерам)***"***

В основу разработки требований безопасности положен системный анализ рисков на основе формальной модели объекта информатизации, основу которой составляет процедура анализа рисков. Классификация угроз безопасности в данном случае проводится не в зависимости от характера ущерба, а в соответствии с функциями безопасности, определяемыми Общими критериями. В данном случае не возникает вопроса о составе функциональных требований безопасности для обеспечения минимального или требуемого уровня защищенности, разрабатываются и обосновываются требования к стойкости средств обеспечения безопасности.

Этот подход уточняет определение типового объекта оценки, облегчает процедуру разработки (выбора варианта) средств обеспечения безопасности. Разработанные с помощью данного метода профили защиты и задания по безопасности целесообразно каталогизировать.

Следовательно, проектирование профилей защиты (заданий безопасности) целесообразно учитывать риски нанесения ущерба владельцам активов, что позволяет научно обоснованно их использовать при разработке средств обеспечения безопасности. Следствием этого является изменение методики разработки профилей защиты.

СИСТЕМНЫЙ АНАЛИЗ РИСКОВ. СПОСОБЫ ОПИСАНИЯ ЭЛЕМЕНТОВ БЕЗОПАСНОСТИ

В.В. АНИЩЕНКО, А.М. КРИШТОФИК

При повышенных требованиях безопасности одним из основных вопросов оценки защищенности объектов информационных технологий является оценка элементов безопасности. Это необходимо для качественной или количественной оценки негативных последствий от нарушения информационной безопасности, т.е. оценки рисков нанесения ущерба владельцам активов. Существующие способы описания элементов безопасности, реализуемые в инструментальных средствах, таких как COBRA, RA Software Tool, CRAMM, Risk Watch, MARION, Buddy System, Method Ware, являются субъективными, требуют одинакового их понимания экспертами, проводящими оценку. В научно-технической литературе делается попытка обоснования их как субъективная вероятность, что противоречит теории вероятностей и математической статистике. Использование же вероятностных способов описания элементов безопасности невозможно вследствие отсутствия статистической информации, а при ее наличии — быстрое ее устаревание.

Предлагаемыми способами описания элементов безопасности являются использование субъективных вероятностных оценок или нечетких интервальных оценок. Субъективные вероятностные оценки получаются путем статистической обработки экспертных оценок, полученных на основании анкетирования большого числа экспертов. При этом могут использоваться численные и гистограммные методы оценки. Данный способ опи-

сания элементов безопасности позволяет получить также доверительную вероятность полученных оценок. Описание элементов безопасности с использованием нечетких интервальных оценок также предполагает получение экспертных оценок на основании анкетирования большого числа экспертов, однако в дано случае статистическая обработка данных не производится, а определяется функция принадлежности нечеткого интервального множества.

СИСТЕМНЫЙ АНАЛИЗ РИСКОВ. ОПРЕДЕЛЕНИЕ ПОТЕНЦИАЛА АТАКИ

А.М. КРИШТОФИК

Выявление атак и других нарушений информационной безопасности, наряду с такими способами как уменьшение вероятности осуществления угроз безопасности, ликвидация уязвимостей или уменьшение их величины, уменьшение величины возможного ущерба, восстановление ресурсов, которым был нанесен ущерб, является одним из направлений снижения рисков нанесения ущерба. Данный способ реализуется путем разработки и использования систем обнаружения атак. Однако при их разработке возникает вопрос определения наиболее опасных атак, обнаружение которых является первоочередной задачей. Данная задача решается путем определения потенциалов атак и их ранжирования.

При использовании системного анализа рисков уточняется определение атаки по отношению к действующей нормативной базе в области безопасности информационных технологий. Потенциал атаки определяется как мера, характеризующая возможности по нанесению негативных последствий от реализации атаки, т.е. через риск нанесения ущерба владельцам активов. В качестве меры потенциала атаки используется частный Интегральный показатель защищенности. Численное значение потенциала атаки определяется на основании параметров и характеристик элементов безопасности с учетом вопросов коррелированности угроз безопасности и уязвимостей объекта оценки. Ранжирование атак проводится на основе коэффициентов их опасности.

Следовательно, при проектировании и разработке систем обнаружения атак с использованием системного подхода необходимо оценивать риски нанесения ущерба владельцам активов в целях определения потенциала атак и проведения их ранжирования

НАПРАВЛЕНИЯ РАЗВИТИЯ ОБЩЕЙ МЕТОДОЛОГИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Т.С. МАРТИНОВИЧ, М.А. ТАЛАЛУЕВА, В.К. ФИСЕНКО

Первая версия Общей методологии оценки безопасности информационных технологий (ОМО, версия 0.6) вышла в двух частях. Первая часть вышла в 1997 г., а вторая — в 1999 г. Соответствующий документ носит название "Common Methodology for Information Technology Security Evaluation": Часть 1: Introduction and General Model (Введение и общая модель); Часть 2: Evaluation Methodology (Методология оценки).

На базе двух частей этой версии ОМО был разработан ОИПИ НАН Беларуси и принят Госстандартом Республики Беларусь

СТБ П 34.101.5-2003 "Общая методология испытаний продуктов и систем информационных технологий на соответствие уровням гарантии", который был введен в действие с ноября 2003 г.

ОМО, как и Общие критерии (ОК) находятся в постоянном развитии, в процессе практического их использования возникает необходимость совершенствовать их структуру, учитывать выявленные недостатки. После выхода первой версии ОМО было несколько новых редакций, последняя из которых (версия 2.4) вышла в марте 2004 г.

Новая версия ОМО претерпела ряд изменений, наиболее существенными из которых являются:

– новая версия объединила обе части, в нее внесены изменения, касающиеся противоречий между ч. 1 ОМО (1997 г.) и ISO/IEC 15408:1999. Основные положения части 1 изложены в подразделе главы 2 "Процесс оценки и соответствующие задачи";

– существенной переработке подверглись главы, касающиеся оценки профиля защиты (ПЗ) и задания по безопасности (ЗБ). Раздел "Оценка ЗБ" ранее был выделен в отдельную главу. В новой версии ОМО рекомендуется проводить оценку ЗБ совместно с объектом, причем методология оценки ЗБ и объекта приведена лишь для уровней гарантии 1 и 4;

– добавлена глава "Устранение недостатков".

По нашему мнению, дальнейшее развитие методологии оценки безопасности должно быть направлено на доработку существующего предстандарта и ввода в действие государственного стандарта с учетом последней версии ОМО.

ПОДХОД К ВЫБОРУ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ КЛАСТЕРНОГО АНАЛИЗА

В.А. КОРЛУЖЕНКО, Е.П. МАКСИМОВИЧ, В.К. ФИСЕНКО

При разработке профилей защиты или заданий по безопасности ключевое значение имеет определение набора требований безопасности (ТБ). Предлагается подход к выбору типового набора ТБ, основанный на экспертном анализе и классификации объектов информационных технологий (ОИТ) относительно предварительно сформированного множества кластеров. Определение множества кластеров сводится к задаче классификации без учителя и с внешней целью.

Реализация подхода разбивается на следующие основные этапы.

1. Построение множества общесистемных признаков для описания ОИТ. Признаки определяются на экспертном уровне и представляют собой лингвистические переменные (ЛП) типа "категория обрабатываемой информации", "условия функционирования ОИТ" и т.д.

2. Формирование множества допустимых ОИТ в терминах введенных признаков. На основании экспертного анализа строится иерархическое дерево. Корень дерева отождествляется со всеми ОИТ. Первое ветвление ведется по 1-му признаку — количество узлов 1-го уровня равно количеству термов (значений) ЛП 1-го признака. От узлов 1-го уровня проводится ветвление по 2-му признаку, учитывая все допустимые возможности. От узлов 2-го уровня — по третьему признаку и т.д. Множество концевых узлов дерева — все допустимые (с учетом предков) ОИТ.

3. Разбиение множества допустимых ОИТ на кластеры. На основе экспертного анализа производится последовательное продвижение сверху вниз по дереву. Корню дерева ставятся в соответствие все классы функциональных ТБ "Общих критериев". Если на некотором уровне выявляются узлы, которым соответствуют заведомо разные ТБ, то соответствующие им ОИТ относятся к разным кластерам. С каждым узлом связывается множество допустимых ТБ. В результате полного просмотра дерева формируется разбиение на кластеры. Каждому кластеру ставится в соответствие множество допустимых ТБ – все ТБ, которые не были отброшены в процессе рассмотрения предков соответствующего узла.

4. Формирование описания кластеров. На основе экспертного анализа для каждого кластера формируются (в терминах термов ЛП признаков) системы продукционных правил. В соответствии с критерием разбиения, любые два кластера отличаются значением хотя бы одного из признаков, вследствие чего для них можно определить разные правила.

5. Построение решающего правила. Правило состоит в проверке для ОИТ продукционных правил каждого кластера и отнесение объекта к тому кластеру, чьи правила для него выполняются.

ОБЕСПЕЧЕНИЕ ДОСТОВЕРНОСТИ И ПРАВОМОЧНОСТИ ДОКУМЕНТОВ, ВЫДАВАЕМЫХ С ПОМОЩЬЮ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

В.Ю. ЛИПЕНЬ, М.А. ВОРОНЕЦКИЙ, Д.В. ЛИПЕНЬ

Одним из путей улучшения информационного обслуживания граждан и субъектов хозяйствования является использование Единого Государственного информационного ресурса (ЕГИР) и реализация принципа "единого окна".

Специалистами ОИПИ НАН Беларуси предлагается подход, при котором обслуживание респондентов, не имеющих возможности обратиться к ЕГИР с помощью собственного сетевого компьютера, осуществляется в специально оборудованных Пунктах информационного обслуживания населения (ПИОН). При этом необходимо разработать несколько модификаций АРМ персонала ПИОН, которые реализуют процедуры идентификации граждан и субъектов хозяйствования, процедуры передачи и получения электронных сообщений от имени обратившегося к ресурсу клиента пион, а также процедуру выдачи запрошенных документов в виде электронных копий, заверяемых ЭЦП уполномоченного служащего, и/или машинозаполняемых бумажных копий, снабжаемых криптографической маркировкой в виде штрих-кодов. Аутентичность электронной и бумажной форм документа достигается за счет использования унифицированных XML-структур при формировании контента. Использование единого уникального криптоидентификатора для обеих форм документа обеспечивает их взаимно однозначное соответствие и упрощает поиск в базе данных.

СРЕДСТВА ЗАЩИТЫ И КОНТРОЛЯ ЗА ОБОРОТОМ ДОКУМЕНТОВ В ЭЛЕКТРОННОЙ И БУМАЖНОЙ ФОРМЕ

В.Ю. ЛИПЕНЬ, М.А. ВОРОНЕЦКИЙ, А.И. ДЕМЧЕНКО, Д.В. ЛИПЕНЬ.

Подход к решению проблемы совместного использования электронных и традиционных "бумажных" документов основывается на учете того обстоятельства, что все увеличивающаяся доля бумажных документов является машинозаполняемыми, т.е. печатается под управлением компьютеров. Это позволяет одновременно с принтерной печатью текста осуществить под управлением криптограмм автоматическое нанесение машиносчитываемых маркеров. Одновременно с печатью бумажной копии осуществляется выдача электронного оригинала, который при необходимости шифруется и снабжается ЭЦП.

Докладчиком демонстрируются образцы документов с машиносчитываемой маркировкой и процедуры их изготовления и верификации. Приводятся структурные схемы систем замкнутого контроля за оборотом машинозаполняемых документов на примере проекта системы контроля за ввозом-вывозом легковых автомобилей, разработанного для Государственного таможенного комитета РБ, а также на примере экспериментального образца системы электронного голосования (ЭГ). Последняя была разработана и передана в 2003 году по заказу Национального научно-технического центра Республики Казахстан и послужила в качестве базы для изготовления и внедрения Центральной избирательной комиссией системы ЭГ "Сайлау". На выборах в Мажилис 9 сентября 2004 года система ЭГ прошла апробацию на 961 избирательном участке Республики Казахстан.

МОДЕЛЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

С.А. ТРУХАН

Под термином "управление информационными рисками" обычно понимается системный процесс идентификации, контроля и уменьшения информационных рисков компаний. Качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации.

Примерно с 1995 года в ряде высокотехнологичных стран мира проводятся ежегодные слушания по вопросам управления информационными рисками. Подготовлено более десятка различных стандартов и спецификаций, среди которых можно выделить следующие ISO 177992002 (BS 7799) [1], GAO и FISCAM, SCIP, NIST, AS/NZS 4360:2004 [2],[3], SAS 78/94 и COBIT. По этому трудно себе представить серьезную систему безопасности без модели управления рисками [4].

Рассмотрим основные принципы, которые закладываются в модель управления информационными рисками.

На первом этапе производится определение обстоятельств проведения оценки рисков. Это предполагает: краткий обзор целей предприятия; резюме целей всех заинтересованных лиц в оценке безопасности; выбор критериев, отражающих основные цели предприятия и позволяющие определить частоту или вероятность реализации риска и наносимый ущерб; выбор защищаемых активов; выбор ключевых элементов (тем), которые

будут рассматриваться последовательно в процессе определения рисков. Важно отметить, что эти темы должны включать в себя основные риски и не сильно затягивать этап определения рисков.

На втором этапе происходит определение рисков. Это предполагает выявление угроз и нежелательных инцидентов, которые могут привести к угрозам. Определение рисков изначально производиться с помощью методов контрольных списков, которые дополняются сессиями мозгового штурма с квалифицированными специалистами из разных областей. Данный подход позволяет максимально выявить и определить основные угрозы и нежелательные инциденты.

На третьем этапе производится анализ рисков. Этот этап предполагает: распределение рисков по родственным группам; определяется вероятность частоты появления рисков; определяется ущерб, наносимый риском; делаются предположения об уровне рисков. На данном этапе вводятся любые коэффициенты, которые будут отображать значение риска и участвовать в управлении риском. Для простых рисков могут находиться вероятности и строиться матрицы. Для сложных рисков, где вовлекается большое количество связанных событий, могут применяться некоторые методы моделирования. Независимо от детализации описания рисков, результат данного этапа – это начальное представление значений выявленных рисков, которые будут корректироваться на этапе оценки рисков.

На четвертом этапе производится оценка рисков, которая является критической для выявления наиболее важных рисков. В сложных ситуациях выявленные риски соотносятся с требованиями и целями предприятия. На основании данного анализа незначительные риски, в данном контексте, отбрасываются. Это позволяет сократить трудоемкость следующего этапа.

На пятом этапе рассматриваются методы "лечения" рисков. На этом этапе производится поиск методов уменьшения вероятности возникновения рисков или, если это невозможно, то поиск способов уменьшение наносимого ущерба. На данном этапе вводятся коэффициенты, которые отражают эффективность применяемых методов. На основании данных коэффициентов формируются планы стратегического поведения предприятия. Данные планы могут применяться для случаев возникновения выше выявленных рисков или вообще обходить данные риски на основании выбранной стратегии поведения предприятия.

Кроме пяти этапов в процессе управления рисками присутствуют ещё два процесса:

1. Процесс контроля и анализа, который присутствует на всех пяти этапах. Основной смысл данного процесса в следующем: в регулировании глубины изучения вопросов; в анализе внешних условий в ходе исследования и при их устаревании, в пересмотре результатов исследования с учетом современного состояния дел; в анализе затрат ресурсов на каждом этапе управления рисками, чтобы гарантировать рентабельность.

2. Процесс общения и консультирования, который присутствует на всех пяти этапах. Основной смысл данного процесса в следующем: в вовлечении максимального количества заинтересованных лиц в процесс оценки рисков; в выявлении наиболее актуальных рисков и определении степени последствий в исследуемой области; в том, что учтены все требования и цели со стороны предприятия.

В заключении хотелось бы заметить, что грамотное использование модели управления информационными рисками позволит получать очень хорошие результаты, наиболее важным из которых, является возможность экономического обоснования расходов предприятия на обеспечение информационной безопасности и непрерывности бизнеса. Экономически обоснованная стратегия управления рисками позволяет, в конечном итоге, экономить средства, избегая неоправданных расходов.

Литература
1. ISO/IEC 17799:2002 Information technology – Code of practice for information security management. International Organization for Standardization (2002);
2. Standards Australia and Standards New Zealand (2004) AS/NZS 4360:2004. Risk Management. Sydney. NSW. ISBN 0 7337 5904 1.
3. Standards Australia and Standards New Zealand (2004) HB 436:2004. Risk Management Guidelines: Companion to AS/XZS 4360:2004, Sydney, NSW. ISBN 0 7337 5960 2.
4. Сергей Петренко, Сергей Симонов, Методики и технологии управления информационными рисками, IT Manager, № 3/2003.

ЮРИДИЧЕСКИЕ ГАРАНТИИ ЗАЩИТЫ ИНФОРМАЦИИ

А.И. КОСТРОВ, Т.В. РАДЫНО

Информация стала первоосновой жизни современного общества, средством и продуктом его деятельности, а процессы ее создания, накопления, хранения, передачи и обработки в свою очередь стимулируют прогресс в области орудий ее производства: электронно-вычислительной техники, средств телекоммуникаций и систем связи. Следствием протекающих в обществе информационных процессов является возникновение и формирование новых социальных отношений и изменение уже существующих. Однако новые информационные технологии дали толчок в плане прогресса общества, но и стимулировали возникновение и развитие неизвестных ранее форм преступности — информационных преступлений.

Поэтому, критически оценивая современное состояние криминалистической теории и учитывая потребности оперативно-следственной практики, надо признать, что в целом проблема данного вида преступлений изучена явно недостаточно. Однако начинать исследование обозначенных проблем необходимо прежде всего с уяснения сути информационных правоотношений и содержания центральных их понятий информации и информационных процессов.

При этом необходимо учитывать следующие основные тенденции информационных процессов: во-первых, информация стала не просто сообщением, имеющим конкретное содержание, а экономической категорией. Она получает рыночную оценку и перестает быть бесплатным товаром. Иными словами, информация, являясь продуктом общественных (информационных) отношений, становится предметом купли – продажи; во-вторых, как известно, производимая в государстве и обществе информация, включаемая в сферу правового регулирования, подлежит, в большинстве случаев, документированию. Фиксация информации и ее идентификаторов на материальном носителе — это важнейший в правовом отношении факт. Понимая это необходимо учитывать, что во вполне обозримом будущем (в ближайшие десятилетия), весь документооборот будет осуществляться на машиночитаемых носителях. Поэтому проблема информационной безопасности становится одной из

самых насущных проблем общества. Без решения этой проблемы невозможен полномасштабный и эффективный переход к цивилизованной экономике и открытому информационному обществу.

СЕКЦИЯ 2. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ СТАТИСТИЧЕСКИХ ПАРАМЕТРОВ РЕЧИ

С.П. ВЕРЛЫГО, А.В. ПОТАПОВИЧ

Эффективность защиты речевой информации в сильной степени зависит от принятой модели источника речевой информации. Так как речевой сигнал имеет всплесковый характер и определяется в первую очередь особенностями говорящего, то выработать требования по защите речевой информации и оценить степень ее защищенности представляется возможным при наличии модели источника речи. Для построения такой модели необходимо экспериментально исследовать статистические параметры речи различных дикторов. Речевой сигнал можно представить как случайный процесс, поэтому для его исследования можно использовать аппарат математической статистики.

Особенностью предлагаемой методики экспериментальных исследований является обработка речевого сигнала на ПК с помощью программных средств. В предлагаемой методике для оценки полученных опытных данных используются математическое ожидание, дисперсия, среднеквадратическое отклонение среднеквадратическое значение. Кроме этого по группированному статистическому ряду строится график функции распределения речевого сигнала. Алгоритм разработанной методики, состоит в следующем: производится запись звука на жесткий диск компьютера, затем вычисляются статистические параметры, получается группированный статистический ряд пиков с помощью ПО, и в конце происходит обработка полученных данных с помощью офисного приложения для электронных таблиц. В методике используется собственная программа, оптимизированная по скорости и по работе с памятью.

Разработанная методика была опробована на тестовой записи объемом 120 Мб длительностью 30 минут (WAV, 16 кГц, 16 бит). Время работы программы составило 6 минут, оформление данных в приложении Excel заняло 10 минут. Методика обеспечивает простоту и удобство, доступность, малую продолжительность проведения исследования, что очень важно для оперативной оценки требуемой защиты для речевого канала передачи информации.

АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

Б.О. ГЛАВИНСКИЙ, Н.А. ДЕЕВ, В.В. ДУБРОВСКИЙ, В.А. ЧЕРДЫНЦЕВ

Существующие системы видеонаблюдения, основанные на аналоговых алгоритмах формирования и обработки сигналов, обладают достаточно высоким потребительским качеством. Одним из важных требований к таким системам является защищённость информации, передаваемой по радиоканалу, от несанкционированного доступа.

Среди возможных алгоритмов преобразования сигнала, несущего информацию о наблюдаемом объекте, наиболее эффективными являются

следующие. Алгоритм, основанный на преобразовании видеосигнала изображения, снимаемого с выхода видеокамеры. Преобразованный (кодированный) сигнал передаётся по радиоканалу, принимается и обрабатывается в приёмном устройстве. Качество воспроизводимого изображения определяется точностью декодирующего устройства. Другой алгоритм основан на преобразовании радиосигнала, содержащего видеоинформацию. Такое преобразование может быть осуществлено на выходе передающего устройства путём скремблирования радиосигнала псевдослучайной последовательностью (ПСП) с определённой тактовой частотой и периодом. На приёмной стороне необходимо обеспечить синхронизацию местного генератора ПСП и демодуляцию принятого радиосигнала (дескремблирование).

Рассматриваются структурные схемы передающих и приёмных устройств, реализующие описанные алгоритмы. Проводится сравнительный анализ эффективности каждого из алгоритмов с точки зрения аппаратно-вычислительных затрат, помехоустойчивости и криптостойкости.

Обсуждаются возможности использования в качестве кодирующих и скремблирующих устройств сигналов псевдохаотических квантованных последовательностей, обеспечивающих высокую криптографическую защиту передаваемых видеоизображений.

МАСКИРОВАНИЕ ПОЛЯ ШИФРОВАННЫХ ДАННЫХ В СИНХРОННЫХ РАДИОСЕТЯХ С ВРЕМЕННЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

Я.С. ЯЗЛОВЕЦКИЙ

Доклад относится к вопросам структурной скрытности синхронных радиосетей с временным разделением каналов, в частности маскирования поля шифрованных данных.

Известны синхронные сети с временным разделением каналов, такие как DECT, GSM, синхронная ALOHA и т.п. В таких сетях разметка временных каналов производится путем передачи сигнала синхронизации в начале каждого канального интервала. После сигнала синхронизации в канальном интервале передаются данные служебной информация и шифрованные данные.

Так как длительность и закон образования сигнала синхронизации, и данные служебной информации изменяются незначительно от цикла к циклу, то возможно определение местоположения в канальном интервале поля шифрованных данных.

В докладе описывается три метода маскирования поля шифрованных данных: 1) изменение закона образования сигнала синхронизации при его неизменной длительности, и скремблирование данных служебной информации; 2) изменение местоположения поля шифрованных данных с помощью изменения длительности сигнала синхронизации; 3) изменение местоположения поля шифрованных данных с помощью добавления ложных шифрованных данных различной длительностью.

Предлагается сравнивать степень маскирования поля шифрованных данных на основе теории информации и корреляционного анализа. Для этого на выбранном интервале, середина которого находится в истинном местоположении поля шифрованных данных, сравниваются ко-

эффициенты полуинтервалов взаимной корреляции между сигналами канального интервала соседних циклов передачи.

Таким образом, путем выбора соответствующих параметров сигналов канального интервала можно добиться определенной степени маскирования поля шифрованных данных при учете оценки затрат на аппаратурную реализацию и оценки возможного снижения пропускной способности временного канала.

АНАЛИЗ ПОМЕХОЗАЩИЩЕННОСТИ УСТРОЙСТВ НАВИГАЦИОННОЙ ИНФОРМАЦИИ

Д.Л. ХОДЫКО С.Б. САЛОМАТИН

Современные радиоэлектронные системы спутниковой навигации (РЭС СН) различного назначения работают в сложной электромагнитной обстановке и включают в свой состав следящие устройства, позволяющие реализовать когерентную (квазикогерентную) обработку сложных сигналов. Оценка помехозащищенности РЭС СН позволяет оценить уровень защиты системы навигационной информации и целостности навигационного поля от преднамеренных радиоэлектронных воздействий.

Один из эффективных методов радиопротиводействия основан на применении структурированной помехи (СП) сложного вида.

Воздействие преднамеренных помех (ПП) различной мощности неоднозначно. Анализ, на основе компьютерного моделирования, показал, что воздействия ПП на схемы с перекрестными связями слежения за задержкой и фазой оказывает неоднозначное влияние. По результатам моделирования выбран ряд помех по критерию максимума дисперсии оцениваемого параметра. В связи с этим, сформирована группировка ПП, оказывающих наибольшее влияние на кольцо слежения за задержкой и фазой РЭС СН.

ОСОБЕННОСТИ ИЗОБРАЖЕНИЙ И МЕТОДИКА РАСЧЕТА ХАРАКТЕРИСТИК ОБНАРУЖЕНИЯ ОБЪЕКТОВ В ИНФРАКРАСНОМ ДИАПАЗОНЕ

А.В. ХИЖНЯК, В.В. МОИСЕЕВ, А.В. ШЕВЯКОВ

Одним из самых информативных каналов утечки информации наряду с оптическим и радиолокационным диапазонами является инфракрасный диапазон. Изображения объектов в инфракрасном (ИК) диапазоне длин волн обладают преимуществами, не свойственными другим диапазонам. К этим преимуществам можно отнести возможность обнаружить на ИК снимках предметы, не заметные на обычных фотопленках. ИК изображения позволяют получать информацию и об объектах, которые уже отсутствуют в момент съемки (по сохранившемуся тепловому портрету объекта). Существует возможность регистрации объектов как при отсутствии падающего излучения, так и при отсутствии температурных перепадов, только за счет различий в излучательной способности их поверхностей. ИК изображения позволяют выявлять информацию о действующих силовых и энергетических установках объектов вследствие более интенсивного их излучения по сравнению с более холодной поверхностью фона.

Скрытие объектов от средств ИК разведки подразумевает снижение теплового контраста объекта с фоном до уровня, при котором средство ИК разведки потеряет способность обнаружить объект при заданной дальности. Требуемый уровень теплового излучения маскируемого объекта необходимо рассчитывать исходя из излучательной способности материала, из которого изготовлен объект, ослабления атмосферой ИК излучения на оптическом пути и порога чувствительности средства ИК разведки.

Методика расчета характеристик обнаружения маскируемого объекта содержит расчет спектральной излучательной способности объекта, модель атмосферы, предназначенную для расчета прохождения ИК излучения, и модель средства обнаружения в ИК диапазоне.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ВРЕМЕННЫХ СВОЙСТВ РАДИОПОГЛОЩАЮЩИХ МАТЕРИАЛОВ В РАДИОЛОКАЦИОННОМ ДИАПАЗОНЕ

А.В. ХИЖНЯК, В.В. МОИСЕЕВ, А.В. ШЕВЯКОВ.

Широкое использование постоянно совершенствующихся средств технической разведки приводит к необходимости исследований средств защиты информации в широком диапазоне длин волн. Эффективность методов подавления каналов утечки информации средствами пассивной защиты (СПЗ) определяется отношением затрат на создание средств защиты к ущербу от утечки информации, по этому критерию они могут быть отнесены к наиболее доступным, поскольку технические средства пассивной защиты информации обладают низкой себестоимостью, просты в изготовлении и удобны в эксплуатации.

Ряд исследований различных радиопоглощающих материалов и их комбинаций показал, что наиболее эффективным и простым в реализации вариантом является использование материалов с жидким технологическим наполнителем. Выбор жидких технологических наполнителей обоснован возможностью эффективно изменять свойства путем изменения состава и концентрации. По разработанной технологии на базе волокнистых материалов были изготовлены поглотители электромагнитного излучения модульной конструкции различной плотности с линейными размерами 0,5x1,0 м., содержащие жидкий технологический наполнитель.

Исследовалась временная стабильность отражающих свойств материалов, в качестве измеряемого параметра выступала электрическая емкость, по которой косвенно судили о равномерности заполнения материала наполнителем и стабильности коэффициента отражения при размещении образца в вертикальном положении длительное время. Так же исследовалась зависимость коэффициента отражения модульной конструкции от типа стыка базовых модулей.

АНАЛИЗ ПОМЕХОЗАЩИЩЕННОСТИ УСТРОЙСТВ НАВИГАЦИОННОЙ ИНФОРМАЦИИ

Д.Л. ХОДЫКО, С.Б. САЛОМАТИН

Современные радиоэлектронные системы спутниковой навигации (РЭС СН) различного назначения работают в сложной электромагнитной обстановке и включают в свой состав следящие устройства, позволяющие реализовать когерентную (квазикогерентную) обработку сложных сигналов. Оценка помехозащищенности РЭС СН позволяет оценить уровень защиты системы навигационной информации и целостности навигационного поля от преднамеренных радиоэлектронных воздействий.

Один из эффективных методов радиопротиводействия основан на применении структурированной помехи (СП) сложного вида.

Воздействие преднамеренных помех (ПП) различной мощности неоднозначно. Анализ, на основе компьютерного моделирования, показал, что воздействия ПП на схемы с перекрестными связями слежения за задержкой и фазой оказывает неоднозначное влияние. По результатам моделирования выбран ряд помех по критерию максимума дисперсии оцениваемого параметра. В связи с этим, сформирована группировка ПП, оказывающих наибольшее влияние на кольцо слежения за задержкой и фазой РЭС СН.

ПОДАВЛЕНИЕ РАДИОКАНАЛА ПЛАМЕНЕМ

Н.С. МИСЮКЕВИЧ, Ю.Э. ЯЦКОВСКИЙ

Задача о горении большого количества твёрдотопливных блоков сложной формы в современной физике относится к числу наиболее сложных. Ещё более сложной является задача о прохождении электромагнитных волн через зону подобного горения. Поэтому в качестве первого приближения воспользуемся следующей моделью.

Рассмотрим область размерами 1000×1000×30 м, заполненную воздухом, обогащённую CO_2 и парами воды, в которой взвешены частицы сажи. Температура воздуха ~1000–1500°С. При горении древесины образуются: избыток CO_2, пары H_2O, сажа. Известно, что на 1 га леса имеется до 30 м^3 деловой древесины и такое же количество лесорубных остатков. Сгорание древесины происходит при недостатке кислорода, следствием чего является образование большого количества сажи (не менее 50% углерода, имевшегося в древесине) [1].

В этом случае электромагнитные волны, проходящие через описанную зону, ослабляются вследствие Релеевского рассеивания на нагретом воздухе, поглощения молекулами газов, рассеивания на частицах сажи, поглощения частицами сажи.

Для f=(150–170)×10^6 Гц, произведение $\sigma l \approx 5\times10^{-23}$, т.е. Релеевское рассеивание практически не влияет на прохождение волн с частотой f.

Поглощение молекулами газов для указанных частот существенно не влияет на прохождение радиоволн с частотой f, т.к. даже для видимого диапазона спектра электромагнитных волн подобные потери при $l \approx$(1–10) rv незначительны.

Так как $\sigma_1 N_1 l \approx 1{,}21 \times 10^{-7}$, то и рассеивание на частицах сажи слабо влияет на прохождение радиосигнала (причина — малые размеры частиц по сравнению с длинной волны).

Известно, что электромагнитное излучение ИК диапазона поглощается практически полностью графитовой плёнкой толщиной в несколько атомных слоёв (ангстремов), когда $l_1 \approx (1{,}5–2) \times 10^{-10}$ м [2–4]. Приняв это во внимание и произведя расчёты для $f = (150–170) \times 10^6$ Гц, получено приблизительное значение величины поглощения данного частотного спектра, составившее 30 % потока полезного излучения.

Следует отметить, что реальные потери электромагнитного излучения окажутся большими из-за дифракции и отражения радиоволн от макроскопических потоков взвешенных частиц (восходящие струи дыма и т.п.), особенно с учётом возможной кратковременной электризации сажи в подобных восходящих потоках.

Расчеты дают минимальную картину негативного влияния пламени на прохождение радиосигнала. Полученные значения указывают на необходимость учета этого влияния при тушении крупных пожаров.

Литература

1. Малая советская энциклопедия. Т. 6. М., 1977 г.
2. О. Маделунг. Теория твёрдого тела. М., 1980 г.
3. Ч. Киттель. Квантовая теория твёрдых тел. М., 1967 г.
4. Л. Жирифально. Статистическая физика твёрдого тела. М., 1975 г.

ИЗМЕРИТЕЛИ ФЛУКТУАЦИЙ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ДЛИН ВОЛН

А.Я. БЕЛЬСКИЙ, А.В. ГУСИНСКИЙ, А.Б. ДЗИСЯК, А.М. КОСТРИКИН

В испытательной лаборатории аппаратуры и устройств СВЧ БГУИР разработаны измерители флуктуаций (ИФ) КВЧ сигналов 8-ми и 3-х мм диапазона длин волн (25,86–37,5 ГГц и 78,33–118,1 ГГц соответственно), позволяющие автоматически измерять амплитудные, частотные и вносимые фазовые флуктуации сигналов КВЧ. При измерении амплитудных шумов используется метод прямого детектирования по одноканальной схеме. При измерении частотных флуктуаций КВЧ сигналов используется двухканальная схема измерителя с подавлением несущей. Вносимые фазовые флуктуации измеряются по классической схеме фазового детектора. Передача измерительной информации от ИФ в IBM PC, а также управление ИФ осуществляется с использованием приборного интерфейса КОП (IEEE-488), (опционально USB, RS-232). Применение в качестве базы измерительной системы средств вычислительной техники позволяет автоматизировать значительное число операций: калибровку, самопроверку, выбор пределов измерений, многократное повторение измерений, обработку результатов измерений и др.

Для калибровки измерителей флуктуаций в лаборатории разработаны устройства формирования КВЧ сигнала с образцовой глубиной амплитудной модуляции и образцовым индексом частотной или фазовой модуляции.

Основные технические характеристики, разработанных измерителей флуктуаций, следующие: 1) частота анализа (отстройки) 20 Гц–1 МГц; 2) минимальная
мощность КВЧ сигнала ≥3 мВт при измерении АМ и ФМ шумов, ≥10 мВт

при измерении ЧМ шумов; 3) чувствительность измерения амплитудных шумов на частоте анализа 1 кГц/10 кГц/100 кГц соответственно составляет –125 дБ/–135 дБ/–150 дБ;
4) чувствительность измерения частотных шумов составляет соответственно –80 дБ/–100 дБ/–130 дБ; 5) чувствительность измерения вносимых фазовых флуктуаций –100 дБ/–120 дБ/–140 дБ; 6) основная погрешность измерения составляет ± 3дБ.

КОММУТАЦИОННАЯ СХЕМА ПОСТРОЕНИЯ УСТРОЙСТВА АВТОМАТИЧЕСКОЙ КАЛИБРОВКИ ВЕКТОРНОГО АНАЛИЗАТОРА ЦЕПЕЙ

М.С. СВИРИД

Калибровка векторного анализатора цепей (ВАЦ) является обязательной процедурой при работе с прибором. Процесс традиционной калибровки предполагает многократное подключение требуемых мер к измерительным входам прибора. При этом происходит износ мер и измерительных входов прибора вследствие их многократного соединения. В процессе калибровки не исключены ошибки оператора, которые могут существенно повлиять на результаты измерения.

Одним из путей решения проблем возникающих при калибровке ВАЦ, является использование устройства автоматической калибровки (УАК), позволяющего автоматизировать процесс калибровки, значительно уменьшить время измерений, увеличить точность измерения и степень доверия к результатам измерения. Среди большого количества возможных вариантов построения ВАЦ с возможностью автоматической калибровки нами была выбрана коммутационная схема построения УАК внешней конструкции. Коммутационная схема построения УАК напоминает традиционную калибровку с помощью мер. Переключатели подключают требуемые меры, обеспечивающие режимы, близкие к режимам короткого замыкания, холостого хода, согласованной нагрузки, передачи сигнала на проход. При этом нет необходимости применять меры с параметрами приближенными к идеализированным, что имеет место при традиционной калибровке. Для реализации калибровки достаточно заранее провести достоверные измерения всех состояний УАК.

Анализ показал, что погрешности измерения параметров передачи и отражения, получаемые при использовании УАК соизмеримы с погрешностями в случае применения традиционных калибровочных мер.

АНТЕННЫЕ ИЗМЕРЕНИЯ МОЩНОСТИ ИЗЛУЧЕНИЯ ИНДУСТРИАЛЬНЫХ РАДИОПОМЕХ

Ю.Е. ГУРЛО

Антенные устройства занимают в радиотехнике важное место, так как любая установка, предназначенная для излучения или приема радиоволн, содержит антенну. Широкое применение в технике антенных измерений и измерений характеристик электромагнитного поля находят рупорные антенны благодаря их большой диапазонности и простоте конструкции, так как это определяет существенные достоинства данного типа антенн СВЧ.

Для определения мощности и напряженности электромагнитного поля была разработана методика выполнения измерений мощности излучения индустриальных радиопомех. Методика включает в себя требования к аппаратуре, оборудованию и измерительным антеннам; условия проведения измерений, методики проверки и калибровки измерительной площадки; проведение измерений методом замещения испытуемой установки излучающей антенной, подключенной к генератору синусоидальных сигналов; проведение измерений методом непосредственного измерения плотности потока мощности с помощью измерительной антенны. Проведение измерений по данной методики возможно с помощью разработанного анализатора спектра с диапазоном частот от 0,01 ГГц до 178,40 ГГц, который перекрывается восемью внешними смесителями в 13-ти поддиапазонах. А встроенный в него компьютер, позволяет осуществлять цифровое управление и обработку информации, автоматизированную калибровку, протоколирование результатов измерений, упрощает работу с графиками спектра, представляет полную информацию о форме модулируемых сигналов, стабильности амплитудных и частотных флуктуаций.

Проведенные антенные измерения с использованием анализатора спектра в диапазоне частот 78,33–118,1 ГГц показали, что разработанную методику антенных измерений можно применять при оценке мощности излучения индустриальных радиопомех.

ОПТИЧЕСКИЕ СВОЙСТВА ГЕТЕРОГЕННЫХ ПОГЛОТИТЕЛЕЙ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Т.В. БОРБОТЬКО, ХАЙ НГУЕН ВАН

Противодействие средствам визуально-оптической и оптико-электронной разведки осуществляется как активными, так и пассивными методами. Наиболее экономически выгодным представляется пассивное противодействие, где важнейшим направлением является создание фрагментов естественных сред технологическими методами. Основными критериями, предъявляемыми к таким материалам, являются: широкополосность, высокая эффективность, возможность серийного производства.

Решение данной проблемы может быть найдено путем разработки новых материалов с управляемыми свойствами на основе гетерогенных поглотителей электромагнитного излучения, как наиболее отвечающим выше перечисленным критериям.

На основе машинно-вязаных полотен и порошковых материалов, с использованием технологического наполнителя, были выполнены образцы поглотителей электромагнитного излучения. Их оптические свойства исследовались в лабораторных условиях на гониометрической установке, в качестве источника света использовалась галогеновая лампа, имеющая максимум спектральной плотности энергетической яркости (СПЭЯ) на длине волны 1,0 мкм.

Отраженный свет фиксировался спектрополяриметром при фиксированных углах наблюдения и при положении оси поляроида, относительно вертикальной плоскости, соответствующей 0, 45 и 90^0. По полученным СПЭЯ были рассчитаны яркость отраженного света от образцов и его

степень поляризации для различных углов визирования. Установлено, что использование технологического наполнителя позволяет управлять характеристикой яркости и степени поляризации исходных материалов.

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОТ ПСИХОТРОННЫХ ВОЗДЕЙСТВИЙ

Л.М. ЛЫНЬКОВ, Т.В. БОРБОТЬКО, С.Н. ПЕТРОВ

Под психотронным воздействием понимается коррекция поведенческого архетипа человека с помощью механоэлектронных устройств с цель подчинения данного архетипа командам оператора вышеупомянутых устройств. Принцип действия технических средств (психотронного оружия), способных оказывать психотронное воздействие, основан на генерации электромагнитных, звуковых или торсионных полей, а так же их комбинации в определенном диапазоне частот. Опасность данного воздействия заключается в том, что оно происходит дистанционно без наличия непосредственного контакта объекта, на который оказывается воздействие и самого технического средства. Процесс воздействия, без наличия соответствующего оборудования зафиксировать практически не возможно. Воздействию может подвергаться не только человек в отдельности, но и группы людей.

Цель психотронного воздействия — подавление воли человека к сопротивлению, противодействию, неповиновению, а также уменьшение защитных свойств иммунной системы, ухудшения его самочувствия. Второй этап — воздействие методом нейролингвистического программирования (НЛП) — зомбирование со специальной методикой корректировки побочных факторов. Таким образом, существует возможность дистанционного управления человеком или группой лиц, в результате чего возникает необходимость защиты человека от психотронных воздействий, что может быть обеспечено путем создания защитных материалов и изготовление на их основе специальной одежды и помещений, способных ослаблять вышеназванные физические поля до уровней безопасных для организма человека.

ОБ ОДНОМ СПОСОБЕ ОПРЕДЕЛЕНИЯ ВОСПРИИМЧИВОСТИ ГЕНЕРАТОРОВ СВЧ ПРИ ВОЗДЕЙСТВИИ ПОМЕХ

А.М. БРИГИДИН

Беспрецедентное развитие беспроводных технологий способствовало многократному увеличению числа радиопередающих средств, что заметно усложнило электромагнитную обстановку. В устройствах формирования радиосигналов в современной аппаратуре большое место занимают автогенераторы СВЧ. Эти автоколебательные системы не только весьма чувствительны к помехам, но и, в случае проникновения в них мешающих сигналов, сами могут служить источниками помех. Попадание посторонних воздействий в автогенераторы происходит через цепи нагрузки, питания, синхронизации, управления, вентиляционные отверстия и т.д. Восприимчивость к помехам у автономных генераторов проявляется в виде отклонения рабочих параметров от номинальных, искажения закона модуляции, появления на выходе интенсивных побочных излучений.

В работе получены расчетные соотношения, связывающие параметры помехи и автоколебательной системы. Для оценки способности автогенератора противодействовать влиянию электромагнитных помех введен параметр «восприимчивость генератора». Приведен пример расчета этого показателя при уровне составляющей выходного спектра генератора на частоте помехи по отношению к сигналу автогенерации $P_{\text{п}}$=–30 дБ. Предложены меры по снижению восприимчивости генератора СВЧ к воздействию непреднамеренных помех.

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНЫХ ИСТОЧНИКОВ ЭЛЕКТРОПИТАНИЯ КОМПЬЮТЕРОВ

В.П. ЛУГОВСКИЙ, И.М. РУСАК

Для защиты компьютерной информации и надежного электропитания ПЭВМ обычно рекомендуется использовать источники бесперебойного электропитания. Однако необходимо учитывать, что современное развитие таких источников, а также блоков электропитания ПЭВМ, идет по пути их интеллектуализации и широкого внедрения в их схемы микроконтроллеров. Например, фирма APC использует в своем источнике бесперебойного питания SU/250/600 для управления микроконтроллер типа S87C654-4N40. Значительная номенклатура микросхем микроконтроллеров, специализированных для построения источников вторичного электропитания, также серийно выпускается фирмами Texas Instrument, Maxim Motorola, Unitrode и др.

Несомненно, что применение микроконтроллеров для управления работой источников электропитания, по сравнению с жестким схемным управлением, имеет ряд преимуществ. Так микропроцессорное управление позволяет сравнительно легко решать следующие задачи: обеспечение различных устройств вычислительной системы высококачественными стабилизированными питающими напряжениями разных номиналов и формы; фильтрация и компенсация сетевых и коммутационных помех; защита от перенапряжений, пропадания фазы сетевого напряжения и перегрева в устройствах; осуществление аппаратного мониторинга за параметрами питающей сети и узлов электронной системы; обеспечение коммутации и распределения питающего напряжения по устройствам системы; обеспечение удаленного контроля состояния аппаратных средств электронной системы, а также возможности удаленного обслуживания системы; обеспечение различных режимов работы системы (нормальный, энергосберегающий, ждущий, по программе и т.д.); повышение КПД. и коррекция реактивной составляющей мощности и ее прогнозирование; сигнализация о состояниях работы устройств системы электропитания в нормальном, профилактическом, аварийном режимах работы и прогнозирование их состояния; формирование специальных защитных сигналов при аварийных режимах работы в питающей сети для обеспечения возможности нормального завершения работы всей системы без потери массивов информации.

Вместе с тем, вычислительные системы и ПЭВМ, с точки зрения защиты информации, оказываются более уязвимыми по сравнению с использованием в них вторичных источников электропитания и источников бесперебойного электропитания, выполненных по традиционным схемам.

Наличие в репрограммируемой памяти микроконтроллеров специального программного обеспечения для управления источниками повышает риск нарушения информации (аппаратные и программные закладки, вирусы и т.п.). Положение усугубляется также тем, что возможно прямое электромагнитное воздействие на источник через вентиляционные отверстия устройства охлаждения, что, как правило, невозможно при использовании в системе закрытого металлического корпуса.

В докладе рассматриваются возможные конструктивные и другие способы защиты информации в компьютерах с интеллектуальными источниками электропитания.

МЕТОД КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ВИДЕОИНФОРМАЦИИ В СРЕДСТВАХ ОБРАБОТКИ ДАННЫХ

А.В. ХИЖНЯК, А.В. ИГНАТЧЕНКО

Предлагаемый метод криптографической защиты видеоинформации может быть использован для создания защищённых средств обработки данных (СОД) от утечки информации за счёт побочного электромагнитного излучения (ПЭМИ).

Прохождение электрических сигналов по цепям средства обработки данных и соединительным кабелям сопровождается возникновением побочных электромагнитных излучений в окружающей среде. Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств контроля. В СОД, как например, персональная ЭВМ (ПЭВЭМ), основными источниками электромагнитных излучений являются устройства ввода и вывода информации совместно с их адаптерами (монитор, принтер, клавиатура, печатающее устройство и т.д.), а также центральный процессор. Утечке информации в ПЭВМ способствует применение коротких видеоимпульсов прямоугольной формы и высокочастотных коммутирующих сигналов. Исследования показывают, что излучение видеосигнала монитора является достаточно мощным, широкополосным и охватывает диапазон метровых и дециметровых волн.

Для уменьшения уровня побочных электромагнитных излучений применяют специальные средства защиты информации — экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений и наводок при помощи различных резистивных и поглощающих согласованных нагрузок.

В отличие от известных методов и средств защиты информации от утечки за счёт ПЭМИ, предлагаемый метод позволил создать модель системы криптографической защиты видеоинформации в СОД с секретной передачей ключа, обеспечивающей теоретическую стойкость шифра по Шеннону, что позволяет с уверенностью говорить о несостоятельности решения при криптоанализе. Использование данного метода позволяет впервые не говорить о контролируемой территории для данного канала утечки, так как её значение сводится к нулю. Отсутствует также необходимость в использовании экранирующих материалов и всевозможных фильтрующих устройств в канале передачи видеоинформации.

Важным достоинством метода является так же то, что он позволяет создать модель криптосистемы, которая не только защищает видеоинформацию в средствах обработки данных, но и осуществляет информационное противодействие по каналу ПЭМИ, в целях полного или частичного дезинформирования злоумышленника.

РАЗРАБОТКА СРЕДСТВ ИМИТАЦИИ НАЗЕМНЫХ ОБЪЕКТОВ

Л.М. ЛЫНЬКОВ, С.С. КУЗНЕЦОВ, Т.В. БОРБОТЬКО

Для повышения эффективности мероприятий по маскировке наземных объектов целесообразно использовать ложные объекты путем применения средства их имитации. Основные требования, предъявляемые к таким средствам: размер макета наземного объекта должен быть идентичный настоящему объекту, макет должен имитировать объект в видимом инфракрасном и радиолокационном диапазонах длин волн и иметь соответствующие спектральные характеристики и аналогичную эффективную площадь рассеяния, низкие стоимость и время развертывания.

Перспективной представляется разработка макетов наземных объектов на основе волокнистых материалов, содержащих проводящий технологический наполнитель, имеющий высокий коэффициент отражения электромагнитного излучения радиолокационного диапазона. Такой материал, окрашенный в защитный цвет, может быть закреплен на разборном каркасе, имитирующем силуэт наземного объекта в видимом диапазоне. Имитация в ближнем инфракрасном (ИК) диапазоне может быть достигнута за счет использования технологического наполнителя, который способен эффективно отражать электромагнитное излучение как радиолокационного, так и ближнего ИК диапазона.

Получение спектральных характеристик в среднем ИК (тепловом) диапазоне идентичных имитируемому объекту может быть достигнуто за счет применения, например, каталитических печей типа КФП-1-180 или тепловых имитаторов КТИ, размещенных внутри макета. Для повышения вероятности принятия макета за действующий наземный объект, могут быть использованы дополнительные технические устройства, для придания макету демаскирующих признаков, например, устройства имитации работающих двигателей, систем связи и т.д.

СКРЫТИЕ НАЗЕМНЫХ ОБЪЕКТОВ В ШИРОКОМ ДИАПАЗОНЕ ДЛИН ВОЛН

В.М. ПАРКУН, С.С. КУЗНЕЦОВ, Т.В. БОРБОТЬКО

Разработка новейших технологий в области микроэлектроники позволили создать комбинированные средства технической разведки с высокой разрешающей способностью, имеющие несколько каналов обнаружения (визуально-оптический, инфракрасный, радиолокационный), способные на больших дальностях обнаруживать, распознавать и измерять характеристики наземных объектов с высокой достоверностью. В результате чего использование естественных сред и существующих технических средств скрытия, для маскировки наземных объектов на данном этапе, представляется малоэффективным, что остро ставит проблему разработки

маскировочных материалов, способных оказывать высокоэффективное противодействие существующим и перспективным средствам технической разведки.

Важнейшей задачей при разработке подобных материалов является создание высокотехнологичных изделий, имеющих параметры аналогичные окружающей среде, низкую стоимость при их промышленном производстве и малое время развертывания.

Эта задача может быть решена путем разработки базового модуля площадью 1-1,5 м^2. Между собой модули соединяются внахлест, что делает такой материал легко транспортабельным и сокращает время необходимое для маскировки одного объекта. В качестве основы для таких материалов можно использовать капиллярно-пористые матрицы выполненные методом машинной вязки с поверхностной плотностью 1000 г/м^2 и более, заполненных технологическим наполнителем.

Материал для скрытия наземных объектов может содержать несколько слоев с градиентом распределения технологического наполнителя по его объему, что позволит получить низкий коэффициент отражения в радиолокационном диапазоне и высокое поглощение оптического излучения инфракрасного диапазона. Скрытие в видимом диапазоне длин волн может быть обеспечено за счет деформирующей окраски поверхности материала под цвет окружающего фона.

ВЛИЯНИЕ РАСТВОРНЫХ НАПОЛНИТЕЛЕЙ ГИБКИХ РАДИОПОГЛОЩАЮЩИХ МАТЕРИАЛОВ НА ЭФФЕКТИВНОСТЬ ПОДАВЛЕНИЯ ЭЛЕКТРОМАГНИТНОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ

В.А. БОГУШ, О.И. ЗУБАРЕВИЧ, Н.В. КОЛБУН, А.А. ПОЗНЯК

Современные средства подавления электромагнитного излучения (ЭМИ) основаны на использовании различных радиопоглощающих материалов, включая композиционные, и конструкций электромагнитных экранов. Специфические свойства воды и водных растворов, возможность получения заданных электрических характеристик растворов за счет изменения концентрации и природы растворяемого электролита обусловили перспективность применения растворных наполнителей в конструкциях гибких радиопоглощающих материалов.

Исследовано влияние природы и концентрации компонент водных растворов на коэффициент отражения и ослабление ЭМИ волокнистыми матрицами с максимальным влагосодержанием, составляющем 1,667 мл/г. В качестве капиллярно-пористой матрицы использовалось полотно из полиакрилонитрильных волокон с поверхностной плотностью 1313 г/м^2. Для пропитки матриц использовали дистиллированную воду, 0,1 М растворы сульфосалициловой, щавелевой, малоновой, винной, лимонной и борной кислот; 0,1 и 1 М растворы хлоридов натрия и калия, гексацианоферрата (III) калия; 0,1 и 0,4 М растворы бихромата калия. Для снижения испарения жидкости с поверхности образцов и стабилизации их свойств после пропитки, производили герметизацию с использованием многослойных полиэтиленовых пленок.

Коэффициенты передачи и отражения ЭМИ исследовали в диапазонах частот 8…11,5; 38…55,4 и 78…118 ГГц. С помощью панорамных измерителей коэффициентов стоячей волны по напряжению и ослабления с волноводным измерительным трактом и векторный анализатор

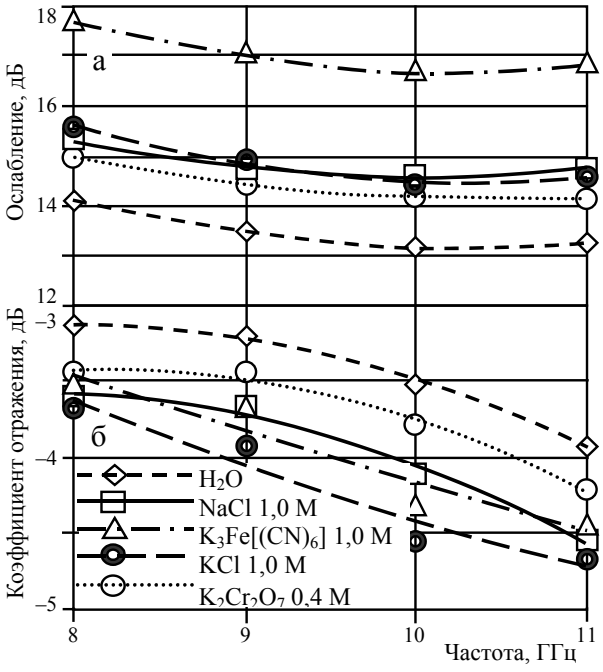


Рис. Частотные зависимости ослабления (а) и коэффициента отражения (б) растворосодержащих волокнистых матриц.

волноводным измерительным трактом и векторный анализатор параметров четырехполюсников. Образцы размещали внутри волновода или между рупорными антеннами.

Как показывают исследования во всех частотных диапазонах, свойства гибких экранов на основе волокнистых матриц, пропитанных дистиллированной водой и разбавленными растворами кислот, различаются несущественно, что объясняется доминирующим влиянием растворителя, обладающим высоким коэффициентом подавления ЭМИ. Это приводит к снижению измеряемого сигнала до уровня собственных шумов измерительного оборудования. Установлено, что при увеличении концентрации растворенной соли для всех образцов уменьшается максимальное значение коэффициента передачи, что соответствует повышению эффективности экранирования.

Наименьшим коэффициентом отражения обладают полотна, пропитанные раствором $K_2Cr_2O_7$, причем при увеличении концентрации растворяемой соли коэффициент отражения уменьшается, что указывает на увеличение коэффициента поглощения ЭМИ.

Показано, что растворосодержащие композиционные структуры обладают высокой эффективностью подавления ЭМИ в СВЧ диапазоне и перспективны для подавления нежелательных электромагнитных излучений средств обработки информации.

ПОДАВЛЕНИЕ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ КОМПОЗИЦИОННЫМИ ЭКРАНИРУЮЩИМИ ПОКРЫТИЯМИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ СВЯЗИ

Е.С. ПУЛКО, В.А. БОГУШ

В связи с бурным развитием локальных и глобальных сетей связи, связанным с увеличением объема и скорости передаваемой по ним данных, актуальной становится задача обеспечения конфиденциальности информационного обмена. В случае высокой защищенности сети на программно-аппаратном уровне часто используются методы добывания информации, не связанные с необходимостью проникновения в локальную сеть. В связи с этим в последнее время активно развиваются методы перехвата информации по каналам побочных излучений и наводок (ПЭМИН) элементов локальной сети. Для обеспечения информационной безопасности особую актуальность приобретает разработка средств подавления

электромагнитных излучений, к которым относятся электромагнитные экраны и радиопоглощающие покрытия.

Методика защиты отдельных компьютеров достаточно хорошо проработана, подкреплена необходимыми нормативными документами. Задача же защиты информации от утечки по каналам ПЭМИН в сетях связи существенно сложнее, чем для автономно используемых устройств. Источниками электромагнитных излучений в сетях связи являются, безусловно, рабочие станции (компьютеры) и активное сетевое оборудование.

Например, современная техника позволяет восстановить изображение на мониторе, принятое после многократных отражений его от стен и всех предметов. Излучение монитора не является единственным каналом утечки, излучают большинство элементов компьютера, и в большинстве случаев излучение этих элементов может содержать ценную информацию.

Для снижения уровня электромагнитного излучения активного оборудования применяются экранированные шкафы и помещения. В конструкции таких шкафов применяются специальные меры по улучшению экранирующих свойств, связанные с обеспечением электрической однородности, благодаря чему достигается ослабление радиочастотных сигналов свыше 80 дБ на частоте 30 МГц. На более высоких частотах уровень ослабления лежит в пределах от 40 до 70 дБ.

Хорошей практикой является размещение в этих же шкафах и серверов. Иногда в таких шкафах можно разместить и компьютеры. Однако чаще компьютеры устанавливаются на рабочих местах и, соответственно, приходится полагаться на экранирующие свойства их корпусов, которые часто не обеспечивают требуемого подавления сигнала. Более того, качество экранирования корпуса системного блока компьютера влияет на уровень излучения всех устройств, подключенных к системному блоку. Повышение рабочей частоты современных вычислительных систем приводит к необходимости расширения диапазона рабочих частот экранов. Практическая задача доработки стандартных корпусов, шкафов и линий связи, пусть даже с улучшенными характеристиками по электромагнитной совместимости, оказывается достаточно сложной и требует применения специальных материалов и конструктивных решений.

Повышение эффективности экранирования достигают за счет применения композиционных покрытий с улучшенными электрическими и магнитными характеристиками. Одним из перспективных высокотехнологичных способов получения таких покрытий является осаждение металлов из водных растворов. Разработана технология формирования на поверхности диэлектрических материалов и металлов композиционных покрытий серебра с вольфрамом с повышенной удельной электропроводностью и стабильностью при эксплуатации на воздухе, что позволило повысить эффективность экранирования элементов конструкции и расширить диапазон рабочих частот экранов. Показано, что метод формирования композиционного покрытия из водного раствора легко адаптируется для совершенствования стандартных конструктивных элементов сетей и устройств связи.

КОМБИНИРОВАННЫЕ ГИБКИЕ ПАНЕЛИ ДЛЯ БИОЛОГИЧЕСКОЙ ЗАЩИТЫ ОРГАНИЗМА ОТ ЭЛЕКТРОМАГНИТНЫХ И АКУСТИЧЕСКИХ ВОЗДЕЙСТВИЙ

А.М. ПРУДНИК, Н.Е. АЛЕХИНА, Ю.В. СМИРНОВ, Г.А. ВЛАСОВА, С.Н. ПЕТРОВ

В современном мире наряду с бурно развивающейся техникой все острее становится проблема формирования электромагнитной обстановки, обеспечивающей нормальное функционирование электронных устройств и биологически опасные условия труда. Электромагнитная обстановка представляет собой совокупность электромагнитных полей в заданной области пространства, которая может влиять на функционирование конкретного радиоэлектронного устройства или биологического объекта.

Исследованиями выявлена восприимчивость человеческого организма даже к самым слабым электрическим и магнитным полям, не говоря уже о более мощных излучениях, исходящих от мониторов компьютеров, телевизоров, мобильных и радиотелефонов. Дозированное воздействие слабых уровней ЭМИ широко используется в медицинских целях. Однако техногенные излучения, проникая в биологический объект, воздействуют на организм на межклеточном уровне, вызывая в организме различные нарушения, и, как следствие, заболевания. Особенно чувствительна к воздействию вредных излучений центральная нервная система человека.

ЭМИ могут вызывать заболевания нервной, сердечно-сосудистой, дыхательной систем, изменять показатели крови, обмена веществ. При длительном воздействии СВЧ излучений могут иметь место изменения в крови, помутнение хрусталика глаза, нервно-психологические заболевания, нарушение работы механизмов адаптации организма к изменениям условий внешней среды, а при увеличении энергии излучений — к нагреванию тканей, ожогам [1].

В целях биологической защиты организма человека от электромагнитных и акустических воздействий перспективным направлением является использование комбинированных гибких панелей поглотителей ЭМИ на основе растворосодержащих волокнистых материалов [2, 3]. Их преимущество заключается в обеспечении высокого коэффициента ослабления при невысоком уровне отражаемого сигнала. При этом ослабление электромагнитной энергии происходит в результате вносимых диэлектрических потерь жидкой среды, а снижение коэффициента отражения — за счет гидродисперсной структуры поглощающего материала. С другой стороны применение комбинированных конструкций поглотителей позволяет повысить общие характеристики за счет улучшения согласования параметров материала и свободного пространства в первом слое и высокой эффективности экранирования второго слоя [4].

Литература

1. Григорьев Ю.Г., Григорьев О.А. Персональный компьютер: физические факторы воздействия и здоровье пользователя // Энергия: Экон., техн., экол. – 1999. – N 7. – С.29-33; N 8. – С.29-33.
2. Лыньков Л.М., Борботько Т.В., Колбун Н.В. Прудник А.М. Гравиметрическое исследование временной стабильности жидкостносодержащих поглотителей ЭМИ // Доклады Белорусского государственного университета информатики и радиоэлектроники. — 2004. — № 5. — С. 48-50.
3. Лыньков Л.М., Колбун Н.В., Прудник А.М. Физические основы моделирования процесса пропитки капиллярно-пористых материалов для жидкостно-содержащих экранов ЭМИ // Известия Белорусской инженерной академии. — 2003. — № 4. — С. 133-135.акустика,
4. Украинец Е.А., Колбун Н.В. Экранирующие свойства многослойных конструкций электромагнитных экранов на основе материалов с малоразмерными включениями металлов и жидких сред // Доклады БГУИР. 2003. Т. 1, №4. С.118–122.

УСТАНОВКА ДЛЯ ИЗМЕРЕНИЯ ДИНАМИЧЕСКИХ СИЛ, РАЗВИВАЕМЫХ ЭЛЕКТРОАКУСТИЧЕСКИМИ ПРЕОБРАЗОВАТЕЛЯМИ УСТРОЙСТВ АКУСТИЧЕСКОГО МАСКИРОВАНИЯ РЕЧЕВЫХ СИГНАЛОВ

В.И. ВОРОБЬЕВ, Г.В. ДАВЫДОВ

Для защиты помещений от несанкционированного прослушивания действующих в них речевых сигналов широко используется маскирование этих сигналов различного рода акустическими помехами. Последние излучаются устанавливаемыми на стенах и оконных стеклах защищаемых помещений различного рода электроакустическими преобразователями (ЭАП). На ЭАП со специальных генераторов подаются электрические колебания со спектрами в частотном диапазоне речевых сигналов.

Для обеспечения эффективности защиты речевых сигналов весьма важно оценивать развиваемые применяемыми ЭАП в диапазоне частот 160–4000 Гц динамические силы.

Сравнение различных ЭАП по развиваемым ими в одинаковых условиях динамическим силам позволяет осуществлять созданная в БГУИР измерительная установка. Основу установки составляет аттестованный датчик динамических сил ДС-100 с подсоединенным к его выходу измерительным усилителем с входным сопротивлением 100 МОм. Датчик имеет коэффициент преобразования 12,5 мВ/Н в диапазоне сил 0,1–2 Н на частотах 160–4000 Гц. ЭАП посредством резьбового соединения жестко закрепляется на одном из торцов ДС-100, вторым торцом, имеющим вид кругового фланца, датчик шестью болтами прочно присоединяется к инерционной цилиндрической стальной массе в 16 кг.

С генератора сигналов специальной формы типа Г6–28 через усилитель мощности LV-102 на исследуемый ЭАП подается гармонический сигнал на заданной частоте. Уровень возбуждения контролируется милливольтметром В3-55.

Проведенные исследования ЭАП различных типов показали, что у многих из них на частотах около 1000 Гц имеются зоны резкого (в десятки раз) увеличения развиваемых усилий при неизменном уровне возбуждения, что определенно является недостатком таких ЭАП.

СЕКЦИЯ 3. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

ПРИМЕНЕНИЕ ТЕОРЕМЫ БАЙЕСА ПРИ ПОСТРОЕНИИ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА БАЗЕ КЛАВИАТУРНОГО ПОЧЕРКА

А.В. БОКУНОВИЧ, Л.И. МИНЧЕНКО, Е.В. ХАРИТОНЕНКОВ

Основной задачей обеспечения безопасности информационных компьютерных систем является задача ограничения круга лиц, имеющих доступ к конкретной информации и защита ее от несанкционированного доступа. Отождествление пользователя ЭВМ - задача, решение которой позволяет организовать весь процесс управления правами доступа, а также реализовать ряд других вспомогательных задач, имеющих самостоятельное прикладное значение. На сегодня одним из самых перспективных способов идентификации пользователя является идентификация по клавиатурному почерку, так как она не требует установки ни какого дополнительного оборудования и соответственно дешева во внедрении.

Суть метода статистической фильтрации состоит в применении математической теоремы Байеса к времени между нажатиями известных буквенных сочетаний и позволяет вычислить вероятность успешного совершения некоторого события на основании статистики совершения этого события в прошлом.

В нашем случае весь процесс набора текста будет разбиваться на токены (время нажатий комбинаций по 2 и 3 клавиши), вероятности которых будут использоваться для нахождения общей оценки клавиатурного почерка с учетом времени суток. Что позволяет существенно улучшить эффективность оценки и практически довести эффективность фильтра до 98 %.

ЗАЩИТА РЕЧЕВЫХ СООБЩЕНИЙ НА ОСНОВЕ ПСЕВДОСЛУЧАЙНЫХ И ОДНОРОДНЫХ ПЕРЕСТАНОВОК

А.А. БОРИСКЕВИЧ, А.Ю. ЛАГОЙКО

Известные методы блочного скремблирования речевого сигнала (РС) во временной области не обеспечивают нулевой разборчивости, сохранения ширины спектра и высокой криптостойкости. Для устранения этих недостатков предлагаются два алгоритма скремблирования РС во временной области, основанные на псевдослучайных и однородных перестановках речевых отсчетов, позволяющие управлять соотношением остаточной разборчивости, криптостойкости и времени задержки. Алгоритмы псевдослучайных и однородных перестановок основаны на формировании с использованием секретных ключей криптографических матриц размером, определяемым длительностью кадра, и состоящие из нулей и единиц, позиции последних задают новое расположение отсчета РС в кадре. В случае однородных перестановок на передающей и приемной стороне секретные ключи представляют собой взаимообратные числа по модулю,

равным размеру кадра. Для метода псевдослучайных перестановок множество секретных ключей определяется количеством примитивных полиномов и разрядностью регистра сдвига с линейной обратной связью. Для алгоритмов скремблирования исследована зависимость остаточной разборчивости и времени задержки от длительности кадра, и установлено, что оба алгоритма обеспечивают минимальную алгоритмическую задержку и нулевую разборчивости РС при минимальном размере кадра РС. Определено, что ширина спектра скремблиро-ванного РС не изменяется, а характер спектра приближается к равномерному распределению частотных составляющих с увеличением длительности кадра. Преимущество алгоритма однородных перестановок для решения задач скремблирования состоит в том, что количество возможных секретных ключей увеличивается значительно быстрее с ростом числа отсчетов в кадре, чем для псевдослучайных перестановок, Кроме того, он обеспечивает более высокую временную криптостойкость и минимальное время задержки при минимальном размере кадра РС. Моделирование процесса скремблирования и дескремб-лирования проведено в среде программирования MATLAB.

СИНТЕЗ И АНАЛИЗ ХАОТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ЛИНЕЙНЫХ И НЕЛИНЕЙНЫХ МЕТОДОВ

А.А. БОРИСКЕВИЧ, А.А. МЕРКУШОВ

В настоящее время отсутствуют средства для эффективной оценки и улучшения параметров генераторов криптографических последовательностей на основе динамических хаотических систем, основной особенностью которых является существенная зависимость от начальных условий. Оценка параметров хаотических последовательностей имеет ряд особенностей, заключающихся в необходимости использования сочетания линейных и нелинейных методов тестирования. Предлагаются алгоритмы модификации для улучшения свойств хаотических последовательностей и набор взаимосвязанных тестов для анализа их параметров. Тестирование заключается в использовании дополняющих друг друга трех классов оценок. На основе результатов первого класса оценок, основанного на построении бифуркационной диаграммы, показателя Ляпунова, фрактальных размерностей, осуществляется синтез и выбор хаотических последовательностей с требуемыми криптографическими свойствами. Второй класс оценок, определяющий параметры синтезированных последовательностей в частотной, временной и пространственной областях., предназначен для принятия окончательного решения о возможности использования синтезированных последовательностей в задачах передачи и защиты данных. Третий класс, определяющий временную динамику изменения параметров последовательностей, прошедших два предыдущих уровня тестирования, позволяет оценить непредсказуемость структуры последовательности по ее сегменту ограниченной длинны.

БЕЗОПАСНОЕ ПРОГРАММИРОВАНИЕ НА ЯЗЫКАХ СЕРВЕРНЫХ СЦЕНАРИЕВ PEARL И PHP

А.Л. ГАРЦУЕВ, А.В. БОРЗЕНКОВ

Языки PHP и Pearl являются одними из самых популярных средств написания серверных сценариев. Данные языки применяются в основном на небольших сайтах и часто применяются для единичного использования, что не повышает их безопасности.

Основной и наиболее частой уязвимостью серверных сценариев является недостаточная проверка входных данных. Основные уязвимости характерные для сценариев на языке Peri связаны с командой открытия файлов - open(), где имя открываемого файла содержит переменную, значение которой получено от пользователя. Символ с кодом %00 интерпретируется в Peri как признак конца строки. Ели этот символ не отфильтрован, то может быть использован для отсечения ненужного расширения в имени файла или отсечения SQL-запроса.

Для сценариев на языке PHP характерны уязвимости при записи в файл с расширением "php" или вставка в исходный код файлов, имена которых образуются из данных, полученных от пользователя.

SQL-базы данных, взаимодействующие с пользователем через серверные сценарии, написанные на любом языке программирования, могут быть прочитаны или изменены с помощью SQL-инъекций.

В работе подробно рассматриваются уязвимости серверных сценариев с недостаточной проверкой входных данных, приведены примеры подобных сценариев и методы устранения уязвимостей.

ВЫЧИСЛЕНИЕ КОМПЛЕКСНОГО КОЭФФИЦИЕНТА ПЕРЕДАЧИ СВЧ ЧЕТЫРЕХПОЛЮСНИКА В УЗКОЙ ПОЛОСЕ ЧАСТОТ

В.В. ВЕЛИЧКОВСКИЙ

Как известно, действительная и мнимая составляющие комплексного коэффициента передачи линейного четырехполюсника связаны через интегральное преобразование Гильберта. Задача состоит в вычислении комплексного коэффициента передачи по известной его вещественной составляющей. В реальных условиях действительная составляющая задается на отрезке. Это приводит к появлению существенной ошибки преобразования, особенно на концах отрезка. При дискретном задании вещественной составляющей интегральное преобразование вырождается в дискретное преобразование Гильберта (ДПГ). Оптимизируя коэффициенты ДПГ можно снизить ошибку преобразования на срединной части отрезка, но на концах она остается существенной. Учитывая, что преобразуемая функция является низкочастотной, была выполнена ее экстраполяция влево и вправо с использованием интерполяционного полинома Лагранжа. Как показало моделирование, этим способом удается экстраполировать вещественную составляющую на 10–15 точек в обе стороны, что в сочетании с оптимизированными коэффициентами существенно снижало ошибку преобразования на концах отрезка.

МЕТОДЫ ЗАЩИТЫ SWF-ФАЙЛОВ ОТ ДЕКОМПИЛЯЦИИ

В.С. БАЕВ, И.В. ДАЙНЯК

Одним из широко распространенных средств для разработки небольших мультимедийных роликов является среда разработки Flash MX, разработанная фирмой Macromedia. Среда позволяет разрабатывать и воспроизводить с помощью специальной программы Flash-Player короткие анимации на основе векторной графики.

Рабочим форматом среды Macromedia Flash MX является формат FLA, в котором описываются все элементы и сцена, а последовательность анимации задается либо по кадрам, либо программированием на специальном языке Action Script. Выходным форматом является формат SWF, который и воспроизводится с помощью Flash-Player.

Задачу защиты SWF-файла можно сформулировать так: обеспечить невозможность получения элементов сцены и исходных текстов программ, или сделать их искаженными и бессмысленными для взломщика.

Стандартная методика защиты, которую предлагает фирма Macromedia, — это пароль для предотвращения импорта SWF-файла в среде Flash MX. Но этот способ защиты очень легко обойти.

Нестандартные методы взлома реализованы специальными программами-декомпиляторами, которые размещены в сети Интернет. Примерами данных программ являются: Flash Decompiler, Movies Extractor, SWF Scanner, Sothink SWF Decompiler, Action Script Viewer. Эти программы позволяют извлечь из SWF-файла любые его элементы, такие как звуки, графика, текст, изображения, и, самое главное, управляющие программы.

Методами защиты от программ-взломщиков являются специально разработанные в этих целях программы. Например, Action Script Obfuscator (ASO), Flashincrypt, и др. Эти программы преобразуют элементы SWF-файла так, что программа-взломщик получает в результате список бессмысленных графических элементов и модифицированные программы с бессмысленными идентификаторами и функциями.

ЗАЩИТА МУЛЬТИМЕДИЙНОГО КОНТЕНТА СЕТЕВОЙ ИНТЕРАКТИВНОЙ МУЛЬТИМЕДИЙНОЙ ОБУЧАЮЩЕЙ СИСТЕМЫ

И.В. ДАЙНЯК, В.С. БАЕВ, С.Е. КАРПОВИЧ

В лаборатории Математического моделирования технических систем и информационных технологий БГУИР разрабатывается Сетевая Интерактивная Мультимедийная Обучающая Система (СИМОС), которая предназначена для самообучения, дистанционного обучения или самостоятельной работы без непосредственного участия преподавателя.

Основным элементом СИМОС является интерактивная мультимедийная страница, элементами которой могут быть текст, рисунки и интерактивные элементы на основе управляемой анимации. Элементы страниц хранятся в базе данных, а описание структуры страниц осуществляется с помощью форматов HTML и XML. Интерактивные мультимедийные элементы разрабатываются в среде Macromedia Flash MX, выходным форматом которых является формат SWF.

Защиту мультимедийного контента СИМОС предлагается строить на нескольких уровнях: 1) *уровень хранения*; 2) *уровень сервера*; 3) *уровень клиента*.

Первые два уровня защиты обеспечиваются программными средствами СУБД и сервера СИМОС через авторизацию пользователей и контроль доступа к системе.

Наиболее важным вопросом является обеспечение защиты на стороне клиента: предотвращение работоспособности интерактивных мультимедийных страниц без подключения к серверу СИМОС, в обход первых двух уровней, и обеспечение невозможности декомпиляции страниц, так как пользователь может загрузить страницу и скопировать ее на другой компьютер. Для решения этого вопроса предлагается проверка обязательного соединения с сервером после запуска страницы и обеспечение неработоспособности мультимедийного элемента при отсутствии подключения (текст и статические рисунки имеют второстепенное значение, поскольку их можно посмотреть в книгах и печатных изданиях). Для предотвращения декомпиляции страниц предлагается использовать специальные программные средства, преобразующие мультимедийный контент и встроенные в него программы.

ПОВЫШЕНИЕ НАДЕЖНОСТИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ ВРЕМЕННЫХ ХАРАКТЕРИСТИК ПРОЦЕССА ШИФРОВАНИЯ

Е.А. КАРАСИК

Криптографическая защита является в настоящее время важным аспектом обработки информации. Стойкость большинства применяемых шифров основывается на секретности ключа, используемого для расшифровки, сам же шифрующий алгоритм предполагается известным. Следовательно, криптосистема поддается взлому путем перебора ключей, причем технические возможности для этого со временем расширяются, а при использовании в качестве ключа осмысленных комбинаций символов, например, вводимых пользователем паролей, эффективность перебора возрастает многократно. Криптостойкость повышается последовательным применением нескольких различных, в том числе динамически сменяемых ключей либо комбинированием нескольких способов генерации составного ключа. Эффективным средством противодействия могло бы стать также принципиальное ограничение минимального времени одной попытки предъявления подбираемого ключа.

Автором предлагается следующий подход к повышению надежности криптографических систем: в состав комбинированного ключа шифрования включается элемент, генерируемый способом, зависящим от времени, т.е. ключ шифрования с заданной временной периодичностью, меняется по секретному алгоритму. Главное свойство этого алгоритма заключается в защищенности от взлома и воспроизведения. Этого можно достичь несколькими способами: использование сложных математических алгоритмов, понижающих читаемость дизассемблированного кода, а также использование функций реального времени в качестве аргументов алгоритма, тем самым, усложняя отладку запущенного приложения.

В работе рассматриваются варианты применения данного подхода к практическим задачам, а также различные подходы к усложнению взлома секретного алгоритма.

АВТОМАТИЗИРОВАННОЕ ПРОЕКТИРОВАНИЕ СИСТЕМ С ФАЗОВЫМ УПРАВЛЕНИЕМ

А.П. КУЗНЕЦОВ, Д.А. ГАНЬШИН, Л.В. РУСАК, А.А. СЕДУШКИН, Х.А. АЛЬКАТАУНА.

Среди множества систем автоматического управления, нашедших широкое применение в современных средствах связи и радиотехники, следует особо выделить класс систем с фазовым управлением (СФУ). Работая на больших частотах, эти системы автоматического управления показывают высокие точностные характеристики.

С целью автоматизации решении задач синтеза данных систем было разработано программное обеспечение (ПО) макропроектирования систем с фазовым управлением.

Рассмотрим алгоритм, лежащий в ее основе.

Принцип работы строится на предварительном выборе параметров системы с фазовым управлением по линеаризованной модели с последующим уточнением по нелинейной.

В базу данных ПО уже входят модели и принципиальные электрические схемы типовых узлов систем с фазовым управлением: сравнивающих устройств, операционных усилителей, фильтров, генераторов, делителей и т.п. Есть возможность подключения библиотек описания новых устройств. Проектирование начинается с выбора структурной схемы системы и задания разработчиком начальных значений параметров: коэффициентов передачи и постоянных времени основных блоков. Затем производится построение в плоскости двух параметров системы областей синхронизации, устойчивости, качества по быстродействию и шумам. Пользователь имеет возможность выбора более удобной для восприятия формы графического представления информации.

В целях экономии машинного времени расчет, и построение областей производятся по линеаризованным моделям. Так как это только предварительный этап в общем процессе синтеза СФУ, — требований к высокой точности здесь не предъявляется. В случае системы высокого порядка предусмотрена программа выдачи оптимальных параметров системы.

Далее полученные предварительные оценки, уточняются по нелинейным моделям. Строится переходный процесс, проверяются его длительность, устойчивость СФУ, а также определяются полосы захвата, удержания и т.п.

ПО было разработано в среде Visual Studio 6.0. с применением динамический библиотек пакета автоматизации инженерных расчетов MatLab 6.0.

ПСЕВДОСТОХАСТИЧЕСКИЕ НЕЙРОННЫЕ СИСТЕМЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

В.М. КОЛЕШКО, Ю.Д. КАРЯКИН

Существенный прогресс в области интеллектуальных систем достигнут в связи с развитием нейронных сетей, теории эволюционной оптимизации и генетических алгоритмов. Эти современные технологии обеспечивают высокую эффективность, так как основаны на стохастичности большинства лежащих в их основе алгоритмов. Однако стохастические нейронные сети и построенные на их основе интеллектуальные системы имеют два основных существенных недостатка:

1) неравномерное начальное распределение в многомерном пространстве весовых векторов, что приводит к резкому увеличению времени обучения сети;

2) случайный характер весовых векторов не позволяет использовать быстрые алгоритмы умножения входного вектора на матрицу весов.

Нейронная сеть обработки и защиты информации требует огромного количества операций для процедуры обучения и становится практически не реализуемой. Ситуация совершенно меняется, если в качестве начального множества векторов использовать не случайные, а псевдослучайные последовательности, т.е. псевдостохастические нейронные сети. На примере малогабаритного мобильного комплекса для сейсмической разведки полезных ископаемых и глубоко залегающих объектов рассмотрена эффективность и красота технического решения псевдостохастической нейронной системы обработки и защиты информации.

ИДЕНТИФИКАЦИЯ АВТОРА ЭЛЕКТРОННОГО ПРОДУКТА

С.А. ТЫКОЦКИЙ

Проблема идентификации автора вредоносного кода и доказательство принадлежности кода определенному автору — главная задача нашего исследования.

Вирусы, "трояны", взлом программного обеспечения с каждым годом наносят все больший урон компьютерной индустрии. Как найти виновного? Как доказать его вину? Типичными уликами, остающимися после атаки, является исполняемый модуль или исходный код. Оба случая требуют различного подхода при их анализе.

В работе проведены исследования по определению характерных признаков электронных продуктов на примере исходных кодов программ и исполняемых модулей. Лингвистическая и стилистическая составляющие являются наиболее показательными для статистического анализа, позволяют наиболее точно идентифицировать субъекта. Сама же идентификация производится не по одному из признаков, а по их совокупности.

В случае работы с исходными кодами мы имеем достаточно большие возможности для идентификации автора. Отождествление может быть осуществлено по следующим признакам, которые различны для каждого субъекта: форматирование исходного кода, стиль написания комментариев, именование переменных, грамматические ошибки при объявлении переменных и написании комментариев, степень владения автора возможностями языка программирования, использование нулевых ветвей

в коде программы, типичные ошибки, допущенные при кодировании программы.

В случае работы с исполняемыми модулями возможности анализа заметно сокращаются, вследствие преобразования исходного кода на стадии компиляции. Однако и в данном случае существуют методы и характеристики, позволяющие идентифицировать автора: анализ структур данных и алгоритмов, ошибки, допущенные при разработке, системные вызовы, уровень знания языка программирования и операционной системы, компилятор, используемый при сборке исполняемого модуля.

Исследования, в области идентификации автора электронного продукта, сталкиваются с рядом проблем. Довольно часто, при разработке программного обеспечения, используется чужой код или же разработку проекта ведет группа программистов. Разработчик может преднамеренно вносить искажения в исходный код. Размер кода, необходимый для объективного анализа принадлежности его автору остается достаточно субъективной величиной. Среда разработки также в некоторой степени нивелирует стилистические различия в написании кода разными авторами. Несмотря на все это, остается достаточное количество признаков, по которым возможна идентификация автора электронного продукта.

ОБ ОРГАНИЗАЦИИ ЗАЩИТЫ КОРПОРАТИВНЫХ ДАННЫХ

М.Г. УСОВА, Д.М. СТЕРИНЗАТ, М.С. ТИВАНОВА

Выбор средств обеспечения безопасности и объем их использования зависит от того, насколько продуманно и эффективно реализованы меры по предоставлению пользователю прав на те или иные корпоративные данные. Авторами предложен следующий подход в решении поставленной задачи.

Пользователей корпоративной информационной системы делят на группы. Это пользователи: а) формирующие данные, входящие в корпоративную информацию, б) выполнение должностных обязанностей которых предполагает использование полной информации о деятельности организации, в) которым предоставляются индивидуальные наборы различных данных. Различия между группами обусловило использование способов защиты информации, как на уровне клиентских приложений системы, так и на уровне базы данных.

Назначение прав на уровне приложения подразумевает наличие в программе участка кода, который определяет имя пользователя и, в зависимости от уровня привилегий, формирует содержание отображаемой страницы. При назначении прав на уровне базы для каждой таблицы перечислен список учетных записей пользователей и привилегии каждого из них на выполнение различного типа запросов. Поэтому при попытке выполнения SQL-запроса, на который данная учетная запись не имеет прав, СУБД реагирует возникновением исключительной ситуации, обрабатывая которую приложение сигнализирует о возникновении аномалии доступа и возвращается к предыдущей странице. Применяя комбинацию приведенных способов, авторы добились упрощения приложения и оптимизации процесса назначения прав. Используя доступ на уровне приложения, мы обеспечиваем выбор из специально созданной таблицы состава

меню для групп, в которые входит одна и та же учетная запись. Далее, исходя из определения прав, в БД путем создания представления пользователя, формируется ограниченный набор данных.

ОБНАРУЖЕНИЕ ЭНЕРГЕТИЧЕСКИ СКРЫТНОГО КОДИРОВАННОГО СИГНАЛА

А.И. МИТЮХИН

С целью защиты информации от несанкционированного доступа, обеспечения скрытной передачи в радиоэлектронных системах используется низкоскоростное кодирование. Во избежание эффективного обнаружения и декодирования сигналов перехватывающей станцией, передача информации ведется с помощью кодов большой значности (n>100) с апериодической сменой ансамблей равновероятных кодовых слов кода . При этом период кодового слова может превышать время затрачиваемое на передачу символа сообщения. Данная тактика кодирования не позволяет перехватчику информации использование оптимальных методов обнаружения и декодирования сигналов по минимуму расстояния Хэмминга.

Показано, что без чрезмерных временных и технических затрат достичь устойчивого перехвата информации с заданными характеристиками обнаружения — вероятностью правильного обнаружения $P_{по}$, вероятностью ложной тревоги $P_{лт}$ вероятностью ошибки декодирования $P_{ош}$ практически невозможно. Для заданного диапазона отношений $q=S/N$ (мощности сигнала к средней мощности шума) на входе некогерентного обнаружителя определены временные параметры декодирования в основном канале и канале перехватчика. Например, для получения оценки обнаружения широкополосного кодированного сигнала полосой 1 Мгц со значениями вероятностей $P_{по}$=0,9999; $P_{лт}$=0,1 требуется время анализа (накопления) соизмеримое с величиной $T_н$=1000 с., (q=–7 db). Время декодирования этого же сигнала в основном канале с вероятностью правильного декодирования P=0,9999 не превышает величины T=110 мкс. Высокое качество обнаружения энергетически скрытного сигнала достигается за недопустимо большое время.

ИЗМЕРЕНИЕ ВРЕМЕННЫХ ПАРАМЕТРОВ КОНСОЛЬНОГО ВВОДА ДЛЯ ЗАДАЧИ АНАЛИЗА КЛАВИАТУРНОГО ПОЧЕРКА

С.И. СИРОТКО

Перспективным направлением в современных системах защиты информации и контроля доступа является использование биометрических характеристик пользователя. Однако применение в этих целях специализированных устройств усложняет состав периферии рабочего места и не всегда оправдано экономически. В ряде случаев целесообразным представляется привлекать устройства, уже присутствующие у типичной персональной ЭВМ, в первую очередь, устройства ввода. Например, анализ особенностей клавиатурного почерка хотя и не обеспечивает сам по себе необходимую надежность идентификации пользователя, но эффективно

дополняет парольную систему и, кроме того, позволяет организовать непрерывный дополнительный контроль в процессе работы.

Так как при использовании стандартной клавиатуры для наблюдения доступны только моменты нажатий клавиш, от точности их измерения зависит достоверность последующего анализа клавиатурного почерка. Однако стандартные средства ввода систем семейства Windows эту точность существенно ограничивают.

В работе рассматриваются вопросы, связанные с точностью измерения моментов нажатий клавиш: факторы, влияющие на величину задержки, собственные временные характеристики клавиатур, оценка влияния точности измерений на достоверность результатов анализа и технические способы ее обеспечения. Приводятся полученные количественные оценки.

ПРОТОКОЛЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ VPN-СОЕДИНЕНИЯ

А. Э. АФАНАСЕНКО

Virtual Private Network (виртуальная частная сеть) – технология, которая была разработана для создания надежно защищенных сетей на базе имеющейся и функционирующей инфраструктуры какой-либо глобальной сети. Технология VPN может использоваться для объединения нескольких локальных сетей в одну существующую инфраструктуру, а также для связи одного компьютера с сетью. Объединение сетей происходит с помощью VPN-туннелей, "проложенных" в Интернете. Для их создания и поддержания в рабочем состоянии необходимы специальные протоколы, программное обеспечение, специфическое оборудование. Важно позаботится о защите корпоративной информации (среди которой могут быть и секретные данные), которая будет передаваться по туннелям. Для создания VPN могут использоваться различные протоколы. Тем не менее, на практике почти всегда применяются только два из них: SocketSecure-Layer и IPSec. Большинство же разработчиков выбирают именно второй вариант.

Протокол IPSec включает два протокола: Authentication Header (AH) и Encapsulating Secure Payload (ESP). Первый создает конверт, обеспечивающий аутентификацию источника данных, их целостность и защиту от навязывания повторных сообщений. С его помощью аутентифицируется каждый пакет. Протокол ESP обеспечивает конфиденциальность данных. Поскольку основной целью ESP является обеспечение конфиденциальности данных, разные виды информации могут требовать применения существенно различных алгоритмов шифрования. Следовательно, формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов.

Чтобы установить защищенное соединение, оба участника сеанса должны иметь возможность быстро согласовать параметры защиты, такие как алгоритмы аутентификации и ключи. IPSec поддерживает два типа схем управления ключами, с помощью которых участники могут согласовать параметры сеанса. С текущей версией IP, IPv4, могут быть использованы или Internet Secure Association Key Management Protocol (ISAKMP), или Simple Key Management for Internet Protocol. IPSec поддерживает не-

сколько типов шифрования, в том числе Data Encryption Standard (DES) и Message Digest 5 (MD5).

Протокол IPSec является лучшим среди всех других протоколов защиты передаваемых по сети данных, разработанных ранее.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ И КОРПОРАТИВНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ WINDOWS FIREWALL

В.Л. ЛАЗАРЕВИЧ

Когда дело касается безопасности компьютерных систем, большинство организаций сосредоточивает свои усилия на серверах. Но многие из недавно объявившихся сетевых вирусов, разрушивших целые сети и стоивших компаниям миллионы долларов, нанесли этот огромный ущерб, проникнув в сеть через беззащитные рабочие станции. Злоумышленники – будь то посторонние лица или недовольные сотрудники компании, умеющие контролировать рабочую станцию и имитировать легитимного пользователя системы, могут получать доступ к конфиденциальной информации и ресурсам на локальной системе и в локальной сети. Прошли те времена, когда локальную сеть можно было расценивать как безопасное убежище. Теперь от атак вирусов и действий злоумышленников нужно защищать все рабочие станции.

Очевидно, разработчики Microsoft отдают себе в этом отчет. Именно поэтому в рамках инициативы Trustworthy Computing компания сделала вопрос безопасности ключевым при разработке пакета обновлений Windows XP Service Pack 2 (SP2) — самого крупного ориентированного на безопасность пакета обновлений. Он до отказа набит новыми функциями безопасности для борьбы с вирусами и вредоносными программами, которые могут поражать сети через незащищенные рабочие станции. Самой важной частью SP2 является Windows Firewall — заметно усовершенствованная версия Internet Connection Firewall (ICF). Изменение названия функции отражает тот факт, что Microsoft делает упор на использовании технологии локального брандмауэра для защиты рабочих станций, которые подключены только к внутренней локальной сети, в той же мере, что и для защиты рабочих станций, имеющих подключение к Internet.

По умолчанию Windows Firewall работает в режиме максимальной безопасности и принцип его работы таков — запросы приложений выпускаются наружу, а снаружи принимаются только пакеты, пришедшие в ответ на запросы (соответствие запрос-ответ явно ведется в виде динамической таблицы). Таким образом, при сканировании портов на компьютере с включенным Windows Firewall нет ни одного открытого порта (это логично – пакеты сканера портов не будут пропущены, т.к. их никто не запрашивал). Аналогично дело обстоит с различного рода атаками, основанными на отправке нестандартных пакетов.

ПОСТРОЕНИЕ СИСТЕМЫ ПЕРЕПОДГОТОВКИ КАДРОВ НА БАЗЕ ПЛАТФОРМЫ MICROSOFT ELEARNING SERVER

Е.В. ЛАЗАРЕВИЧ

В современном мире очень ценится время и знания. Microsoft eLearning Server позволяет сотрудникам современных компаний получить нужные знания, и сэкономить время.

Microsoft eLearning Server очень удобен в применении. Система имеет динамическое содержание и может приспосабливаться к разнообразным стилям обучения.

Используя данную систему, пользователь может:

Получить детальную информацию о концепциях программного обеспечения и принципах его работы, и о диапазоне задач, необходимых для его работы.

Оценить уровень своих знаний в любое время.

Получить новые практические навыки.

Регулировать скорость обучения, на основании своего графика работы; система управления обучением отслеживает уроки, которые пользователь взял, поэтому он может начать с того места, на котором остановился.

Обучаться, находясь в автономном режиме, а потом система синхронизирует продвижение по курсу, когда пользователь подключится к Интернету.

Данную систему очень удобно использовать в крупных компаниях, работа которых связана с программным обеспечением. В системе всегда есть курсы по всем известным и новым технологиям, таким образом, сотрудники могут постоянно повышать свою квалификацию, не отходя от рабочего места.

ПРОГРАММНЫЙ МОДУЛЬ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

В.С. НЕКРАСОВ, А.С. ЛЕТОХО

Данный модуль осуществляет идентификацию пользователей распределенной информационной системы по динамике клавиатурного набора. Для анализа динамики клавиатурного набора исследуется относительное расстояние между векторами характеристик текущего пользователя и эталона, хранящегося в базе данных. На основе полученных данных строится решающее правило, которое позволяет либо принять, либо отвергнуть гипотезу о принадлежности полученного входного множества векторов к тому или иному классу.

В состав программного модуля входят: модуль распознавания по фиксированной парольной фразе, модуль распознавания по “свободному набору”, модуль распознавания по динамике работы со служебными клавишами, программный агент, центральный программный анализатор.

Программный агент представляет собой системный сервис, который устанавливается на клиентских компьютерах и управляется центральным приложением, либо администратором сети. Программный агент осуществляет перехват клавиатурных событий, инициированных пользователем и измерение временных интервалов между событиями. По

расписанию, заданному центральным приложением, агент выполняет отправку измеренных характеристик по защищенному протоколу.

Центральный программный анализатор представляет приложение, осуществляющее управление агентами, получение и обработку данных от агентов, распознавание пользователей, редактирование эталонных значений в базе данных, принятие решения о продолжении работы, блокировке компьютера, уведомление администратора о подозрительном поведении.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СИСТЕМЫ ПРОФИЛИРУЮЩЕЙ КАФЕДРЫ

В.В. ГОЛЕНКОВ, Ю.И. ИВАНЧЕНКО, А.Ю. ДЕЕВ.

В рамках проекта "Виртуальная кафедра" ведутся работы по созданию кафедральной корпоративной системы. При этом основной целью проекта является минимизация временных затрат на взаимодействие участников учебного процесса, повышение уровня самостоятельности и ответственности каждого из них.

Основными участниками проекта являются студенты и преподаватели. Это определяет некоторые особенности: ежегодное изменение состава пользователей; присутствие пользователей с разным уровнем знаний и различной мотивацией поведения; затрудненность непосредственного контроля каждого пользователя; существенное различие уровня доступа и контроля некоторых групп студентов и преподавателей; участие студентов непосредственно в процессе разработки.

В связи с этим возникают проблемы обеспечения безопасности, как деятельности самой кафедры, так и кафедральной корпоративной системы.

Часть этих проблем решается традиционными средствами и методами – средствами операционной системы и документооборота, и разработанными на их основе приложениями. Другую часть указанных проблем, например таких как:

– семантический анализ, мониторинг деятельности пользователей (выявление событий и изменений выходящих за рамки рабочих изменений);

– оперативное принятие решений при опасных действиях пользователя;

– ненавязчивое обучение пользователя грамотному безопасному использованию кафедральной корпоративной системы;

– прогнозирование действий пользователя (в том числе администратора безопасности) с целью предотвращения действий деструктивно влияющих на функционирование ИТ и системы обеспечения безопасности;

– установление прав доступа к различным фрагментам материала обучающей системы, предлагается решать с использованием технологий искусственного интеллекта.

СТАТИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

А.В. ГЕМБИЦКИЙ, С.Б. САЛОМАТИН

В задачах защиты информации применяются преобразования на эллиптических кривых (ЭК), которые используют в качестве базовой, операцию умножения точки P ЭК E на число k. Принцип генератора ПСП на эллиптических преобразованиях состоит в последовательном вычислении координат точек, путем суммирования начальной точки с другой точкой (базовой) либо в многократном умножении начальной точки на скаляр. Вычисления могут осуществляться как в аффинных, так и в проективных координатах. Выход ПСП формируется путем конкатенации отдельных или нескольких координат точек, получаемых на каждом шаге работы генератора.

Для тестирования генераторов ПСП был использован статистический пакет NIST STS (NIST Statistical Test Suite). В пакет NIST STS входит 16 статистических тестов, которые в зависимости от входных параметров позволяют получить 189 значений вероятности.

Суть тестирования сводилась к получению с помощью специальной функции и статистики теста значения вероятности, лежащего в диапазоне от 0 до 1. Полученное значение вероятности сравнивалось с уровнем значимости равным 0.01. Если значение вероятности превышало этот уровень, то принималось решение о случайности тестируемой последовательности. Эффективность тестирования оценивалась как проценты прохождения последовательностями тестов и количество тестов, результаты которых превысили соответствующую долю. Результаты тестирования сравнивались с показателями генератора ПСП типа BBS.

Для генератора ПСП на эллиптических преобразованиях минимальное значение вероятности составило 0.96 при проверке неперекрывающихся шаблонов, тогда как для генератора BBS — 0.9403 при проверке случайных отклонений. Генератор на эллиптических преобразованиях проходит тест при установлении порога в 96% последовательностей, тогда как генератор BBS требует порога в 94 %, что свидетельствует о некотором преимуществе генератора на эллиптических преобразованиях и позволяет рекомендовать его для практического применения.

ОЦЕНКА МОЩНОСТИ ОТКРЫТЫХ КЛЮЧЕЙ В КРИПТОСИСТЕМЕ МАК-ЭЛИСА-СИДЕЛЬНИКОВА

В.А. ГОТОВКО, В.А. ЛИПНИЦКИЙ

Берлекэмп, Мак-Элис и Тилборг [1] установили NP-полноту ряда задач помехоустойчивого кодирования. На этой основе в 1978 г. Мак-Элис предложил криптосистему с открытым ключом [2], построенную на основе помехоустойчивого кодирования. Суть криптосистемы в следующем. Берется линейный (n, k)-код C над конечным полем F_q, исправляющий t ошибок (сам Мак-Элис за основу брал коды Гоппы). Как известно, такой код однозначно задается своей порождающей матрицей G порядка $k \times n$ над полем F_q. Абонент A с помощью секретного ключа — пары матриц H, Г (H — произвольная невырожденная матрица над F_q, Г — перестановочная), создает открытый ключ $E=H \cdot G \cdot$Г, который рассылает заинтересо-

ванным лицам или делает его общедоступным. Абонент B передает абоненту A конфиденциальную информацию $\overline{m}$ - k - мерный вектор над F_q. Он зашифровывает сообщение в виде вектора $\overline{c} = \overline{m} \cdot E + \overline{z}$, где $\overline{z}$ вектор ошибок, корректируемый кодом C. Получатель, используя закрытый ключ и декодирующие алгоритмы, восстанавливает информацию. Мак-Элис предполагал, что атака на шифр возможна только перебором закрытых ключей (NP-полная задача). Позднее было замечено, что E является матрицей кода C', эквивалентному коду C. На этом основании в [3] В.М. Сидельниковым и С.О. Шестаковым установлено, что криптосистема Мак-Элиса на основе кодов Гоппы может быть вскрыта за полиномиальное время. Тем не менее, В.М. Сидельников [4] модифицирует криптосистему: а) предлагает за основу взять коды Рида-Маллера (длиной N), имеющие быстрые алгоритмы декодирования [5]; б) увеличивает секретный ключ, взяв в качестве такого $(\widetilde{H}, \widetilde{\Gamma})$, где $\widetilde{H} = (H_1, ..., H_u)$, H_1 — невырожденная $k \times k$ матрица, $\widetilde{\Gamma}$ — $uN \times uN$ перестановочная. Такая система имеет высокую скорость передачи и криптографическую стойкость. Это подтверждено, в частности, работой [6], где установлено точное значение мощности ключей $(\widetilde{H}, \widetilde{\Gamma})$ при u=2.

В докладе приводится и обосновывается значение мощности открытых ключей при $u = 3$, приводится оценка этой мощности для произвольного u.

Литература

1. Berlekamp E.R., McEliece R.J., van Tilborg H.C.A. On the Inherent Intractability of Certain Coding Problem. //IEEE Trans. Inf. Theory, 1978. V. 29. №3. - P. 384 – 386.
2. McEliece R.J. Public-key cryptosystem based on algebraic coding theory. //DSN Prog. Rep., Jet Prog. Lab., California Inst. Technol., Pasadena, 1978. - P. 114 – 116
3. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на осно-ве обобщенных кодов Рида-Соломона. //Дискр. матем., 1992. Т. 4, №3. - С. 57 – 63.
4. Сидельников В.М. Открытое шифрование на основе двоичных кодов Рида-Маллера. //Дискр. матем., 1994. Т. 6, №2. - С. 3 – 20.
5. Сидельников В.М., Першаков А.С. Декодирование кодов Рида-Маллера при боль-шом числе ошибок. //Пробл. передачи информации, 1992. Т. 28, №3. – С. 80 – 94.
6. Карпунин Г.А. О ключевом пространстве криптосистемы Мак-Элиса на основе двоичных кодов Рида-Маллера. //Дискр. матем., 2004. Т. 16, №2. – С. 79 – 84.

ИМИТАЦИЯ УДАЛЕННЫХ АТАК, НАПРАВЛЕННЫХ НА ОТКАЗ В ОБСЛУЖИВАНИИ СЕТЕВЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Д.С. ПРИЩЕПА, В.Ф. ГОЛИКОВ

Атакой на информационную систему называется действие или последовательность связанных между собой действий нарушителя, которые приводят к реализации угрозы путем использования уязвимостей этой информационной системы. Все атаки можно разделить на локальные, которые производятся в пределах самой информационной системе, и удаленные, которые проводятся через сеть общего пользования. Первый тип атак является легко обнаружимым и нейтрализуемым с помощью административных мер. Второй класс является самым распространенным и наиболее тяжело поддается обнаружению и нейтрализации.

Удаленная активная атака – это упорядоченный набор сетевых операций, выполняемых на каждой фазе проведения атаки, организованный по последовательной или параллельной схемам воздействия на атакуемые узлы и направленный на обход средств защиты атакованного уз-

ла. Каждая сетевая операция, входящая в состав удаленной активной атаки, называется элементарной атакой.

Элементарная атака — это действия и правила, описывающие цикл сетевой операции в составе атаки, результат которого не обязательно направлен на обход защиты атакованного узла.

Одним из самых распространенных видов удаленных атак, который часто применяется как составная часть других более сложных атак, является класс атак, направленных на отказ в обслуживании (DoS — Denial of Service). Основной принцип таких атак — генерация большого числа запросов к атакуемой системе, приводящего к ухудшению работоспособности системы и, возможно, к отказу в обслуживании запросов от легальных клиентов. Примерами таких атак являются:

– затопление SYN-пакетами, которое приводит к блокированию атакуемого узла из-за переполнения его очереди запросов на установление TCP-соединений;

– передача широковещательного запроса от имени жертвы, что приводит к получению жертвой большого количества ответов от других узлов сети;

– рассинхронизация TCP-соединения, приводящая к разрыву установленного атакуемым узлом TCP-соединения;

– затопление UDP-пакетами, приводящее к блокированию атакуемого узла, всей сети или участка сети, вызванному чрезмерной загрузкой сети UDP-пакетами;

– зацикливание IP-пакетов, приводящее к блокированию атакуемого узла из-за переполнения его очереди TCP-соединений вследствие некорректной реализации стека протоколов TCP/IP.

Идеальная система обнаружения вторжений (СОВ) должна иметь средства определения аномального трафика и развитую систему принятия решений, способную блокировать трафик, сгенерированный нарушителем, оставляя таким образом систему доступной для легальных пользователей. В современных СОВ развиваются два типа методов обнаружения вторжений: методы обнаружения злоумышленного поведения и методы выявления аномальной активности. Первый метод основан на сравнении текущего поведения субъектов с сигнатурами (известными сценариями атак) злоумышленного поведения. Примером СОВ, использующей такие методы, является экспертная система P-BEST, входящая в состав продукта EMERALD [1]. Недостаток такого подхода в том, что нарушитель может прибегнуть к атаке, в ходе которой он генерирует безупречные с точки зрения политики безопасности запросы. Подобную атаку сигнатурными методами обнаружить невозможно. Способ проведения такой атаки известен: если генерировать поток обычных пакетов очень высокой интенсивности, можно добиться переполнения буфера ресурса и вызвать, таким образом, отказ в обслуживании.

Наибольший интерес представляют методы второго типа, так как они позволяют обнаруживать неизвестные атаки, для которых еще не составлены сигнатуры. Они основаны на сравнении текущих значений параметров субъекта или объекта, собранных за несколько часов со значением этих параметров, собранных за несколько недель или месяцев. Первые параметры составляют краткосрочный профиль активности, а вторые составляют долгосрочный профиль, значение которого является нормой.

Например, в системе NIDES [2] краткосрочный профиль представляет набор значений параметров активности, полученных из нескольких сотен последних записей аудита; долгосрочный профиль формируется из записей аудита, собранных в течение нескольких недель с учетом коэффициента старения данных.

Для исследования вопросов борьбы с перечисленными атаками необходимо научиться моделировать атакующие воздействия. В работе [3] была построена система имитации фонового трафика и потока запросов, созданного атакующим. При этом было сделано допущение, что время между поступлением запросов от легальных пользователей является случайной величиной и имеет нормальное распределение.

Для генерации атакующего трафика создавался поток запросов, не находящих подтверждения установления соединения, которые находятся в буфере в течении некоторого максимального срока, устанавливаемого администратором. При этом запросы генерировались через некоторый заданный интервал времени.

Данная система генерирует трафик по протоколу TCP (затопление SYN-пакетами).

В работе [4] была проведена доработка данной системы, в результате которой были добавлены некоторые протоколы прикладного уровня (SMTP, FTP и HTTP). Так же была добавлена возможность несколько увеличить максимальную интенсивность генерируемого трафика путем создания нескольких независимых процессов генерации.

Основными недостатками разработанной системы являются:

1) ограничение на интервал между генерацией двух запросов (10000 мксек), накладываемое ядром операционной системы Linux 2.4.22 на процессы, выполняемые на прикладном уровне;

2) нераспределенность атакующего трафика, что позволяет атакуемой системе блокировать трафик на основе отслеживания IP-адреса источника запросов;

3) ограниченность протоколами TCP, SMTP, FTP и HTTP.

В дальнейшем предполагается существенная доработка системы имитации трафика путем:

1) встраивание системы генерации в ядро операционной системы с использованием и доработкой существующего в ядре Linux 2.6.9 модуля pktgen;

2) создания системы шаблонов запросов для протоколов прикладного уровня, что приведет к возможности добавлять в систему новые протоколы без необходимости модификации самого модуля;

3) построение модели распределенной атаки путем использования нескольких узлов сети, синхронизированных по некоторому управляющему протоколу;

4) рассмотрение возможности расширения реализуемых моделей атакующего трафика.

Литература

1. Neumann Peter G., Porras Phillip A. Experience with EMERALD to DATE// Computer Science Laboratory SRI International. 1st USENIX Workshop on Intrusion Detection and Network Monitoring. Santa Clara, California, 11–12 April 1999. http://www.csl.sri.com/neumann/det99x.html#IDESFinal92.
2. 29 Javitz H. S., Valdes A., The NIDES Statistical Component: Description and Justification. March 1993 SRI International Menlo Park, California. http://www.sdl.sri.com/nides/reports/statreport.ps.gz.
3. Прищепа Д.С. Дисс. ... магистр техн. н. БГУИР. М. 2004г.
4. Отчет о научно-исследовательской работе "Разработать систему для проведения анализа устойчивости операционных систем (ОС) к воздействию удаленных активных атак и разработать рекомендации

по обеспечению устойчивости ОС, используемых в государственных структурах Республики Беларусь (заключительный)", номер госрегистрации 20013187, Минск, 2004 г.

ЗАЩИТА ИНФОРМАЦИИ ОТ ИСКАЖЕНИЙ МЕТОДОМ ВСТРЕЧНОЙ ФИЛЬТРАЦИИ

В.В. ВЕЛИЧКОВСКИЙ

Пусть на отрезке в N равноудаленных точках задана функция x(n)=s(n)+m(n), где s(n) — низкочастотная полезная составляющая функции x(n), а m(n) — аддитивная широкополосная помеха. Задача состоит в сглаживании аддитивной помехи с минимальными искажениями s(n). Использование низкочастотного фильтра с хорошо подобранной частотной характеристикой подавляет помеху, но при этом s(n) претерпевает сдвиг во времени, что в ряде случаев нежелательно. Предлагается способ сглаживания путем пропускания через низкочастотный фильтр двух функций: x(n) и x(N–n). Оценка полезного сигнала в момент $n=n_0$ формируется как полусумма его оценок, получаемых при сглаживании функции x(n) от момента n=1 до $n=n_0$ и при сглаживании ее в обратном направлении от N=n до n=n0. Анализ предложенного метода сглаживания показал, что существенно уменьшается запаздывание полезного сигнала. Аддитивная помеха при этом с одной стороны подавляется фильтром, а с другой стороны уменьшается при вычислении полусуммы, так как слагаемые при широкополосной помехе статистически практически независимы в силу того, что одно слагаемое есть результат усреднения помехи на отрезке от n=1 до $n=n_0$, а второе – на отрезке от $n=n_0$ до n=N. Этим обеспечивается дополнительное практически двукратное снижение дисперсии помехи на выходе. Предлагаемый метод в ряде случаев оказывается более эффективным по сравнению с описанной в литературе реверсной фильтрацией.

ТЕХНИЧЕСКИЕ СРЕДСТВА ВИЗУАЛИЗАЦИИ ИНФОРМАЦИИ

К.Д. ЯШИН, Л.И. АЛЕКСЕЙЧУК, В.С. ОСИПОВИЧ, С.Е. ПИЦУК

Постоянно ведутся исследовательские работы по совершенствованию методов лечения и диагностики различных заболеваний. Совершенствуются циторедуктивное лечение высокодозной химиотерапии, лечение лимфогранулематоза, метаболических сдвигов, полихимиотерапия, цитологическая диагностика, диагностика эндогенной интоксикации методом ЭПР-спектрометрии, метод квантовой гемофизиотерапии, диагностика параметров эндотоксикоза. Быстрое обнаружение и идентификация возбудителей опасных заболеваний занимают ключевое место в современной медицине. Особое внимание уделяется развитию методов ранней диагностики раковых заболеваний. Развиваются следующие технические методы визуализации медицинской информации. Изотопный метод. Имеет относительно высокую чувствительность и селективность. Хемилюминесцентный метод. Основан на явлении излучения фотонов при переходе электронно-возбужденных продуктов окислительных химических реакций в исходное энергетическое состояние. В таких реакциях выделяется значительное количество энергии и квантовый выход излучаемого света достаточно высок. Тепловизионный метод. В основе лежит бесконтактный метод выявления болезни с помощью тепловизоров из-за повышения хими-

ческой и кровяной деятельности сосудов в предраковых и раковых тканях. Обработка полученных термограмм позволяет прогнозировать развитие раковых опухолей еще до того, когда они могут быть выявлены какими-либо другими методами. Газоразрядная визуализация. Получают изображения, формируемые в результате свечения газового разряда. Разряд возникает вблизи поверхности объекта, помещенного в электромагнитное поле высокой напряженности. Этот подход к ранней диагностике патологических состояний организма основан на анализе изменений газоразрядных изображений плазмы крови человека, подвергнутой процедуре потенцирования лекарственных препаратов. Спиновые метки широко применяются при исследовании биологических систем на самых разных уровнях их структурной и функциональной организации (белки и сложные белковые комплексы, биомембраны, клетки, ткани и органы). Спиновые метки – химически стабильные парамагнитные молекулы, которые используются в качестве молекулярных зондов для изучения структуры и молекулярной подвижности различных физико-химических и биологических систем [1].

Иммунофлуоресцентный анализ — совокупность иммунохимических методик, использующих иммунореагенты, в состав которых введены флуоресцентные метки. Применение квантовых точек в качестве флуоресцентных меток имеет ряд преимуществ по сравнению с традиционными методами. Во-первых, в отличие от традиционных химических красителей, у квантовых точек интенсивность фотолюминесценции при облучении светом не уменьшается. Во-вторых, интенсивность свечения квантовых точек на несколько порядков выше, чем у обычных красителей. И в-третьих, цвет излучения квантовых точек сильно зависит от их размера, что дает возможность получать цветные изображения [2]. Люминесцентные метки включают полупроводниковое соединение (CdSe), покрытое дополнительной полупроводниковой оболочкой (ZnS) для улучшения оптических свойств материала. Эта структура ядро-оболочка в дальнейшем покрывается полимерным соединением, что позволяет материалу соединяться с биомолекулами и сохранять свои оптические свойства [3]. Уникальные характеристики полупроводниковых кристаллических наночастиц делают их лучшим на сегодня инструментом для биотехнологических и диагностических целей.

Литература

1. Спиновые метки. Соросовский обозревательный журнал, № 1, 1998, стр. 8–15.
2. Яшин К.Д., Пицук С.Е., Осипович В.С. Медэлектроника, 2004, стр. 153.
3. Qdot technology basics. http://www.evidenttech.com.

ЭКРАНИРУЮЩИЕ СВОЙСТВА ПОРОШКООБРАЗНОГО ВЛАГОСОДЕРЖАЩЕГО МАТЕРИАЛА НА ОСНОВЕ БЕНТОНИТА

Н.В. КОЛБУН, ФАН Н. ЗАНГ, Л.М. ЛЫНЬКОВ

Введение

Основным и наиболее эффективным техническим средством защиты информации является создание экранированных помещений. Обычно экранирующая конструкция представляет собой металлический корпус, создающий значительное затухание электромагнитной энергии и препят-

ствующий выходу электромагнитных сигналов за пределы защищаемой области. При этом для предотвращения утечки информационного сигнала через любые каналы ПЭМИН используются помехоподавляющие фильтры в цепях питания, кабельных вводах в помещение, системах телекоммуникаций, воздуховодах. Однако использование металлических конструкций приводит к возникновению значительных переотражений внутри т.н. клетки Фарадея, напряженность поля в некоторых областях вследствие суперпозиции волн может превышать предельно допустимые уровни в десятки раз. Это создает неблагоприятную электромагнитную обстановку для обслуживающего персонала. В связи с этим перспективным направлением является разработка радиопоглощающих материалов, обладающих невысоким коэффициентом отражения [1].

Исследования [2] показали перспективность применения влагосодержащих наполнителей для создания конструкций экранов электромагнитного излучения с невысоким коэффициентом отражения. Преимуществами таких конструкций является возможность получения заданных характеристик экранирования, высокая технологичность и относительно небольшая стоимость.

Для формирования пространственной гидродисперсной структуры и стабилизация ее свойств было предложено использовать влагопоглотители на основе бентонитов [3]. Бентониты представляют собой коллоидные глины и имеют резко выраженные сорбционные свойства и высокую пластичность.

Исследовались коэффициенты ослабления и отражения электромагнитной энергии в диапазоне 8–11,5 ГГц влагосодержащих материалов на основе мелкодисперсного порошка бентонита и временная стабильность этих характеристик.

Методика проведения эксперимента

Образцы представляли собой мелкодисперсный бентонит, содержащий растворный наполнитель в различных количествах. Толщина образцов составляла 3 мм. В качестве растворных наполнителей использовались вода и водные растворы соли NaCl (10 %) и ПАВ (1 %). Коэффициент влагосодержания образцов оценивался гравиметрически с использованием прецизионных весов ВЛР-200. Для измерения экранирующих характеристик в диапазоне частот 8–11,5 ГГц использовался панорамный измеритель КСВН и ослабления Р2-62 с волноводным измерительным трактом. Измерения производились в панорамном режиме после калибровки приборов. Исследуемый образец помещался между фланцами волноводного тракта.

Для предотвращения испарения жидкости и стабилизации свойств образцы герметизировались многослойными полиэтиленовыми пленками толщиной 200 мкм. Результаты исследования снижения влагосодержания герметизированного образца с влагосодержанием 31,4 % приведены на рис. 1.

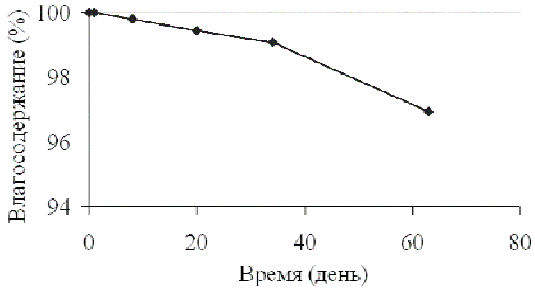


Рис. 1. Снижение влагосодержания в % от начального значения в зависимости от времени хранения

Исследовалась зависимость экранирующих характеристик дисперсных материалов на основе бентонита от их влагосодержания. Измеренные коэффициенты ослабления и отражения ЭМИ образцов приведены на рис. 2.

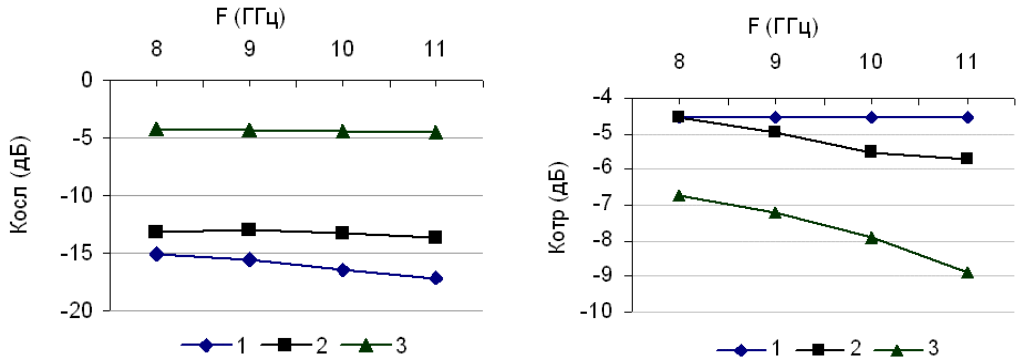


Рис. 2. Частотные зависимости коэффициентов ослабления (а) и отражения (б) ЭМИ мелкодисперсного порошка бентонита, заполненного водой с различным влагосодержанием: 1 — 31,4%; 2 — 25,3%; 3 — 16,5%

Исследовалось влияние водных растворов ПАВ и NaCl на взаимодействие влагосодержащего бентонита с ЭМИ. Результаты измерений экранирующих характеристик порошка бентонита, содержащего водные растворы ПАВ и NaCl, приведены на рис. 3 и 4.

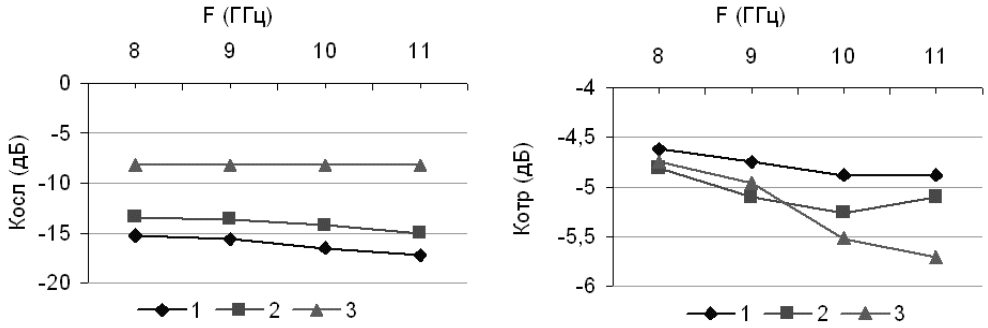


Рис. 3. Частотные зависимости коэффициентов ослабления (а) и отражения (б) мелкодисперсного порошка бентонита с водным раствором ПАВ с различным влагосодержанием: 1 — 31,1 %; 2 — 25,1 %; 3 — 17,1 %

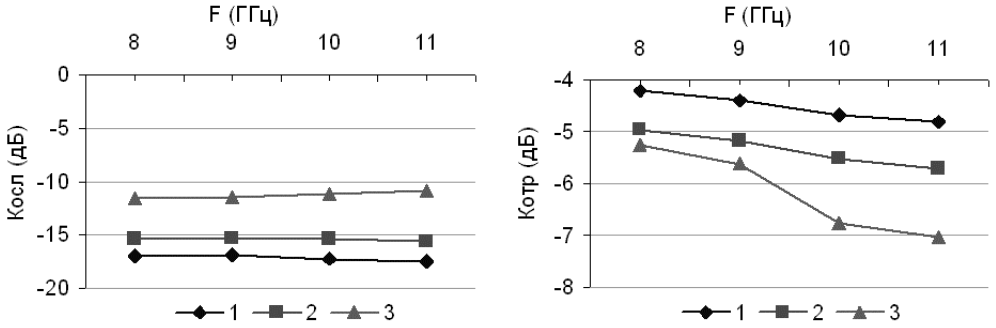


Рис. 4. Частотные зависимости коэффициентов ослабления (*а*) и отражения (*б*) мелкодисперсного порошка бентонита с водным раствором NaCl с различным влагосодержанием: 1 — 30,8 %; 2 — 24,1 %; 3 — 16,5 %

Результаты и обсуждение

Исследования показали, что скорость ухода влаги зависит от вида используемого влагопоглотителя, от материала, с помощью которого герметизированы образцы, и от температуры, при которой находятся исследуемые образцы. Снижение коэффициента влагосодержания составляет около 3 % в течение 65 дней от начального значения.

Коэффициент ослабления ЭМИ образцов с влагосодержанием свыше 30 % составляет не более –15 дБ в диапазоне частот 8…11,5 ГГц при коэффициенте отражения ЭМИ –4…–5 дБ. Снижение влагосодержания приводит к повышению значения коэффициента ослабления ЭМИ на 5 дБ при снижении уровня коэффициента отражения ЭМИ до –7…–9 дБ. Использование в качестве влагосодержащего наполнителя водного раствора ПАВ незначительно отражается на экранирующих характеристиках образцов (по сравнению с водой) и может применяться для активизации сорбционных свойств бентонита и повышения временной стабильности свойств экранирующих материалов на его основе. Введение в состав водного раствора соли NaCl приводит к увеличению коэффициента отражения ЭМИ (до –4 дБ), в результате чего общая эффективность экранирования понижается (по сравнению с образцами, содержащими воду и водный раствор ПАВ) до –17 дБ.

Выводы

Использование влагосодержащих материалов на основе мелкодисперсного порошка бентонита позволяет получать экранирующие материалы с коэффициентами ослабления ЭМИ в пределах –5…–17 дБ и отражения в пределах –8…–4,5 дБ. Изменение коэффициента влагосодержания образцов и состава влагосодержащих наполнителей позволяет получать заданные экранирующие характеристики образцов.

Литература

1. Новые материалы для экранов электромагнитного излучения / Л.М. Лыньков, В.А. Богуш, Н.В. Колбун и др. // Доклады БГУИР. — 2004. — Т.2, №5. — С.152–167.

2. Украинец Е.А., Колбун Н.В. Экранирующие свойства многослойных конструкций электромагнитных экранов на основе материалов с малоразмерными включениями металлов и жидких сред // Доклады БГУИР. — 2003. — Т.1, №4. С.118–122.

3. Свойства растворосодержащих широкодиапазонных поглотителей электромагнитного излучения для технических средств защиты информации / Н.В. Колбун, Т.В. Борботько, И.С. Терех, Фан Н.Занг, Л.М. Лыньков // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: Матер. докладов Международного научн.-техн. семинара. — Минск, 2004. — С.78–84.

ВЛИЯНИЕ ИМПУЛЬСНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ВЛАГОСОДЕРЖАЩИЕ КАПИЛЛЯРНО ПОРИСТЫЕ МАТЕРИАЛЫ.

И.С. ТЕРЕХ, Г.П. ТУРУК, А.В. РУБАНИК, Л.М. ЛЫНЬКОВ, Н.В. КОЛБУН

Сильные электромагнитные поля образуют во всех проводящих материалах большие токи [1]. В результате этого возможна деструкция токопроводящих дорожек в микрочипах и чувствительных электронных узлов. Посредствам короткого, интенсивного импульса могут быть мгновенно парализовано производственное электронное оборудование различного назначения, а также финансовые центры, базы данных, военные сооружения [2].

Целью работы является исследование величины ослабления импульсного электромагнитного излучения образцов воды, влагосодержащих образцов целлюлозы, и машиновязаного материала в зависимости от толщины слоя образца.

Для измерений использовался импульсный генератор, измерительный аттенюатор, детекторный блок, осциллограф, и блоки питания. Структурная схема приведена на рис. 1. Генератор формирует электромагнитные импульсы с длительностью импульсов 400 нс и периодом повторения импульсов 50 Гц. Частота заполнения импульса равна 37 ГГц. Мощность в импульсе составляет 20 кВт.

В ходе измерений образец помещали между фланцами волноводов в первую измерительную зону (рис. 1), где импульсным источником формируются электромагнитные импульсы мощностью 20 кВт (средняя мощность 0,4 Вт). Форма электромагнитного импульса на выходе генератора и форма напряжения на выходе детекторного блока представлены на рис. 2, рис. 3 соответственно. Метод измерения ослабления образцов основан на компенсировании мощности измерительным аттенюатором таким образом, чтобы мощность электромагнитного импульса на входе измерительного блока с экраном и без него была одинаковой. Калибровка измерительной установки сводилась к установке такой мощности генератора, чтобы вершина импульса была различима на фоне помех. Затем, помещая образец в измерительную зону, мощность на входе измерителя увеличивается с помощью аттенюатора до уровня калибровки. Разница уровней ослабления аттенюатора являлась искомой величиной ослабления. Результаты исследования представлены на рис. 4.

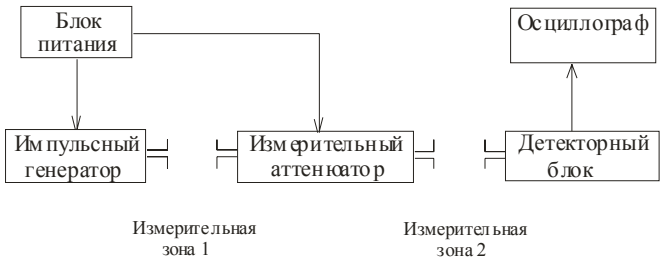


Рис. 1. Структурная схема измерительной установки

Рис. 2. Форма импульса на выходе импульсного генератора

Рис. 3. Форма импульса напряжения на выходе детекторного блока

Герметизированный полиэтиленом водный образец, с толщиной слоя воды 3 мм позволяет обеспечить ослабление ЭМИ в 58 дБ, толщина слоя целлюлозы при этом значении ослабления должна быть увеличена примерно в 1,5 раза (рис. 3). С уменьшением толщины слоя воды ослабление электромагнитного излучения уменьшается, это обусловлено малой толщиной скин-слоя материалов для описанного выше излучения. Указанная закономерность проявляется в случае целлюлозы и машиновязаного материала. Величина ослабления изменяется от 15 дБ до 47 дБ для влагосодержащего образца целлюлозы и от 15 дБ до 29 дБ для влагосодержащего машиновязаного материала.

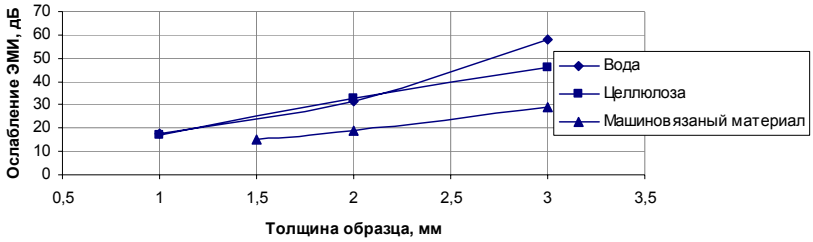


Рис. 4. Зависимость ослабления электромагнитного излучения образцов на основе воды влагосодержащих целлюлозы и машиновязаного полотна от толщины образца

В результате проведенной работы показано, что величина ослабления увеличивается с увеличением влагосодержания материала и толщины. При этом наибольшим ослаблением при одинаковых толщинах обладает герметизированный водный образец.

Литература

1. Рикетс Л.У., Бриджес Дж.Э., Майлетта Дж. Электромагнитный импульс и методы защиты: Пер. с англ. /Под ред. Н.А. Ухина. – М.: Атомиздат, 1979. – 328 с.
2. Лыньков Л.М., Борботько Т.В., Терех И.С., Электромагнитное оружие массового поражения и защита информации. Известия Белорусской Инженерной Академии № 1 (15)/2, Минск, 2003. Стр. 218-221.

ОТБРАКОВОЧНЫЕ ИСПЫТАНИЯ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ

Л.М. ЛЫНЬКОВ, Т.Г. ТАБОЛИЧ

В настоящее время электронные пластиковые карты (ЭПК) получили широкое распространение в таких областях человеческой деятельности как коммуникационная, финансово-экономическая, торговая, бытовая. При эксплуатации ЭПК имеют место сбои и отказы в работе. Целью данной работы являлось выявление потенциально ненадежных элементов ЭПК.

Анализ этих отказов может решать следующие задачи:

1. Установление видов отказов на этапах производства, испытаний и эксплуатации. Обобщение данных по отказам.

2. Изучение количественных изменений во времени.

3. Составление гипотез о механизме отказа и его причинах. Проведение исследований для подтверждения предполагаемых гипотез.

4. Анализ отказов на этапах производства, испытаний и эксплуатации.

5. Разработка принципов неразрушающих методов определения потенциально ненадежных ИС на основе результатов исследований механизмов отказов.

6. Разработка рекомендаций по устранению причин отказов определенного вида.

В результате анализа причин отказов появляется возможность совершенствования технологии изготовления модулей. Для осуществления анализа на первом этапе производился сбор данных о ЭПК, возвращенных с МЦК РО «Белтелеком» с февраля по август. Данные карты были забракованы покупателями и отправлялись изготовителю (УП «ЦНИИТУ») в сопровождении необходимой документации.

Анализ отбракованных карт показал, что часть ЭПК не отвечали стандартам предприятия изготовителя, а остальные вполне работоспособны и могут продолжать выполнять свои функции. Все карточки были отсортированы по виду дефектов. Сортировка проведена по 4 категориям, что не дает полной картины причин отказов ЭПК. Поэтому был проведен вторичный анализ с целью раскрытия наиболее полной картины причинно-следственных связей отказов модулей с привлечением статистических методов.

Данный анализ проводили по развернутой схеме. Были учтены все виды дефектов, обрывы выводов, переменный характер отказов, не пройденная аутентификация и проч.

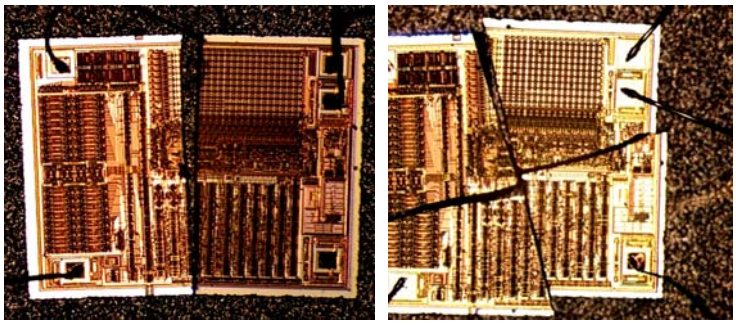
Выборка составила 1931 шт. Карты в количестве 1634 шт. признаны негодными по причине электрических механических повреждений контактов и кристалла электронной пластиковой карточки (обрывы контактов). Всего получили 34 категории, по которым классифицировались отказы.

Как показывает общая статистика брака телефонных карточек серий 02-17, 30 % брака карточек занимают обрывы выводов (в эту категорию входят все обрывы, которые наблюдались во время эксперимента).

Данная методика сбора данных позволила сделать выводы о надежности данного вида электронных пластиковых карточек предназначенных для оплаты услуг телефонной сети посредством таксофона.

Таким образом, в процессе расширенного анализа отказов ТЭПК выявляются ранние отказы всех видов — как устойчивые, так и перемежающиеся [1]. Ресурсные отказы практически выявить невозможно, так как срок службы ЭПК до ее разрушения намного превышает срок ее эксплуатации (срок расхода заложенных в ЭПК тарифных единиц). В [1] кратко описаны исследования по анализу отказов телефонных электронных пластиковых карт (ТЭПК) (УП «ЦНИИТУ»). На втором этапе для выявления механизма и причин отказа проведены исследования на выборке из 20 карт. В первую очередь проведено рентгенографическое исследование, которое не выявило дефектов кристалла. Далее провели вскрытие корпуса микромодуля ТЭПК.

На рис. 1 показан внешний вид кристалла, из которого видно, что карточки с различными отказами имели расколы микрочипа в различных местах, однако основные части не деструктурированы.



а *б*

Рис. 1. Внешний вид модулей ТЭПК с различными видами отказов: *а* — отказ обрыв выводов, ключ 01; *б* — брак, полный отказ

Сделано предположение о нарушении целостности кристалла из-за различных температурных коэффициентов используемых меди и кремния. Толщина медного слоя меди 50 мкм, кристалла 180 мкм. Известно, что температурный коэффициент линейного расширения (ТКЛР) меди равен $17 \cdot 10^{-6}$ ãðàä$^{-1}$, кремния $2{,}55 \cdot 10^{-6}$ ãðàä$^{-1}$ [2]. По технологии изготовления кристалла можно сказать о том, что все легированные и диффузионные зоны занимают приблизительно 30 % от всего кристалла. Таким образом, 2/3 кристалла составляет кремний, поэтому целесообразно рассматривать свойства ИС как свойства кремния. По причине неодинакового расширения меди и кремния возникают механические напряжения, особенно при использовании на производстве клея ВК-26М для посадки кристалла к медному основанию [3]. Предположительно при повышении температуры появляются различные механические напряжения, медное основание изгибается в ту или иную сторону для компенсации напряжений. Медь имеет металлическую, кристаллическую кубическую гранецентрированную решетку, за счет этого уровень ее пластичности высок и она деформируется. Так как ТКЛР меди на порядок больше, то степень изменения физического состояния больше чем у кремния.

На рис. 2 представлена схема изменения напряженно-деформированного состояния элементов конструкции микромодуля ТЭПК. Из-за жесткой сцепки и невозможности изгиба кристалл кремния ломается, так как кремний более хрупкий материал. В подтверждение данной гипотезы, чтобы уменьшить процент брака, связанный с данным

механизмом отказа, предложено ввести в технологический процесс сборки ЭПК дополнительные отбраковочные испытания. Термоциклирование происходит с протеканием процессов, таких как: изменение электрофизических параметров материалов, изменение механических напряжений в местах сопряжения разнородных материалов. Возможным результатом воздействия являются нестабильность электрических параметров обрывы и короткие замыкания.

Для проведения операции термоциклирования использовалась камера тепла КТХ-0,4-350 Я7М2.700.009, стол бестумбовый, часы, электронные пластиковые карточки в межоперационной таре. Схема измерений приведена на рис. 2.

Поскольку термоциклирование проводится на всей карте целиком, условия для проведения эксперимента рассчитывались с учетом максимальных температур, выдерживаемых модулем ТЭПК. Проводились 6 циклов испытаний с граничными температурами –50°С, +50°С. Испытываемые модули для ТЭПК производства «ЦНИИТУ-КАРТ» в количестве 2880 шт. разделены на две партии — одна контрольная, в процесс сборки другой партии введена операция термоциклирования с заданными выше параметрами. Операция термоциклирования выполнена после операции термовыдержки. По завершению эксперимента сравнивалось количество отбракованных карточек после технологического процесса сборки с применением операции термоциклирования и без данной операции.

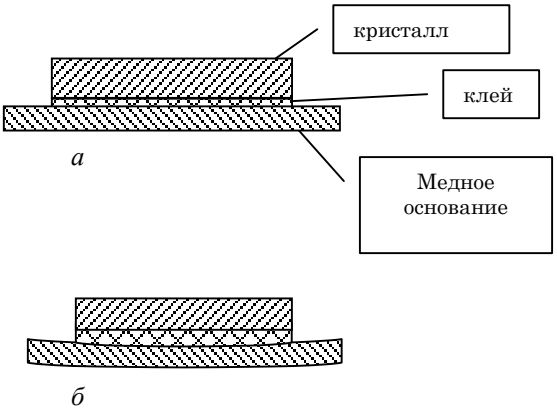


Рис. 2. Схематическое изображение напряженно–деформированного состояния элементов конструкции модуля ТЭПК: а — при нормальной температуре; б — при повышенной температуре

В результате эксперимента установлено, что количество бракованных карт партии, сборка которых происходила по предложенному нами маршруту, с внедрением в технологический процесс сборки операции термоциклирования на 25 % больше, чем количество карточек прошедших сборку в обычных условиях.

В результате проведенных исследований показано, что уровень возвратов от потребителей снижается, как и материальные затраты на обслуживание вторичного брака.

Литература

1. Вечер Д.В., Таболич Т.Г. Оценка фактической надежности телефонных ЭПК относительно перемежающихся отказов // Известия Белорусской Инженерной Академии. 2003. Вып. 1(15)/3. Ч. 3. С. 60–62.
2. Ландсберг Г.С. Элементарный учебник физики. М., 1975.
3. Емельянов В.А. Корпусирование интегральных схем. Мн., 1998.

ОЦЕНКА ИНТЕГРАЛЬНЫХ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ТАКСОФОННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ПЛАСТИКОВЫХ КАРТ

Т.Г. ТАБОЛИЧ, Г.В. СЕЧКО

Согласно ГОСТ 15467-79 «Управление качеством продукции. Термины и определения» качество продукции — это совокупность её свойств, обусловливающих ее пригодность удовлетворять определённые потребности в соответствии с ее назначением. Под свойством продукции понимается объективная особенность последней, проявляющаяся при ее производстве, эксплуатации или потреблении. Количественная характеристика свойств продукции, называется показателем качества продукции. Показатели качества делятся на е*диничные* (характеризуют одно свойство продукции) и *комплексные* (характеризуют совокупность нескольких свойств продукции). Для таксофонных интеллектуальных пластиковых карт (ТИПК), получивших широкое распространение в последние 7 лет [1–5] для безналичной оплаты таксофонных разговоров, основными единичными показателями качества могут быть выбраны себестоимость, степень защиты информации и надёжность ТИПК. Для объединения перечисленных единичных показателей в комплексном последний целесообразно представить в идее интегрального показателя качества вида

$$\hat{E} = \grave{a}_{\tilde{n}}\tilde{N} + \grave{a}_{ç}Ç + \grave{a}_{i}\acute{I} \quad , \qquad (1)$$

где C — экономический единичный показатель качества (стоимость) ТИПК, $З$ и $Н$ — единичные показатели назначения ТИПК (соответственно степени защиты информации и надёжности), $a_с$, $a_з$, $a_н$ — весовые коэффициенты при единичных показателях качества, определяемые методом экспертных оценок или социологическим опросом потребителей, причём

$$\grave{a}_{\tilde{n}} + \grave{a}_{ç} + \grave{a}_{i} = 1 \qquad (2)$$

Нагляднее всего интегральный показатель качества оценивать по 10-балльной шкале (наивысшее качество — 10 баллов). Для сведения разноплановых единиц измерений единичных показателей качества к стандартной форме последние также удобно оценивать по шкалам балльных оценок, как это сделано ниже. В этих условиях целью настоящей работы является подтверждение возможности практической оценки интегрального показателя $К$ качества ТИПК.

Для решения поставленной задачи оценим интегральный показатель качества ТИПК двух белорусских производителей-конкурентов — ПО «Интеграл» и УП «ЦНИИТУ» [1–5]. Для этих карт экономическим единичным показателем выбираем себестоимость (для обеих ТИПК она равна примерно 2 $), показателем степени защиты информации — разрядность индивидуального ключа карты (ИКК) из конструкторской документации (48 разрядов для изделий ПО «Интеграл» и 256 разрядов для изделий УП «ЦНИИТУ», [1–5]), показателем надёжности — проектную среднюю наработку до отказа (СНО) чипа карты из его конструкторской документации (258 лет для карт ПО «Интеграл» и 114 лет для карт УП «ЦНИИТУ», [1–5]). Шкалы балльных оценок единичных показателей приведены в табл. 1.

Таблица 1. **Шкалы балльных оценок единичных показателей**

	Значения		
Себестоимость, $	Более 3	От 1 до 3	Менее 1
Разрядность ИКК	До 50	От 50 до 250	Более 250
СНО, лет	До 100	От 100 до 300	Более 300
Балл	2	5	10

Весовые коэффициенты при единичных показателях качества, определённые методом экспертных оценок, равны $\grave{a}_{\tilde{n}} = 0{,}25; \grave{a}_{\varsigma} = 0{,}5; \grave{a}_{i} = 0{,}25;$

В этом случае результаты расчета интегрального показателя качества по формуле (1) при вышеопределенных исходных данных представлены в табл. 2

Таблица 2. **Результаты расчета интегрального показателя качества**

	Карты УП «ЦНИИТУ»	Карты НПО «Интеграл»
Себестоимость, $	1,25 балла	1,25 балла
Разрядность ИКК	1,5 балла	1 балл
СНО, лет	1,25 балла	1,25 балла
Итого	5 баллов	3,5 балла

Таким образом, сравнение таксофонных электронных пластиковых карточек УП «ЦНИИТУ» и НПО «Интеграл» по величине интегрального показателя качества показывает, что карты УП «ЦНИИТУ» имеют более высокую оценку качества (5 баллов), чем карты НПО «Интеграл» (3,5 балла). Без применения интегрального показателя качества сравнение изделий УП «ЦНИИТУ» НПО «Интеграл» по отдельным единичным показателям дало бы неопределенный результат. Действительно, при одинаковой себестоимости защищенность информации в картах УП «ЦНИИТУ» выше, чем в картах НПО «Интеграл», однако надежность их ниже. Это показывает целесообразность и возможность применения предложенного интегрального показателя для сравнения качества таксофонных электронных пластиковых карт.

Литература

1. Вечер Д.В., Таболич Т.Г. Оценка фактической надежности телефонных ЭПК относительно перемежающихся отказов//Известия Белорусской Инженерной Академии. 2003. Вып. 1(15)/3. Ч. 3. С. 60–62.
2. Вечер Д.В., Прибыльский А.В., Реуцкий В.С., Таболич Т.Г. Сравнение кристаллов пластиковых карт по степени защиты информации // Доклады БГУИР. 2003. №. С. 31–32.
3. Вечер Д.В., Таболич Т.Г. Сравнение проектной надёжности ИМС телефонных карт с различной степенью защиты информации // Доклады БГУИР. 2004. № 5. С. 62–63.

ВНЕШНИЙ АКТИВНЫЙ АУДИТ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

В.В. АНИЩЕНКО, Ю.В. ЗЕМЦОВ

В настоящее время все более востребованной на рынке информационной безопасности становится услуга внешнего активного аудита безопасности корпоративной сети. Данный вид аудита представляет собой моделирование действий злоумышленника, намеренного проникнуть в корпоративную сеть извне. При этом аудитор искусственно ставится именно в те условия, в которых работает злоумышленник, – ему предоставляется только та информация, которую можно раздобыть в открытых источниках. Естественно, атаки только моделируются и не оказывают де-

структивного воздействия на корпоративную сеть. Результатом внешнего активного аудита является информация об уязвимостях, степени их критичности и методах устранения, сведения о широкодоступной информации (информация, доступная любому потенциальному нарушителю) сети.

Объектами внешнего активного аудит обычно являются корпоративные сети и Web-сайты. Однако не так давно появилась новая методика – имитация атаки на внутренних пользователей системы путем применения реверсивных "троянских коней". Эта прогрессивная технология взлома, в которой используются уязвимости клиентского ПО рабочих станций и методы социальной инженерии, позволяет проникать в защищенные корпоративные сети и контролировать их изнутри. По сути, она дискредитировала концепцию защиты от атак путем обеспечения безопасности только внешнего периметра сети, вынудив защищать каждое рабочее место с помощью комплекса мер верхнего уровня в соответствии со стандартом ISO 17799.

В данной работе описывается процесс проведения внешнего активного аудита безопасности корпоративной сети, анализируется ее структура, функции и особенности, выявляются наиболее значимые угрозы информационной безопасности и основные пути их реализации, а также проводится проверка возможности получения несанкционированного доступа к данным, несанкционированной модификации данных и нарушения работоспособности тестовой корпоративной сети.

ФИЛЬТРАЦИЯ ЛОЖНЫХ СИГНАЛОВ ТРЕВОГИ С ПОМОЩЬЮ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

В.В. АНИЩЕНКО, Ю.В. ЗЕМЦОВ

В последнее время наблюдалась тенденция к использованию методов интеллектуального анализа данных в области обнаружения атак на продукты и системы информационных технологий. Предлагаемые подходы чаще всего базировались на применении того или иного алгоритма интеллектуального анализа данных для обнаружения аномалий, которые связывались со злонамеренной активностью. В некоторых работах предлагалось даже заменить существующие методы выявления атак методами обнаружения аномальной активности, основанными на технологии интеллектуального анализа данных. Однако, за исключением отдельных узких областей, таких как обнаружение широко распространенных "червей", практического применения подобные подходы не получили. Связанно это главным образом с их невысокой эффективностью, а также сложностью сбора данных, пригодных для последующего анализа.

В тоже время, основанные на правилах методы выявления атак, являющиеся наиболее эффективными на сегодняшний день, имеют существенный недостаток, заключающийся в общем характере этих правил, что приводит к большому количеству ложных срабатываний. Уменьшение количества ложных сигналов тревоги обычно достигается за счет ухудшения качества обнаружения.

В данной работе предлагается оригинальный подход к редуцированию количества ложных срабатываний для систем обнаружения атак, основанных на правилах. Суть подхода состоит в использовании технологии интеллектуального анализа не для самого процесса выявления атак,

а исключительно для фильтрации ложных сигналов тревоги. Проводя интеллектуальный анализ данных, сгенерированных системой обнаружения атак за время обучения, можно выявить схожие группы сигналов тревоги (базовые кластеры). Затем, вычисляя отклонения групп сигналов тревоги, выявленных за последующие периоды времени от базовых кластеров, можно выделить сигналы тревоги, которые действительно представляют интерес.

НЕКОГЕРЕНТНЫЙ АЛГОРИТМ ОБРАБОТКИ ШУМОПОДОБНОГО СИГНАЛА В СОВМЕЩЁННОЙ СИСТЕМЕ ПЕРЕДАЧИ ИНФОРМАЦИИ

В. В. ДУБРОВСКИЙ

Отличительными особенностями предлагаемого алгоритма являются: отсутствие цепей фазовой автоподстройки частоты (ФАП) опорного гармонического колебания и схемы слежения за задержкой (ССЗ) псевдослучайной последовательности (ПСП) ; квадратурная обработка смеси сигнала и шума; ориентация на цифровые методы выделения информации. В качестве полезного сигнала выступает узкополосный процесс, у которого амплитуда определяется тремя мультипликативными составляющими: постоянным числом a_0 – в реальных каналах связи оно может медленно изменяться; бинарной информационной последовательностью (ИП) $X(t)$, принимающей значения ± 1; ПСП $g(t)$, значения которой также принадлежат множеству ± 1. В течение длительности элемента ИП T должно укладываться целое число элементов ПСП $\tau_э$. Очевидно, что для повышения энергетической и структурной скрытности, необходимо, чтобы $T/\tau_э >> 1$. Полная фаза процесса состоит из трёх слагаемых: линейно нарастающего со скоростью ω_0; медленно меняющегося по сравнению с $\tau_э$ (обозначим его $\varphi(t)$) и пропорционального интегралу от некоторого аналогового сообщения, что определяет частотную модуляцию; константы, отображающей случайную равномерно распределенную начальную фазу.

Основной замысел и новизна предлагаемого алгоритма обработки состоит в преломлении теории совместной фильтрации на квадратурную обработку. Это позволяет синтезировать эффективные алгоритмы *некогерентной* обработки, приближающиеся по помехоустойчивости к квазикогерентным. Применение обратной связи по решению позволяет осуществить демодуляцию сложного совмещённого сигнала на фоне как аддитивных, так и мультипликативных помех. В таком сигнале информация закладывается и в амплитуде, и в фазе (частоте), что существенно повышает эффективность использования канала связи. Отметим важные аспекты работы схемы. Входная смесь при перемножении на опорные гармонические колебания, сдвинутые по фазе на $\pi/2$, расщепляются на два ортогональных процесса. Всю схему можно условно разделить на две части. Первая выделяет тактовую частоту, подаваемую на формирователь ПСП, и осуществляет свёртку смеси и шумоподобного сигнала. Выделение тактовой частоты осуществляется перемножением сигнала на самого себя, задержанного на $\tau_э/2$, т. е. применён автокорреляционный приём, что избавляет от необходимости использования ССЗ. Вторая часть осуществляет собственно демодуляцию совмещенного сигнала. Особенность выделения дискретной информации состоит в том, что в каждом квадратурном канале при использовании обратной связи по дискретному параметру $X(t)$

формируются с заданной точностью значения cos и sin от начальной фазы. После их перемножения на свою квадратуру и последующего суммирования удаётся избавиться от влияния начальной фазы, таким образом, она не сказывается на качестве различения. Отметим, однако, что проблему обратной работы алгоритм не решает. Схема частотного демодулятора является принципиально новой и упрощённо принцип её работы описывается так: в схеме сформировано значение $\sin[\varphi(t)]$; на малом интервале изменения $\varphi(t)$ значение синуса равно его аргументу; осуществив дифференцирование процесса $\sin[\varphi(t)]$, получаем аналоговый информационный процесс.

Предложенный алгоритм отличается помехоустойчивостью и гибкостью в реализации по отношению к параметрам передаваемого сигнала и канала связи. При наличии априорных сведений, например, о помехах целесообразно адаптировать схему для конкретных условий. Важно, что после разложения на квадратурные компоненты алгоритм допускает полностью цифровую обработку. Так как начальная фаза может медленно меняться, то опорный генератор не управляется схемой ФАП, что исключает присутствие аномальных ошибок демодуляции. Эффективность алгоритма подтверждена численным моделированием.

КОРРЕКТИРУЮЩИЕ ВОЗМОЖНОСТИ УКОРОЧЕННЫХ РС-КОДОВ

В.К. КОНОПЕЛЬКО, В.А. ЛИПНИЦКИЙ

Коды Рида-Соломона (РС-коды) относятся к разряду наиболее популярных как в теории, так и на практике среди помехоустойчивых линейных кодов. Для них доказана возможность коррекции ошибок, кратность которых выходит за пределы кодового расстояния, они удобны для декодирования модулей и пакетов ошибок; для РС-кодов разработаны эффективные норменные методы коррекции ошибок.

Длины классических РС-кодов жестко связаны с порядком конечного поля определения этого кода. Однако на практике приходится учитывать требования технического и технологического плана, что приводит к необходимости использования укороченных РС-кодов. При укорочении кодов обычно теряются важные свойства исходных – полных кодов, как, например, их цикличность. Тем не менее, во многих ситуациях учет связей укороченных кодов с исходным кодом позволяет достаточно полно изучить их свойства и корректирующие возможности.

В докладе рассматриваются некоторые результаты, полученные проекцией теории норм синдромов на укороченные РС-коды. Исследуются части Г-орбит полных кодов, остающиеся после укорочения; для них сохраняются многие результаты теории норм синдромов, что существенно упрощает изучение кодов. Таким образом, в частности, найдена серия укороченных кодов с хорошими декодирующими возможностями на небольших, приемлемых для применений длинах кодов.

О ПРОГРАММНОЙ РЕАЛИЗАЦИИ КРИПТОСИСТЕМЫ МАК-ЭЛИСА– СИДЕЛЬНИКОВА

В.А. ЛИПНИЦКИЙ, А.В. КОСТЕЛЕЦКИЙ

В 1978 году Мак-Элис (McEliece) предложил криптосистему с открытым ключом, основанную на сложности ряда задач теории кодирования. Суть её заключается в следующем. Имеется G — порождающая матрица линейного двоичного $[n, k]$-кода, исправляющего t ошибок и имеющего быстрый алгоритм декодирования. Абонент случайно, равновероятно и независимо выбирает невырожденную матрицу H (размерности $k \times k$) и перестановочную матрицу Γ (размерности $n \times n$). Эта пара матриц — секретный ключ абонента. Матрица $E=HG\Gamma$ — открытый ключ (общедоступный).

Мак-Элис предлагал взять за основу коды Гоппы, затем, по предложению Сидельникова В.М., стали использоваться коды Рида-Маллера, имеющие быстрые алгоритмы кодирования и декодирования.

Коды Рида-Маллера — низкоскоростные, но исправляющие большое число ошибок. Эти коды используется в космических исследованиях (передачи с Марса, связь с “Вояджером” и прочее). Кроме того, криптосистемы, основанные на этом коде, обладают высокой стойкостью к нападению.

Сидельников В.М. предложил модификацию рассматриваемой системы с целью увеличения криптографической стойкости. Абонент случайно, равновероятно и независимо выбирает набор $H=(H_1, H_2, \ldots H_u)$, состоящий из u невырожденных матриц размерности $k \times k$, и перестановочную матрицу Γ размера $un \times un$. Затем образуется набор матриц $E_1=H_1G$, $E_2=H_2G$, …, $E_u=H_uG$, и матрица $E=(E_1 \mid E_2 \mid \ldots \mid E_u)\Gamma$. Матрица E — открытый ключ, пара (H, Γ) — секретный ключ абонента. Также Сидельников разработал алгоритмы декодирования, которые могут исправлять значительно больше чем t ошибок.

Одним из основных препятствий в применении криптосистем с открытым ключом является сложность реализации некоторых этапов (обычно медленное декодирование, как, например, в криптосистеме RSA). В этом плане криптосистема Мак-Элиса – Сидельникова находится в стадии теоретической разработки. В докладе идёт речь об опыте программной реализации этой криптосистемы. В частности, с помощью пакета Mathematica 4.2, разработана программа задания кода Рида-Маллера с заданными параметрами (формирование порождающей и проверочной матриц, получение кодовых слов), программа формирования секретных и открытых ключей в модифицированной криптосистеме Сидельникова. И программа коррекции ошибок в криптосистемах с большим кодовым расстоянием.

ГЕНЕТИЧЕСКИЙ АЛГОРИТМ МАРШРУТИЗАЦИИ ПАКЕТОВ НА ОСНОВЕ РЕКУРСИВНЫХ РАЗВЕРТОК ДЛЯ ЗАЩИТЫ МЕДИАТРАФИКА

А.А. БОРИСКЕВИЧ, В.В. ЛИВОЧКИН, А.А. ПОДЛУЦКИЙ, В.Ю. ЦВЕТКОВ

Распределение медиатрафика критичного к задержкам (содержащего видео- и аудио-компоненты) реализуется в мультисервисных сетях на основе виртуальных каналов и технологии быстрой коммутации паке-

тов. Для уменьшения вероятности перехвата медиаданных, их ответвления и искажения в промежуточных узлах сети эффективным методом является поочередная передача пакетов по нескольким переключающимся виртуальным каналам, выбираемым алгоритмом маршрутизации. Организация множества переключающихся виртуальных каналов в реальном времени проблематична, поскольку сопряжена с перебором маршрутов, требует значительных вычислительных ресурсов и нереализуема с усложнением структуры сети. Для безопасного распределения медиаданных в сети с переключающимися виртуальными каналами предлагается генетический алгоритм маршрутизации пакетов на основе n-мерных рекурсивных разверток. Использование генетического алгоритма для маршрутизации позволяет заменить поиск оптимального решения на основе полного перебора маршрутов эвристическим поиском решения близкого к оптимальному за меньшее число шагов. Для ускорения генетического алгоритма предлагается распределять номера узлов сети в генетических кодах маршрутов с помощью рекурсивных разверток топологии сети. Переход от n-мерного пространства маршрутизации к одномерному в представлении генетических кодов маршрутов осуществляется выбором мерности и шага развертки в соответствие с числом и связностью узлов сети. Использование рекурсивных разверток приводит к увеличению локальной коррелированности номеров узлов сети в пространстве маршрутизации и ускорению генетического алгоритма, организующего виртуальные каналы.

МЕТОД ШИФРОВАНИЯ РЕЧИ И ДАННЫХ НА ОСНОВЕ РЕКУРСИВНЫХ РАЗВЕРТОК И МУАРОВЫХ КЛЮЧЕЙ

А.А. БОРИСКЕВИЧ, В.Ю. ЦВЕТКОВ

Для современных инфокоммуникационных систем и сетей актуальна проблема унификации алгоритмов обработки и распределения различных видов информации, составляющих мультимедийные данные. Представляют интерес универсальные алгоритмы шифрования, эффективные для защиты всех компонент медиаданных – видео, неподвижных изображений, речи, файлов данных. Ключевым вопросом унификации алгоритмов шифрования является представление защищаемой информации в виде, соответствующем структуре выбираемого криптоалгоритма. Предлагается метод защиты речевых сообщений в сетях с коммутацией пакетов, включающий преобразование одномерного пространства речевого сигнала в двумерное посредством рекурсивных разверток и шифрование полученных речевых 2D образов посредством муаровых ключей. Использование рекурсивных разверток для формирования речевых 2D образов обусловлено возможностью сохранения корреляции речевых отсчетов и применения методов визуальной криптографии для защиты речевых фрагментов. Для шифрования предлагается использовать 2D ключи, сформированные на основе муаровых эффектов. Муаровые ключи могут быть использованы также для защиты файлов данных. Преобразование одномерного представления файлов данных в двухмерное может осуществляться посредством как рекурсивных, так и линейных разверток, ввиду отсутствия пространственной корреляции между информационными единицами. Предлагаемый метод визуальной криптографии на основе муа-

ровых ключей и рекурсивных разверток является эффективным для защиты видео, речевой и документальной конференцсвязи.

АДАПТИВНО-ДИНАМИЧЕСКИЙ МЕТОД ВНЕСЕНИЯ ЗАЩИТНЫХ ЭЛЕМЕНТОВ В ВИДЕОИЗОБРАЖЕНИЕ

А.А. БОРИСКЕВИЧ, В.В. ЛИВОЧКИН, А.А. ПОДЛУЦКИЙ, В.Ю. ЦВЕТКОВ

При распространении коммерческих видеоматериалов актуальной проблемой является защита авторских прав. Методы защиты авторских прав основаны на внесении в изображение видимых или не видимых глазом элементов защиты для подтверждения авторства на видеоматериалы. В качестве элементов защиты могут выступать изображения, представляющие авторские знаки. Основными проблемами защиты видеоинформации от несанкционированного использования являются минимизация искажений, вносимых элементами защиты, а также обеспечение устойчивости элементов защиты к различным атакам – искажениям контраста и яркости, аффинным преобразованиям, фильтрации и сжатию. Предлагается новый метод внесения защитных элементов на основе контрастно-яркостной обработки динамически выделяемых при смене кадров однотонных областей изображений. Обработка пикселей выделенной зоны производится в пределах границ элемента защиты с учетом динамического диапазона яркости изображения. В результате образ внедряемого элемента защиты проявляется на фоне выделенной области. Для эффективного поиска и контурной обработки однотонных областей предлагается использовать методы ретинальной фильтрации и модель клеточного автомата. Адаптивность метода внесения элементов защиты состоит в согласовании геометрии выделенных областей и геометрии элементов защиты для качественного восстановления исходного изображения при санкционированном доступе. Поиск элементов защиты на изображениях предлагается осуществлять на основе нейросетевых алгоритмов, быстро локализующих элементы защиты инвариантно к различным преобразованиям изображений. Достоинством предлагаемого метода является устойчивость элементов защиты к различным видам атак, обусловленная непредсказуемым выбором количества и расположения элементов защиты при смене видеокадров, а также использованием площадных образов для формирования элементов защиты. Данный метод эффективен как для авторизованного распределения видеоматериалов по сети, так и для распространения их на цифровых носителях.

ПРИМЕНЕНИЕ ПОМЕХОУСТОЙЧИВЫХ ТУРБО-КОДОВ В СИСТЕМАХ СВЯЗИ

А.В. ШКИЛЕНОК

При передаче данных по каналам связи возможно возникновение ошибок, вследствие воздействия шумов. Если передача данных осуществляется без изменений, возможна потеря целого блока информации, которую затем невозможно восстановить. Поэтому, на протяжении уже длительного времени разрабатываются различные методы кодирования данных, позволяющие избежать потерь при передаче информации.

Хорошие помехоустойчивые корректирующие коды, которые позволяют исправлять несколько комбинаций ошибок, должны удовлетворять некоторым требованиям. Во-первых, ограниченная длина кодового блока, во-вторых, алгоритм декодирования должен иметь малую сложность (программную и аппаратную), в-третьих, должно быть согласование кодов, корректирующих ошибки, видов модуляции, алгоритмов декодирования и характеристик канала связи.

На сегодняшний день найден код, наиболее соответствующий данным требованиям - турбо-код. Главной особенностью турбо-кода является наличие двух или более кодеров рекурсивных сверточных кодов (РСК) и устройств перемежения. Турбо- код представляет собой систематический код, в котором проверочная группа образуется из проверочных битов, генерируемых двумя или более составными кодерами РСК, причем информационная последовательность подается в кодер первого РСК непосредственно, а в кодер второго РСК через устройство псевдослучайного перемежения, и т. д. Для регулирования общей скорости турбо-кода применяется схема выкалывания проверочных бит. Причина высокой помехоустойчивости турбо-кодов лежит в сочетании следующих свойств:

– сильная зависимость веса выходной последовательности РСК от вида входной информационной последовательности, т.е. от порядка расположения нулей и единиц в ней;

– применение перемежителя для изменения вида входной последовательности, подаваемой на входы кодеров составных РСК.

Сочетание этих свойств приводит к тому, что если при подаче определенной информационной последовательности на вход кодера одного РСК вес его проверочной последовательности оказывается малым, то перемеженная версия этой информационной последовательности, подаваемая на вход другого кодера РСК, с высокой вероятностью приведет к генерации проверочной последовательности большого веса из-за указанного выше свойства РСК. Таким образом, если какая-либо комбинация ошибок не может быть исправлена одним РСК, то это почти наверняка будет сделано с помощью проверочной группы другого РСК и наоборот.

Недостатком системы является высокая избыточность каскадного кода и большая задержка информации при декодировании.

СКВОЗНАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ КАНАЛОВ НА ЛОКАЛЬНОЙ СЕТИ

М.П. РЕВОТЮК, К.Е. КОЛОТЫГИН

Прикладные системы, построенные на основе распределенных архитектур, могут нуждаться в организации надежной защиты логических каналов обмена данными на локальной сети. Например, ввод пароля для доступа к СУБД с рабочей станции, использование низкоуровневых интерфейсов доступа к данным могут порождать угрозу перехвата. Система ответственного назначения не должна становиться уязвимой из-за ошибочных или преднамеренных действий административного или технического персонала корпоративной сети, а также недостаточной защищенности ее компонент.

Надежный метод предвосхищения подобных угроз – сквозная защита критической по безопасности информации, базирующаяся на созда-

нии канала VPN (Virtual Privacy Network) по инициативе конечных пользователей. VPN поддерживается Windows 2000/XP/2003. Однако в последнее время доступны несимметричные криптосистемы с аппаратным хранением ключей или даже программ криптоядра на персональных носителях, например, отечественные разработки “CryptoKey 2001”, “EnigmaCrypt” ООО “Энигма”, практически не нуждающиеся в администрировании.

Объект рассмотрения – каналы VPN на основе персональных аппаратных устройств, обеспечивающие независимость уровня скрытия информации от настроек операционной системы, а также физического канала. Для образования защищенного канала на рабочих станциях абонентов должен быть установлен сервис, реализующий дуплексный обмен с шифрованием трафика по выбранному, из соображений технической реализуемости, открытому протоколу транспортного уровня, например, TCP/IP. Такой сервис играет роль локального прокси-сервера между прикладной программой и внешней средой, активизируемого только после предъявления аппаратных устройств абонентами.

Применение несимметричной криптосистемы обеспечивает гарантированную взаимную аутентификацию абонентов канала и снимает проблему управления ключами. После взаимной аутентификации с целью повышения быстродействия шифрования возможен управляемый переход на режим использования симметричного ключа.

Рассмотренный прием использован для построения защиты эксплуатируемых комплексов, соединяемых по открытым интерфейсам RPC (Remote Procedure Call).

ЗАЩИТА ПРОГРАММ ОТ АВТОРИЗОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

М.П.РЕВОТЮК, Е.П. БАЦЕКИНА

Статистика компьютерных преступлений показывают доминирование угроз безопасности от сотрудников организации. Авторизованные пользователи имеют легитимную возможность физического доступа к рабочим станциям и разделяемым файлам локальных вычислительных сетей.

Операционные системы семейства Windows 2000/XP/2003, предоставляя необходимые средства контроля последовательности событий раскрутки вычислительного процесса, начиная от загрузки операционной системы, автоматически не создают достаточные условия безопасности. Объект рассмотрения –специализированные системы динамической защиты программ, обеспечивающие, в частности, организацию фоновой аутентификации, удаленный контроль условий целостности, проверку наличия аппаратного ключа, автоматическое восстановление .

Обрамлением интервала активности пользователя на рабочей станции являются события, контролируемые процессом Winlogon. Обработка событий реализуется динамически подключаемой библиотекой GINA, которая может быть заменена прикладной версией. Для обеспечения стандартной функциональности или поддержки клиентов других операционных систем удобно применить каскадный фильтр операций вызова функций библиотеки. В результате имеется возможность связи стандартных событий с наличием аппаратного идентификатора или ключа.

При этом речь не идет о подмене стандартного интерфейса управления сеансами посредством смарт-карт, а об усилении набора условий запуска прикладной программы.

Взаимосвязь агентов контроля и восстановления, размещаемых на сети, обеспечивается построением взаимно аутентифицированной связи “клиент-сервер” на основе SSPI, где обе стороны представлены стандартными учетными записями LSA. Ввиду доступности процессу Winlogon сети до и после обмена контекстами безопасности, возможно использование сертифицированных протоколов криптозащиты. Включение в пакет дополнительной аутентификации условия отказа в открытии сеанса вне регламента эксплуатации рабочей станции или сервера используется как прием скрытия активизируемых элементов системы или защиты критических ресурсов системы.

АКТИВНАЯ ЗАЩИТА ИСПОЛНЯЕМЫХ МОДУЛЕЙ ОТВЕТСТВЕННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

М.П. РЕВОТЮК, Т.А. ЖИРКО, А.П. КИШКЕВИЧ

Исполняемые модули ответственных систем обработки информации, представленные загрузочными файлами или файлами динамически подключаемых библиотек с открытым форматом PE (Portable Executable) в среде операционных систем Windows уязвимы для ряда угроз несанкционированного использования – копирования, дизассемблирования, модификации и запуска. Один из приемов защиты – связь процесса исполнения программного кода с сервисами группы AAA(Авторизация, Аутентификация, Аудит), рекомендуемых для создания серверных приложений.

Однако технологии создания серверных приложений не защищают файлы исполняемых модулей от дизассемблирования, трассировки или других угроз, реализуемых после получения файла. Кардинальным решением задач противодействия таким угрозам может быть криптографическая защита фрагментов кода.

Так как применение криптографии само по должно быть связано с состоянием аутентификации, то естественно образовать рекуррентную схему его связи с хотя бы одним предшествующим и остальными доступными для фиксации состояниями. Показано, что, используя криптографию с открытым ключом и реально доступные системные события, возможно до этапа инсталляции на ЭВМ построение динамической системы, привязанной к моменту аутентификации, функционирующей только при нулевых масках доступа к процессу лишь при предъявлении ключа зарегистрированного конечного пользователя.

Файл программы выступает как контейнер для хранения скрытых блоков кода. Преобразование кода выполняется в последний момент непосредственно перед использованием в проекции на память. Для проверки и установки в любой момент общесистемных условий целостности и безопасности на рабочей станции программа должна заимствовать на этапе инсталляции право использования строго регламентированных, но достаточных для самозащиты, административных привилегий.

ЗАЩИТА РАСПРЕДЕЛЕННЫХ КООПЕРАТИВНЫХ ВЫЧИСЛЕНИЙ НА ЛОКАЛЬНЫХ СЕТЯХ

М.П. РЕВОТЮК, Н.В. ХАДЖИНОВА

Решение разовых или эпизодически возникающих задач повышенной вычислительной сложности часто удобно проводить по кооперативной схеме использования потенциально доступных ресурсов вычислительной сети. Однако распределение вычислений даже на локальной сети создает угрозу безопасности – модификация кода и данных на отдельных рабочих станциях легко реализуема штатными средствами операционных систем.

Предмет исследования — защита распределенных вычислений двумя взаимосвязанными способами: трансформация представления задачи и обеспечение безопасности вычислительных процессов.

Трансформация представления задачи основана на преобразованиях исходных данных, скрывающих смысл решаемой задачи. Например, для квадратичной задачи о назначении, задач коммивояжера или размещения транспортного типа возможна модификация матрицы стоимости посредством операции приведения с переставленными строками и столбцами. Приведение матриц небесполезно технологически и для реализации итераций метода ветвей и границ. Восстановление смысла задачи без знания вектора перестановок имеет экспоненциальную вычислительную сложность.

Защита вычислительных процессов для кооперативных схем возможна без рассмотрения их содержания при установлении доверительных отношений с резидентом (агентом-диспетчером). Учитывая, что кооперативные вычисления реализуют жадный алгоритм потребления потенциально доступных процессоров на сети, естественным является создание шаблона системы агентов на основе безопасной абстрактной машины, его реализация в рамках объектно-ориентированных технологий и последующая специализация под условия применения.

Практическая реализация системы защиты апробирована в среде Windows NT/2000/XP для кооперации ресурсов ЭВМ на уровне протокола TCP/IP.

СЕКЦИЯ 4. ПРОЕКТИРОВАНИЕ И ПРОИЗВОДСТВО ЭЛЕМЕНТОВ И КОМПОНЕНТОВ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

УГЛЕРОДНЫЕ НАНОТРУБКИ ДЛЯ СВЕРХБЫСТРОДЕЙСТВУЮЩИХ ТРАНЗИСТОРОВ – ЭЛЕМЕНТНОЙ БАЗЫ ИНФОРМАЦИОННЫХ СИСТЕМ БУДУЩЕГО ПОКОЛЕНИЯ

Е.Л. ПРУДНИКОВА

В настоящее время происходит переход от микро- к наноэлектронике, осуществляемый двумя путями — "сверху вниз" и "снизу вверх". Первый путь осуществляется за счет уменьшения размеров транзисторов кремниевых интегральных схем (ИС). В настоящее время уже существуют МОП-транзисторы с расстоянием исток-сток 65 нм. Однако этот путь требует огромных финансовых затрат. Наиболее приемлемым для наших условий является второй путь, когда при достаточно больших размерах транзисторов их функциональные возможности и быстродействие расширяются за счёт использования специально разработанных наноструктурированных неорганических и функциональных органических материалов. Наиболее перспективными для этой цели являются углеродные нанотрубки (УНТ). Несмотря на то, что к настоящему моменту разработано большое количество оптимизированных методов синтеза данных УНТ, как правило, полученный материал неоднороден и содержит различной природы примеси (остатки катализатора, аморфный углерод, фуллерены и другие наночастицы), а сами нанотрубки спутаны, что не позволяет получить отдельные УНТ, пригодные для использования в качестве элементов транзисторов. Следовательно, проблемы очистки, сепарации, а также манипулирования УНТ являются актуальными.

В настоящей работе проведены исследования процессов очистки и сепарации ориентированных массивов УНТ, полученных методом каталитического пиролиза жидких углеводородов (1%-раствор ферроцена в о-ксилоле) при атмосферном давлении, с целью использования в качестве каналов МОП-транзисторов. Для получения отдельных нанотрубок проводилось ультразвуковое диспергирование (10 мВт) в поверхностно-активных веществах (додецилсульфат натрия), органических растворителях (ацетон, толуол, изопропиловый спирт) и кислотных смесях (H_2SO_4:HNO_3 в соотношении 3:1). Образцы исследовали с помощью растровой электронной микроскопии и спектроскопии комбинационного рассеяния. Результаты показали высокую степень разделения исходных массивов на отдельные нанотрубки, что позволит их ориентировать и локализовать из суспензии на системе электродов для исследования электрофизических свойств с целью дальнейшей интеграции в наноэлектронные устройства.

АНАЛИЗ ЭЛЕМЕНТНОЙ БАЗЫ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОМ ЦЕНТРЕ "БЕЛМИКРОАНАЛИЗ"

В.А. ЕМЕЛЬЯНОВ, В.Н. ПОНОМАРЬ, Г.Г. ЧИГИРЬ, В.А. УХОВ

Для повышения эффективности применения, разработки новой элементной базы систем защиты информации требуется комплекс аналитического оборудования для всестороннего анализа параметров. Так как, спектр исследуемых объектов весьма широк, то комплекс оборудования должен иметь возможность анализировать широкий набор физических параметров, иметь возможность при необходимости быстро и достоверно получать необходимую информацию. Наиболее быстро и эффективно такие работы можно выполнить, когда все необходимое аналитическое оборудование сконцентрировано в одном месте, например, как в Государственном центре (ГЦ) "Белмикроанализ".

ГЦ "Белмикроанализ" НПО "Интеграл" Республики Беларусь оснащен современным компьютеризованным аналитическим оборудованием для проведения качественного и количественного анализа состава материалов, исследования структурно-морфологических и электрофизических характеристик различных материалов изделий микроэлектроники и других объектов: вторично-ионный масс-спектрометр IMS-4F ф. Cameca (Франция), электронный Оже-спектрометр PHI-660 ф. Perkin Elmer (США), растровый электронный микроскоп Stereoscan-360 ф. Cambridge Instruments (Англия) со встроенным энергетическим спектрометром AN 10000 ф. Link Analytical, просвечивающий электронный микроскоп H-800 ф. Hitachi (Япония), программно-аппаратный комплекс прецизионных измерений вольтамперных (I–V) и вольтфарадных (C–V) характеристик элементной базы ИМС, программно-аппаратный комплекс для получения цифровых изображений, тепловизионная система Thermovision 880 ф. Agema (Швеция) и др.

ЦИФРОВАЯ ОПТИЧЕСКАЯ МИКРОСКОПИЯ В ПРОИЗВОДСТВЕ ЭЛЕМЕНТНОЙ БАЗЫ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. ЕМЕЛЬЯНОВ, В.Н. ПОНОМАРЬ, Г.Г. ЧИГИРЬ

При переходе к микросхемам с субмикронными проектными нормами использование традиционных оптических микроскопов становится практически невозможным из-за низкого разрешения и ограниченного увеличения.

В данной работе показана возможность использования оптических микроскопов улучшенной конструкции для обеспечения операционного контроля в технологии субмикронных микросхем. Для получения высококачественных оцифрованных изображений элементов сформирован цифровой оптический микроскоп на основе микроскопа ф. Leica INM100 с набором высокоразрешающих объективов PL APO (1,6×, 2,5×, 5×, 10×, 20×, 50×, 100×, 150×), прецизионным сканирующим столиком LSTEP13, цифровой камерой Polaroid DMC Ie с разрешением матрицы 1600×1200 пикселей, управляющим компьютером на платформе Windows с интерфейсом SCSI-II.

Сформированные фрагменты топологии ИМС показывают, что микроскоп обеспечивает контроль элементов топологии до 0,3 мкм без специального препарирования образца и его разрушения. При этом образец может быть взят на любой стадии изготовления ИМС и после проведения контроля его можно использовать в дальнейшем технологическом процессе.

Таким образом, цифровая оптическая микроскопия обеспечивает неразрушающий контроль пластин субмикронных ИМС на любой стадии их изготовления при отсутствии необходимости препарирования образцов, широкую возможность по обработке цифровой информации, ее хранению и передаче по электронной сети.

АНАЛИЗ МИКРОЭЛЕКТРОННЫХ СТРУКТУР С ВЫСОКИМ ПРОСТРАНСТВЕННЫМ РАЗРЕШЕНИЕМ

В.А. ЕМЕЛЬЯНОВ, В.Н. ПОНОМАРЬ, В.А. УХОВ, В.П. ЛЕСНИКОВА

Разработка и промышленный выпуск микросхем с размерами элементов
0,1–0,5 мкм невозможна без применения информативных методов их анализа.. Методы растровой электронной микроскопии могут в ряде случаев оказаться неприемлемым из-за ограничений, связанных с декорированием в химических травителях. Это неизбежно влечет за собой ошибки при переходе к субмикронному и нанометровому диапазону размеров элементов. Методом, который обеспечивает нанометровое разрешение, является просвечивающая электронная микроскопия вертикальных сечений — ПЭМ-скол.

В данной работе для подготовки вертикальных сечений использовались различные механические обработки и финишное утонение ионным пучком. Использование такой комбинации методов является наиболее универсальным, так как способствует минимизации эффектов, связанных с различными свойствами материалов, входящих в многослойные системы, какими являются микросхемы. Изучены и установлены оптимальные условия проведения каждой операции, подробное описание последовательности действий при их выполнении отражены в соответствующих методиках.

Результаты настоящей работы показывают, что ПЭМ-сколы могут использоваться как уникальный способ выявления и прямого наблюдения структуры вертикальных сечений микросхем, степени структурного совершенства кремния, особенностей процессов твердофазного взаимодействия в контактных системах. Применение ПЭМ-сколов позволит с высоким разрешением определять геометрические характеристики технологических слоев и топологических элементов, позволяя получать информацию, которая в ряде случаев недоступна никаким другим методам.

ЭЛЕКТРОПИТАНИЕ МОБИЛЬНОГО КОМПЛЕКСА КОНТРОЛЯ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ

Р.Н. МАКСИМОВИЧ, В.А. ПОПОВ

Питание мобильного комплекса должно обеспечиваться, как от сети 220 В (50 Гц), так и от автономного источника (аккумулятора). Источник питания мобильного комплекса должен иметь минимальные габариты и массу, и обеспечивать время непрерывной работы комплекса в автономном режиме не менее 4-х часов, при потребляемой мощности 10 Вт. Учитывая выше изложенные требования, для источника питания были выбраны литий-ионные (Li-ion) аккумуляторы, обладающие большей энергоемкостью, при аналогичных размерах и массе по сравнению с другими аккумуляторами. Примененные Li-ion аккумуляторы, типа CGR18650A с номинальной емкостью 2000 мА·ч и номинальным напряжением 3,6 В, соединены последовательно в батарею из двух элементов. Для заряда используется метод "постоянное напряжение/постоянный ток", причем каждый из последовательно соединенных аккумуляторов имеет свое зарядное устройство и свою схему мониторинга питания, что позволило упростить схему управления зарядом.

Структурно источник питания состоит из следующих основных частей: двух адаптеров AC/DC (~85…240 В→5 В/1,5 А), встроенных в комплекс; двух схем заряда, реализующих метод "постоянное напряжение/постоянный ток", с токовым ограничением и возможностью прекращения заряда; двух схем мониторинга питания.

Суммарное напряжение с батареи аккумуляторов поступает на преобразователи DC/DC, которые формируют выходные напряжения (+15 В/150 мА, −15 В/150 мА, +5 В/1А), необходимые для работы комплекса. Работоспособность преобразователей обеспечивается при входных напряжениях от 4 В до 9 В, что дает возможность работать комплексу от одного аккумулятора, а также использовать USB-порт персонального компьютера, входящего в состав комплекса, для подзарядки аккумулятора.

Заряд аккумуляторов может осуществляться, как при работающем комплексе, так и при выключенном. Время полного заряда аккумуляторов при выключенном комплексе составляет 4 ч. Для предотвращения разряда аккумуляторов через цепи утечки, предусмотрено его полное гальваническое отключение, при отсоединении комплекса от сети 220 В. Источник питания позволяет работать комплексу без аккумуляторов, от сети 220 В (50 Гц), при этом адаптеры и схемы заряда питают преобразователи DC/DC(±15 В; +5В) постоянным напряжением 8,4 В.

ИСТОЧНИКИ ОДИНОЧНЫХ ФОТОНОВ ДЛЯ КВАНТОВОЙ КРИПТОГРАФИИ: *AB INITIO* ИССЛЕДОВАНИЕ ОДИНОЧНЫХ NV^--ЦЕНТРОВ В НАНОАЛМАЗЕ

В.А. ПУШКАРЧУК, С.Я. КИЛИН, А.П. НИЗОВЦЕВ,
А.Л. ПУШКАРЧУК, В.Е. БОРИСЕНКО, А.Б. ФИЛОНОВ

Благодаря активно ведущимся в мире работам по разработке "аппаратных" средств для квантовой криптографии, основной особенностью которой является обеспечиваемая физическими законами природы невозможность перехвата передаваемой информации, в последние годы был реализован ряд предложенных протоколов и на мировом рынке появились первые, коммерчески реализуемые квантово-криптографические системы [1].

Центральным элементом таких систем является источник излучения, позволяющий генерировать одиночные фотоны в нужные моменты

времени. В качестве кандидатов для этого изучаются различные одиночные квантовые объекты в твердых телах (см. например, спецвыпуск журнала [2]), среди которых одним из наиболее перспективных являются одиночные дефекты "азот-вакансия" (NV^--центры) в нанокристаллах алмаза, которые являются исключительно фотостабильными даже при комнатной температуре. Для оптимизации их работы в качестве генераторов одиночных фотонов исключительно важно детально знать фотофизические, структурные, спиновые и пр. свойства NV^--центров в наноалмазах [3].

В связи с этим в данной работе проведено комплексное теоретическое исследование электронных и спиновых свойств различных нанокристаллов углеродасодержащих NV^--центры. Моделирование свойств указанных кластеров проводили в рамках *ab initio* и полуэмпирических квантовохимических методов. Для расчета выбирались бездефектные и с наличием NV^--центров углеродные кластеры как пассивированные водородом ($C_{38}H_{42}$, $C_{71}H_{84}$, $C_{86}H_{78}$) так и со свободной поверхностью (C_{38}, C_{71}, C_{86}). Исследование свойств негидрогнизированных нанокластеров углерода проводилось впервые. Показано, что в случае углеродных нанокристаллов, пассивированных атомами водорода, формируются алмазоподобные кластеры. Атомарное строение нанокристаллов, непассивированных атомами водорода зависит от числа атомов и начальных геометрических параметров кластера и в некоторых случаях образуются кластеры с фуллерено-подобной поверхностью. В случае нанокристаллов алмаза, пассивированных атомами водорода сверхтонкое взаимодействие обусловлено локализацией спиновой плотности на ядрах атомов являющихся ближайшими соседями NV^--центра. Для углеродных нанокристаллов, непассивированных атомами водорода, сверхтонкое взаимодействие обусловлено локализацией спиновой плотности на ядрах атомов формирующих поверхность нанокристалла.

Литература

1. J.Ouellette // The Industrial Physicist, Dec.-Jan. 2004 24.
2. New J. Of Physics, 2004, 6.
3. Пушкарчук В.А., Килин С.Я., Низовцев А.П., Пушкарчук А.Л., Борисенко В.Е., von Borczyskowski C., Филонов А.Б. // Оптика и спектроскопия, (принята к публикации).

СКРЫТЫЕ ЛЮМИНЕСЦИРУЮЩИЕ ИЗОБРАЖЕНИЯ

Д.А. ЦИРКУНОВ, И.С. МОЛЧАН, Г.К. МАЛЯРЕВИЧ, Н.В. ГАПОНЕНКО

Представляется возможность формирования люминесцирующих изображений с помощью электрохимического анодирования алюминия (формирования пористого анодного оксида алюминия) и золь-гель синтеза [1-3]. Получение люминесцирующих изображений осуществлялось посредством литографии с последующим анодированием алюминия через резистивную маску. Второй способ получения изображений отличается тем, что вначале проводится анодирование всей поверхности алюминия, а литография выполняется на слое пористого анодного оксида алюминия. Далее производилось заполнение проанодированных участков золем, содержащим ионы лантаноидов. Для активации ионов лантаноидов проводилась температурная обработка. В качестве исходных образцов можно использовать алюминиевую фольгу, а также подложку с напыленным слоем алюминия.

Использование золей различного состава, легированных тербием, европием и эрбием позволяет получать люминесцирующие изображения в зеленом, красном и инфракрасном диапазонах. Совместное использование нескольких типов лантаноидов при возбуждении от одного источника, может быть использовано для получения многоцветных изображений. В качестве источника возбуждения изображения пригоден любой источник ультрафиолетового излучения, что позволяет наблюдать видимую невооруженным глазом люминесценцию, интенсивность которой возрастает с увеличением мощности возбуждения.

Проведена работа по использованию данного способа для формирования скрытых изображений на твердых поверхностях, обладающих повышенной стойкостью к изменению атмосферных условий и температуры.

Работа выполняется при поддержке проекта МНТЦ В-276-2.

Литература

1. И.С. Молчан, Оптические свойства европий- и тербийсодержащих оксидных пленок, сформированных золь-гель методом в пористом анодном оксиде алюминия, Дис. к. ф.-м. н., Мн., 2003. —158 с.
2. Н.В. Гапоненко, Пленки, сформированные золь-гель методом на полупроводниках и в мезопористых матрицах, Мн.: Бел. наука, 2003. – 136 с.
3. Н.В. Гапоненко, Формирование пленочных структур золь-гель методом, их свойства и применение в микроэлектронике, Дис. д. ф.-м. н., Мн., 2004. – 249 с.

МОДЕЛИРОВАНИЕ В СРЕДЕ MATLAB ДИСКРЕТНЫХ СИСТЕМ С ФАЗОВЫМ УПРАВЛЕНИЕМ

Л.В. РУСАК, В.Л. БУСЬКО

Система MATLAB (математическая лаборатория) создавалась как язык программирования высокого уровня для технических вычислений. MATLAB является незаменимым средством проведения научных расчетных исследований. Рассмотрим алгоритм в целом, лежащий в основе модели дискретных систем с фазовым управлением (ДСФУ).

При рассмотрении обобщенной структуры ДСФУ выделяется совокупность модулей. Каждый модуль реализуется как отдельная функция. Все модули связываются вместе отдельной функцией, которая обеспечивает взаимосвязь модулей, а так же общее управление работой модели.

Рассмотрим работу алгоритма. Первый этап – выбор параметров системы и их ввод. Ввод осуществляется заполнением списка констант в теле основного модуля. Решение системы производиться в главном модуле, а описание же находится в отдельном модуле. В ходе решения системы ДУ получаемые значения сохраняются для последующей выдачи пользователю и параллельно анализируются модулем обратной связи, для определения факта прихода импульса из цепи обратной связи.

В момент окончания процесса решения системы ДУ, анализируется процесс прерывания. Этот процесс продолжается до тех пор, пока текущее время не совпадет с заданным временем на моделирование. После этого результаты моделирования выводятся на экран.

Фазовый детектор, с точки зрения моделирования, не является сложным звеном и может описываться алгоритмом, реализованным в рамках языка MATLAB.

Рассматривалась реакция системы на переключение делителя частоты цепи ОС от 1564 до 1600.

Моделирование дает возможность изучить системы которые подвергаются исследованию. При получении моделей упрощается процесс

исследования, так как можно изучить реакцию системы на те или иные воздействия, промоделировать систему на работоспособность в различных условиях.

ЭЛЕМЕНТЫ КВАНТОВОЙ ЛОГИКИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Д.А. ПОДРЯБИНКИН, А.Л. ДАНИЛЮК

Основу квантовой криптографии составляет квантовая рассылка ключа QKD (Quantum Key Distribution). Надежность метода основа на законах квантовой механики и связана с невозможностью отвода сигнала с передающей линии. Любая попытка вмешаться в процесс передачи сигнала вызовет непомерно высокий уровень ошибок. Степень надежности в данной методике выше, чем в случае применения алгоритмов с парными ключами (например, RSA).

В данной работе мы предлагаем элемент, обеспечивающий обработку квантовой информации. Нами спроектирован квантовый вычислительный кластер ансамблевого типа на основе кремниевой ступенчатой структуры, содержащей цепочки магнитного изотопа кремния. Кластер предназначен для обработки информации с помощью алгоритма Шора. С помощью этого алгоритма определяется разложение N-значного числа на простые множители за время порядка N^3. Время, необходимое для этого любому классическому компьютеру, растет с N быстрее, чем любая его степень.

Кластер с ансамблевым обращением к кубитам не требует использования высокочувствительной и дорогой аппаратуры для обращения к кубитам. Разделение резонансных частот между цепочками ядерных спинов магнитных изотопов кремния осуществляется с помощью градиента магнитного поля на величину, превышающую частоту их диполь-дипольной связи, а поляризация ядерных спинов – путем возбуждения электронных переходов в наноразмерных областях кремния. Запись и считывание информации с такого вычислительного кластера производиться с помощью методов магниторезонансной силовой микроскопии.

С помощью расчетов показана возможность применения кремниевой ступенчатой структуры, содержащей цепочки магнитного изотопа кремния для создания квантового вычислительного кластера ансамблевого типа. Установлено, что разделение резонансных частот ансамблевых кубит в кремниевом вычислительном кластере эффективно при расстоянии между кубитами 2–3 нм. При этом необходимая величина градиента магнитного поля составляет 0,04 Тл/мкм.

СИНХРОНИЗАЦИЯ АНСАМБЛЯ КУБИТ ПРИ НЕПРЕРЫВНЫХ КВАНТОВЫХ ИЗМЕРЕНИЯХ

А.Л. ДАНИЛЮК, И.Н. ТИТОВИЧ

Разработка систем квантовых вычислений является актуальной задачей для построения квантовых каналов связи, квантовой криптографии и защиты информации на квантовом уровне. В настоящее время на этом пути существуют серьезные проблемы, связанные с подавлением декогеренции квантовых состояний, инициализацией кубит в основное ба-

зисное состояние, записью и считыванием информации во время и после процесса квантовых вычислений. Проблема декогеренции ансамбля кубит существенно ограничивает возможности квантовых вычислительных систем и ведет к уменьшению эффективного числа кубит. Перспективным для решения этих задач является использование непрерывных слабых квантовых измерений, которые не разрушают суперпозицию квантовых состояний. Их применение дает возможность контроля состояний кубит во время вычислений, но является дополнительным фактором потери когерентности квантовых состояний. Подавить декогеренцию можно путем синхронизации внешних резонансных воздействий с эволюцией системы кубит, находящейся в условиях непрерывных измерений во время процесса вычислений.

В работе на основе модели цепочки взаимодействующих спинов (ансамбля кубит) исследованы закономерности взаимодействия и синхронизации кубит ансамблевого квантового вычислительного кластера в условиях непрерывных измерений. На основе разработанной модели получены количественные показатели синхронизации системы ансамблевых кубит квантового вычислительного кластера. Анализируются результаты расчета коэффициента диффузии разности фаз электронного и ядерного спинов в процессе вычислений при различных параметрах квантовой системы. Выявлена его связь с точностью измерений и временем декогеренции. На основе расчета коэффициента усиления цепочки связанных спинов, а также отношения сигнал/шум как функции коэффициента связи и точности непрерывных измерений выявлены условия синхронизации ансамбля кубит в условиях непрерывных измерений.

ВЫЧИСЛИТЕЛЬНЫЕ КЛАСТЕРЫ НА ОСНОВЕ КРЕМНИЯ ДЛЯ КВАНТОВЫХ КАНАЛОВ СВЯЗИ

А.В. КОРОЛЕВ, А.В. КРИВОШЕЕВА, А.Л. ДАНИЛЮК

Необходимость обработки информации на квантовом уровне диктуется перспективностью применения квантовых каналов связи, обладающих существенно более высокой пропускной способностью и защищенностью, которые основаны на принципиально иных свойствах квантовых систем. Принципиальное преимущество квантовых каналов связи по сравнению с классическими заключается в их качественно более высоком уровне защиты: совершенный квантовый канал имеет, в принципе, абсолютную защиту, поскольку любая попытка вмешательства в систему сразу же обнаруживается (квантовый канал связи можно разрушить, но невозможно вскрыть). В то же время на пути создания эффективных систем обработки квантовой информации стоит ряд трудных проблем, связанных с декогеренцией квантовых состояний и синхронизацией квантовых операций. Основным элементом квантового канала связи является квантовый вычислительный кластер.

В данной работе рассмотрены структуры и модели двух квантовых вычислительных кластеров на основе кремния. Первый содержит в качестве ансамблевых кубит квантовые шнуры индия (спин 9/2) на поверхности кремния, не содержащего электрических затворов и примесей. Преимущество подобной системы состоит в возможности организации кроме логических операций NOT, CNOT, AND, XOR, CCNOT также дополни-

тельных функций и ячеек памяти. Во втором кластере в качестве ансамблевых кубит используются наноразмерные слои CaF2, разделенные слоями кремния, очищенными от магнитного изотопа 29Si. Разделение резонансных частот между квантовыми шнурами индия и между слоями CaF2 осуществляется с помощью градиента магнитного поля, создаваемого тонкопленочной магнитной головкой, а поляризация ядерных спинов – путем возбуждения электронов парамагнитных центров в кремнии. Обсуждаются результаты расчетов количественных показателей разделения резонансных частот ансамблевых кубит и подавления декогеренции квантовых состояний, а также расстояния между ансамблевыми кубитами и градиента магнитного поля.

МЕТОДИКА ПОВЫШЕНИЯ УСТОЙЧИВОСТИ РАБОТЫ ИНТЕГРАЛЬНЫХ СХЕМ К ВОЗДЕЙСТВИЮ МОЩНЫХ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ

Н.С. ОБРАЗЦОВ, Д.А. КУЛЕШОВ, А.И. ПИНАЕВ

Последовательность работ по улучшению характеристик устойчивости аппаратуры защиты информации к электромагнитным воздействиям, в состав которых входят ИС состоит из следующих этапов.

Первым этапом повышения электромагнитной совместимости должно быть определение условий воздействия электромагнитного поля. Они определяются путем анализа реальных условий эксплуатации системы, которые предоставляются разработчику РЭС потребителем или определяются опытным путем.

После того, как определены уровни наводок и восприимчивость компонентов, можно сделать оценку восприимчивости в наихудшем случае. Это выполняется путем сравнения ожидаемого максимального уровня наводок с минимальным уровнем сигнала, который вызывает помехи в компоненте. Требования повышения устойчивости определяются отношением ожидаемого уровня наводки к минимальному уровню восприимчивости.

На следующем этапе, в зависимости от требований к повышению устойчивости, определенных на предыдущей стадии, принимается решение о необходимости введения мер по повышению устойчивости системы.

Если отношение меньше 0 дБ, то необходимость защиты от ЭМП отпадает. В случае, когда отношение ненамного больше 0 дБ, примерно до 30 дБ, защита легко обеспечивается экранированием. В противном случае имеет смысл провести более подробный анализ восприимчивости, при этом можно использовать методы моделирования и прогнозирования. Для экономии материалов можно вместо экранирования всего устройства прибегнуть к более тщательному экранированию наиболее уязвимых ее частей, что уменьшить вес и габариты изделия, а следовательно и стоимость.

Повысить устойчивость системы можно. Тщательно проанализировав элементную базу и применив ряд дополнительных элементов, таких как фильтры, прокладки, экранированные кабели, соединители, поглощающие материалы, экраны и т.д.

После использования всех отдельных методов повышения устойчивости следует провести испытание всей системы для проверки эффективности методов повышения устойчивости.

Окончательно систему испытывают при моделировании импульсных воздействий в реальных условиях эксплуатации для того, чтобы она отвечала требованиям ЭМО.

СХЕМОТЕХНИЧЕСКИЕ РЕШЕНИЯ ИМПУЛЬСНОЙ ЗАЩИТЫ НА МОП-ТРАНЗИСТОРАХ

Н.С. ОБРАЗЦОВ, С.Ю. МАКАРЕВИЧ, А.И. ПИНАЕВ

Типовая двухступенчатая схема защиты выводов ИС состоит из полевого транзистора с заземленным каналом, который используется как вторичный защитный элемент для ограничения импульса наводок.

Для обеспечения высокой эффективности данной схемы, необходимо использовать мощную полупроводниковую структуру в качестве главного элемента на первой стадии защиты, такую как электронный ключ либо сапрессор. Между первым и вторым каскадом обычно добавлен резистор для ограничения тока импульсной наводки, протекающего через затвор МОП транзистора на второй стадии защиты. Первичное устройство защиты должно срабатывать до того, как второй каскад выйдет из строя от перенапряжения наводки. В случае, если первичный элемент защиты имеет высокое пробивное напряжение, сопротивление может достигать 1 кОм и более. Большое сопротивление, включенное последовательно и большая емкость элементов защиты вызывает большую задержку входного сигнала, что может отразиться на работе всего цифрового устройства. Поэтому необходимо, по возможности, отказаться от использования последовательно включенного ограничительного сопротивления.

Здесь полевой транзистор с заземленным каналом используется как устройство ограничения импульсных наводок. Однако в этом случае из-за отсутствия сопротивления, ограничивающего ток, эффективность защиты полупроводниковой структуры деградирует с уменьшением геометрических размеров и увеличением степени интеграции ИС из-за того, что полевые транзисторы с заземленным каналом для обеспечения приемлемого уровня защиты должны иметь большие геометрические размеры.

Кроме того, такая структура обладает большой паразитной проходной емкостью, которая влияет на параметры входов ИС. Эта паразитная емкость нелинейна и зависит от уровня входного напряжения. Для некоторых высокоточных схем необходимо исключить такую зависимость.

РАЗРАБОТКА ИСПЫТАТЕЛЬНОГО ОБОРУДОВАНИЯ ДЛЯ ОЦЕНКИ СТОЙКОСТИ К ИМПУЛЬСНЫМ СИГНАЛАМ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Н.С. ОБРАЗЦОВ, В.В. МЕЛЬНИЧУК, А.И. ПИНАЕВ

Типовая схема имитатора помехового воздействия данного вида содержит накопительный конденсатор и быстродействующий бездребезговый переключатель. Заряд конденсатора осуществляется через токоограничивающий резистор от источника высоковольтного напряжения. При достижении установленного напряжения конденсатор переключается на разряд, формируя разрядный импульс.

Применение в качестве функциональной замены элементов коммутации полупроводниковых приборов является наиболее эффективным. Такими приборами могут выступать лавинные транзисторы, диоды, а также тиристоры. Формирователи импульсов на лавинных транзисторах с ограниченной областью объемного заряда имеют малое время задержки (доли-единицы нс) при запуске, высокую частоту повторения (до десятков кГц) и малую длительность (доли-единицы нс) фронта импульса. Однако для них характерна сравнительно малая амплитуда импульсов (до десятков В на один прибор) и малая (до сотен Вт) пиковая мощность. Значительно большую амплитуду и пиковую мощность обеспечивают формирователи на тиристорах.

Существует несколько способов функционального применения тиристоров в качестве коммутирующего элемента. Один из способов основан на последовательном включении тиристоров вместо ключа S. В этом случае речь идет только о тиристорах, как об электронных ключах. Управление отпиранием тиристоров осуществляется путем подачи отпирающего напряжения на все приборы одновременно. Следует отметить, что данный способ запуска требует жесткого подхода к отбору тиристоров по близости их параметров, в частности минимального напряжения отпирания и времени задержки включения. В некоторых случаях требуются выравнивающие цепи, оптимальный подбор которых возможен только опытным путем. Таким образом, получение требуемых временных параметров коммутации представляет собой достаточно сложную задачу.

ОБ ОПТИЧЕСКОМ МЕТОДЕ ИССЛЕДОВАНИЯ ШЕРОХОВАТЫХ ПОВЕРХНОСТЕЙ И ЕГО ПРИЛОЖЕНИИ К ОПРЕДЕЛЕНИЮ ГЕНЕТИЧЕСКОЙ ИНФОРМАЦИИ ПО ПОВЕРХНОСТИ БИОЛОГИЧЕСКОГО МАТЕРИАЛА

А.Б. ГАВРИЛОВИЧ, Н.Я. РАДЫНО

В конце 80-х годов XX века появился и был узаконен в судебной практике метод исследования и идентификации объектов биологического происхождения. Речь идет о методе генной дактилоскопии. Он позволяет однозначно идентифицировать лиц, подозреваемых в половых преступлениях, проводить опознание в особо сложных случаях (расчлененные, обгоревшие, деформированные трупы), а также устанавливать степень родства. При использовании данного метода в решении задач криминалистических экспертиз не имеет значения природа биологического материала (кожа, кровь, сперма, волосы, слюна и др.). Он обладает высокой чувствительностью, и исследования можно проводить на небольшом количестве материала. Единственным необходимым условием является возможность выделения пригодной для анализа ДНК.

Выделение ДНК и ее исследование представляет собой трудную, занимающую достаточно много времени и дорогостоящую процедуру. Суть предлагаемого авторами оптического метода заключается в следующем: на поверхность исследуемого биологического материала падает свет с заданной поляризацией, при взаимодействии света с веществом изменяются поляризационные характеристики света, которые несут в себе как характеристики шероховатой поверхности, так и информацию о молекулярной структуре самого вещества. Вопрос о том, как влияет на характеристики

отраженного света структура ДНК биологического материала, требует точной аппаратуры, фиксирующей поляризационное изображение и экспериментальных данных с биологическим материалом, а главное, развитого математического аппарата для интерпретации экспериментальных данных, связанных с поляризацией света.

Авторами разработана теория процессов, происходящих при отражении света от шероховатой поверхности, накоплен уникальный опыт работы с поляризацией света и подготовлена теоретическая база для создания приборов, определяющих поляризацию отраженного света.

ВЫБОР ИМИТАЦИОННЫХ ВОЗДЕЙСТВИЙ В ЗАДАЧАХ ПРОГНОЗИРОВАНИЯ ПОСТЕПЕННЫХ ОТКАЗОВ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

А.И. БЕРЕСНЕВИЧ, С.М. БОРОВИКОВ

На долю постепенных отказов приходиться примерно 80% всех отказов полупроводниковых приборов. Прогнозирование этих отказов является актуальной задачей. Для решения задачи может быть использован метод имитационных воздействий.

Чтобы использовать какое-то воздействие (температуру, ток коллектора и т.п.) в качестве имитационного фактора при решении задач прогнозирования параметров методом имитационных воздействий, необходимо доказать, что между изменениями, вызываемыми действием имитационного фактора и изменениями, обусловленными длительной наработкой (дрейфом функциональных параметров), существует статистическая аналогия. Ответ на вопрос о наличии статистической аналогии между этими изменениями дает корреляционный анализ.

Информация об изменениях параметров была получена с помощью экспериментального исследования. В качестве функционального параметра рассматривался обратный ток коллекторного перехода (параметр $I_{КЭО}$) транзисторов КТ872А, а в роли гипотетического имитационного воздействия — обратное напряжение, прикладываемое к коллекторному переходу.

Оценка коэффициента корреляции, полученная с использованием экспериментальных данных, составила примерно 0,81. Наличие тесной корреляции между изменениями параметра $I_{КЭО}$, обусловленными сменой значений обратного напряжения на коллекторе, и изменениями, вызванными длительной наработкой транзисторов, позволяет сделать вывод о возможности использования обратного напряжения, прикладываемого к коллектору транзистора, в качестве имитационного фактора

ИСПОЛЬЗОВАНИЕ ПАРАМЕТРОВ ЭЛЕКТРИЧЕСКОГО РЕЖИМА БИПОЛЯРНЫХ ТРАНЗИСТОРОВ В КАЧЕСТВЕ ИМИТАЦИОННЫХ ФАКТОРОВ

А.И. БЕРЕСНЕВИЧ, С.М. БОРОВИКОВ

Методом имитационных воздействий можно решать задачи индивидуального прогнозирования постепенных отказов биполярных транзисторов.

В качестве имитационного фактора обычно используют температуру. Экспериментально, на примере транзисторов типа КТ872А установлено, что диапазону наработок 1000…20000 ч соответствует небольшой перепад имитационной температуры (примерно 16…17 К). При погрешности поддержания температуры, составляющей ±2К, ошибка прогнозирования функционального параметра транзистора может составить значение, неприемлемое для практики.

Имитационным фактором может быть и ток коллектора. В этом случае заметно сокращается длительность процедуры прогнозирования и уменьшается ошибка прогнозирования параметров, чем при использовании температуры. В некоторых случаях имитационное значение тока, соответствующее заданной наработке, может превышать предельно допустимое значение, указываемое в технической документации на транзисторы, что создает риск повреждения приборов.

Поэтому актуальным является поиск других имитационных факторов, которые можно было бы использовать для прогнозирования в тех случаях, когда температура и ток коллектора малопригодны.

В качестве имитационного фактора предлагается использовать напряжения, прикладываемые к p-n-переходам транзистора. Физическим обоснованием возможности использования напряжения является то, что между изменениями функциональных параметров, вызываемыми длительной наработкой биполярных транзисторов и изменениями, обусловленными сменой значений обратных напряжений, прикладываемых к p-n переходам, существует аналогия. Поэтому представляется возможность прогнозировать значения функционального параметра путем его контроля при определенных напряжениях, прикладываемых к p-n-переходам.

ЭФФЕКТИВНОСТЬ ПРОГНОЗИРОВАНИЯ НАДЁЖНОСТИ ЭЛЕМЕНТОВ МЕТОДОМ ПОРОГОВОЙ ЛОГИКИ

С.М. БОРОВИКОВ, Л.Г. НИКИФОРЕНКО

Практическая пригодность любого метода прогнозирования надёжности с использованием информативных параметров, в том числе и метода пороговой логики, определяется не только математическим аппаратом обработки результатов обучающего эксперимента, простотой и оперативностью принятия решения о классе элемента по прогнозирующему правилу (алгоритму прогнозирования), но также вероятностями ошибочных решений, их соответствием допустимым ошибкам.

Основу любого метода прогнозирования надёжности по информативным параметрам составляет алгоритм получения значения решающей функции, соответствующей элементу, уровнем надёжности которого интересуются. Возникает вопрос, какому методу прогнозирования, следовательно, и алгоритму формирования решающей функции отдать предпочтение.

Ставилась задача, используя результаты обучающего эксперимента, исследовать предложенные авторами в методе пороговой логики алгоритмы формирования решающей функции, основанные на положениях теории информации, и дать ответ на вопрос об эффективности этих алгоритмов. Кроме того, необходимо было сравнить предложенные алгоритмы метода пороговой логики с алгоритмами других методов.

Для решения поставленной задачи было предложено использовать вычислительный эксперимент, выполняемый на ЭВМ. Суть его состояла в моделировании для элементов обучающего эксперимента и применении для обработки его результатов различных алгоритмов формирования решающей функции. Это позволило для каждого алгоритма построить прогнозирующее правило и сделать оценку ошибочных решений, к которым оно может привести. Анализ ошибок прогнозирования дал ответ на вопрос об эффективности исследуемых алгоритмов метода пороговой логики и позволил сравнить их с алгоритмами некоторых известных методов прогнозирования.

ЭФФЕКТИВНОСТЬ ПРОГНОЗИРОВАНИЯ ПОСТЕПЕННЫХ ОТКАЗОВ БИПОЛЯРНЫХ ТРАНЗИСТОРОВ МЕТОДОМ ИМИТАЦИОННЫХ ВОЗДЕЙСТВИЙ

С.М. БОРОВИКОВ, Н.Е. МАНДИК

Для индивидуального прогнозирования постепенных отказов биполярных транзисторов можно использовать метод имитационных воздействий. В него основу положен принцип статистической аналогии между изменениями параметра, обусловленными длительным функционированием транзисторов, и изменениями этого же параметра, вызываемыми действием в начальный момент времени имитационного фактора, не приводящего к уменьшению рабочего ресурса прибора.

Эффективность метода определяется удачностью выбора имитационного воздействия (фактора), о чём можно судить по имитационной модели, построенной с использованием результатов обучающего эксперимента.

В работе исследована эффективность прогнозирования методом имитационных воздействий значений параметров мощных биполярных транзисторов для будущих длительных наработок. В качестве имитационного фактора использовалась температура. Предложено об эффективности судить по значению средней ошибке прогнозирования параметра. Получено выражение для определения этой ошибки и показано, как при прогнозировании постепенных отказов методом имитационных воздействий определять её и принимать решение о пригодности полученной имитационной модели – функции пересчёта заданной наработки на значение имитационного фактора.

ИСПОЛЬЗОВАНИЕ НАНОКРИСТАЛЛИЧЕСКОГО КРЕМНИЯ ДЛЯ СОЗДАНИЯ ЛЮМИНЕСЦЕНТНЫХ НАДПИСЕЙ.

Д.Н. УНУЧЕК, С.К. ЛАЗАРУК, П.С. КАЦУБА, А.А. РУМЯНЦЕВ, А.А. ЛЕШОК, В.А. ЛАБУНОВ

Широкое распространение для контроля подлинности ценных бумаг получили скрытые люминесцентные надписи, сочетающие в себе такие качества как простота верификации и надежность. Степень защиты изделия повышается при формировании скрытых изображений, содержащие различные цветные фрагменты. Мы предлагаем использовать известные люминесцентные свойства пористого кремния для создания скрытых надписей на его основе.

Нами были сформированы образцы пористого нанокристаллического кремния с пиком фотолюминесценции в красной, оранжевой, желтой и зеленой областях видимого диапазона. Образцы были сформированы электрохимическим анодированием на кремниевых подложках (001) сопротивлением 10–12 Ом/см, легированных бором. Анодирование проводили в водно-спиртовом растворе плавиковой кислоты в гальваностатическом режиме. После анодирования образцы выдерживали в электролите с целью получения коротковолнового смещения пика фотолюминесценции. При формировании образцов с пиком люминесценции в различных областях видимого диапазона использовали следующие режимы: красная — j_f=50 мА/см^2, t_f=10 мин; оранжевая — j_f=20 мА/см^2, t_f=20 мин; желтая — j_f=20 мА/см^2, t_f=20 мин, t_a=10 мин; зеленая — j_f=20 мА/см^2, t_f=20 мин, t_a=30 мин, где j_f — плотность тока формовки, t_f — время анодирования, t_a — время выдержки в электролите после анодной обработки.

Показано, что люминесцирующий нанокристаллический кремний при смешивании его с различными красителями сохраняет свои люминесцентные свойства. Это позволяет формировать скрытые надписи, люминесцирующие на заданных длинах волн при УФ подсветке.

Таким образом, предложен способ создания фотолюминесцентного материала на основе пористого наноструктурированного кремния для создания скрытых люминесцентных надписей.

ИСПОЛЬЗОВАНИЕ ИНЖЕКЦИОННО-ПОЛЕВЫХ ТРАНЗИСТОРНЫХ СТРУКТУР ДЛЯ АКТИВНОГО ПОДАВЛЕНИЯ ДАННЫХ В СЕТЯХ ЭЛЕКТРОПИТАНИЯ

В.П. ЛУГОВСКИЙ, И.М. РУСАК

Одним из основных средств получения несанкционированного доступа к конфиденциальной информации через силовые цепи является извлечение ее из помех, производимых устройством. В частности, при анализе помех, создаваемых ПЭВМ следует учитывать помехи проводимости — т.е. помехи, распространяющиеся в проводах первичной сети и выходных цепях блока электропитания; Помехи проводимости распространяются по проводам питания по всему устройству ПК и через сетевой шнур питания попадают в первичную сеть электропитания. Основным генератором помех проводимости являются блок питания устройства, в частности, импульсный преобразователь напряжения. Менее мощным генератором помех проводимости являются сами модули ПЭВМ из-за наличия в этих модулях различных импульсных потребителей (микропроцессор интерфейсные микросхемы). Проблема защиты информации, которая циркулирует по сети электропитания может быть решена дополнением в схемы источников питания помехоподавляющих фильтров. Помехоподавляющие фильтры могут быть выполнены как пассивными, так и активными. Пассивные фильтры просты в реализации, но не обеспечивают полной фильтрации данных. Активные фильтры реализуются по компенсационной схеме и обеспечивают избирательное подавление информации, которая может проникать в сети электропитания. Учитывая низкое сопротивление сети электропитания, наиболее рационально использовать в качестве оконечных устройств фильтрации формирователи токовых посылок. Предлагается использовать в качестве таких формирователей схемы

токовых элементов на инжекционно-полевых транзисторных структурах (ИПС). Поскольку ИПС обладают большими пробивными напряжениями, то появляется возможность непосредственного подключения таких выходных каскадов к сетевым проводам. Высокое значение коэффициента передачи тока ИПС дает возможность обеспечить достаточную степень подавления синфазной и дифференциальной составляющей токов цифровых данных, циркулирующих в сети электропитания.

САМОРАЗРУШАЮЩИЕСЯ КРЕМНИЕВЫЕ ЧИПЫ ПРИ ПОПЫТКЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К НИМ.

А.В. ДОЛБИК, С.К. ЛАЗАРУК, П.С. КАЦУБА, А.А. РУМЯНЦЕВ, В.А. ЛАБУНОВ

Пористый кремний, полученный электрохимическим анодированием монокристаллического кремния, обладает уникальными физическими и химическими свойствами, которые определяются его нанокристаллической структурой. Выбирая режимы анодной обработки возможно управлять этими свойствами, создавая в монокристаллической подложке разветвленную систему пор с размерами от единиц нанометров до нескольких микрон и формируя таким образом в пористом слое наноструктурированный материал с определенными свойствами. К таким явлениям относится недавно обнаруженное быстрое окисление слоев пористого кремния, проявляющееся как горение и взрыв этого материала.

Так к возможному практическому использованию процесса взрыва пористого кремния следует отнести изготовление самоуничтожающихся кремниевых чипов. Взрыв либо горение пористого кремния инициируется механическим, электрическим, оптическим либо химическим способом. В частности, электрический импульс с амплитудой тока более 1 А инициирует взрывной процесс с временной задержкой микросекундного диапазона. В наших экспериментах при толщинах пористого кремния более 100 мкм взрыв приводил к полному разрушению кремниевой подложки. В результате взрыва кремниевый чип разделялся на множество осколков, что делало полностью невозможным его дальнейшее использование. При этом сама вспышка не оказывала какого-либо ощутимого воздействия на человека. Следует отметить локальность действия взрывной реакции, ограниченной объемом пористого слоя. Никаких разрушений у объектов, находящихся в непосредственной близости возле взрываемых чипов, обнаружено не было.

Таким образом, взрывная реакция при быстром окислении пористого кремния может быть использована для защиты информации, хранящейся на кремниевом кристалле. Управляемый микровзрыв пористого кремния позволяет разработать микросистемы, обладающие принципиально новыми возможностями в плане защиты информации

ИЗМЕНЕНИЕ ОПТИЧЕСКИХ СВОЙСТВ БУМАГИ ПРИ ВОЗДЕЙСТВИИ ВЫСОКОЧАСТОТНОГО МАГНИТНОГО ПОЛЯ

В.В. АЖАРОНОК, С.В. БОРДУСОВ, И.В. ВОЩУЛА, И.И. ФИЛАТОВА

Традиционные методы защиты ценных бумаг и документов от подделки основаны на использовании вводимых в бумагу-основу защитных

меток (нити, волокна, конфетти и т.д.), служащих для создания специфической морфологии поверхности бумаги или же в качестве индикаторов при воздействии на бумагу химических реагентов и УФ излучения. В последние годы с целью разработки нетрадиционных методов защиты в исследовательских центрах многих стран ведутся работы по созданию плазменно-пучковых и микроволновых способов воздействия на бумагу, направленных на изменение ее надмолекулярной структуры в микронном и субмикронном приповерхностном слое.

В настоящей работе исследовано изменение оптических свойств бумаги в результате ее модификации в мощном магнитном поле, возбуждаемом в мегагерцовом диапазоне частот с использованием генератора высокочастотного синусоидального тока.

Установлено, что воздействие на бумагу высокочастотного магнитного поля приводит к изменению индикатрис коэффициентов отражения и пропускания зондирующего поляризованного излучения He-Ne лазера, связанному с возникновением ориентационных эффектов в протяженных макромолекулах целлюлозы вследствие большой анизотропии их диамагнитной восприимчивости.

МОДЕЛЬ МДП-ТРАНЗИСТОРА С СУБМИКРОННЫМИ РАЗМЕРАМИ

В.Е. ГАЛУЗО

Предлагается простая аналитическая квазидвумерная физико-топологическая модель передаточной и выходной вольт-амперных характеристик (ВАХ) в режиме сильной инверсии МДП-транзистора с субмикронными размерами длины канала, а точнее, с расстоянием между стоком и истоком меньше суммарной толщины обедненных областей их p-n переходов. В модели учитывается уменьшение подвижности и насыщение скорости носителей заряда в сильных продольных и поперечных электрических полях.

Моделирование порогового напряжения осуществляется с учетом влияния на заряд в обедненной области под затвором размеров обедненных областей p–n–переходов стока и истока, т.е. тем самым описывается влияние потенциала на стоке и расстояние между стоком и истоком на величину порогового напряжения. Расчет размеров обедненных областей стока и истока выполняется с учетом влияния заряда подвижных носителей.

При моделировании тока стока предлагается учитывать сложный характер распределения плотности подвижных носителей заряда по длине канала, обусловленный неравномерностью заряда обедненной области под затвором по длине канала.

Результаты моделирования ВАХ хорошо согласуются с экспериментом. Благодаря своей простоте и достоверности модель может быть использована в программах схемотехнического анализа.

СЕКЦИЯ 5. ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ

ИНТЕГРИРОВАННЫЕ СИСТЕМЫ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ БАНКОВСКИХ УЧРЕЖДЕНИЙ

В.В. МАЛИКОВ

Интегрированные системы технических средств охраны (ИС ТСО) — совокупность двух или более взаимоувязанных автоматизированных систем безопасности, в которой функционирование одной из них зависит от результатов функционирования другой (других) так, что эту совокупность можно рассматривать как единую автоматизированную систему безопасности.

Автоматизированная система безопасности – это автоматизированная система, состоящая из персонала и комплекса средств автоматизации, деятельность которых реализует информационную технологию выполнения установленных функций. ИС ТСО состоит из комплекса средств автоматизации, обеспечивающего совместное функционирование входящих в состав ИС подсистем, и подсистем технических средств охраны и жизнеобеспечения зданий объекта.

Комплекс средств автоматизации включает в себя системообразующее ядро и программно-аппаратные средства, обеспечивающие его сопряжение с прикладными подсистемами. Несколько ИС ТСО могут быть объединены в локальную сеть (например VPN) с общим центром — пультом управления. Безопасность передачи сигнала по каналам связи (в т.ч. оптоволоконным) гарантируется применением дополнительных алгоритмов кодирования информации (DES, 3DES, AES), аутентификации пользователей (EAP, PAP) и целостности данных.

Системообразующее ядро обеспечивает интеграцию системы, контроль функционирования подсистем, централизованное хранение базы данных, ведение системных журналов. Доступ к системным ресурсам разграничивается программно, как правило, доступ с правами управления ИС ТСО из "вне" — невозможен, внешние порты ПЭВМ АРМ ДО/ДИ — аппаратно защищены.

Объектами автоматизации являются технические средства охраны в учреждениях банков, к которым относятся подсистемы:

– охранной сигнализации (ОС) — многоуровневая защита извещателями с разными принципами обработки сигнала: ИК, радиоволновой, сейсмический/вибрационный, акустический и др.;

– пожарной сигнализации (ПС) — адресные системы ПС, УПА, пожаротушения;

– видеонаблюдения — отображение/запись с передачей информации о состоянии объекта при срабатывании ОС;

– регистрации полномочий и разграничения доступа персонала в помещения (АСУД на основе магнитных карт и др.);

– контроля и управления технологическими процессами жизнеобеспечения зданий и сооружений.

Цели создания ИС ТСО:

1. Повысить эффективность эксплуатации объекта (общее АРМ ДО/ДИ обеспечивает полный контроль состояния объекта, ТО системы осуществляет одна организация).

2. Сократить время возможных простоев:

– за счет сокращения времени локализации неисправности (тревожной и аварийной ситуации).

– за счет сокращения времени реагирования по локализованной ситуации.

– за счет внедрения оптимальных методов эксплуатации.

3. Оптимизация структуры и занятости обслуживающего персонала.

4. Возможность экстренного и оптимального перераспределения ресурсов (электроэнергия, тепло, вода, резервное оборудование) в экстренной ситуации.

По способу построения ИС ТСО подразделяются:

1. Объединяющие отдельные функционально законченные системы на уровне программируемых релейных контактов.

2. Построенных на базе программно и аппаратно совмещенных систем закрытого типа.

3. Построенных на базе интеграции отдельных функционально законченных самостоятельных систем посредством специализированного ПО (открытые системы).

Этапы создания комплекса:

1. Описание модели объекта управления.

2. Описание поведения системы управления (метод решающих правил, экспертная система).

3. Описание интерфейсов пользователя.

4. Описание прав доступа пользователей.

5. Моделирование, тестирование.

6. Создание драйверов-обработчиков.

7. Внедрение.

ПРОБЛЕМЫ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

А.С. ПОЛЯКОВ, В.Е.САМСОНОВ

Применение электронных документов и электронной цифровой подписи в них регламентируются Законами и стандартами Республики Беларусь. Однако, многие вопросы применения электронных документов (ЭД) и электронной цифровой подписи (ЭЦП) остались нерешёнными и фактически сдерживают практическое использование ЭД.

В докладе анализируются некоторые положения нормативных документов, в которых, по мнению авторов, имеются изъяны, препятствующие практическому применению электронных документов и электронных цифровых подписей.

На основании проведенного анализа делаются следующие выводы:

1. Обмен электронными документами, созданными в соответствии с Закон Республики Беларусь "Об электронном документе", но в разных информационных и вычислительных сетях, будет невозможен в связи с

различными содержанием и структурой карточки открытого ключа проверки подписи, а также содержанием и структурой особенной части электронного документа.

2. Применение электронных документов, использующих ЭЦП, возможно только внутри отдельно взятой корпоративной информационной сети, которая установит собственные правила изготовления личных ключей подписи, открытых ключей проверки подписи, передачи и использования открытых ключей проверки подписи, и все остальные вопросы, связанные с применением электронной цифровой подписи. Но даже в этом случае электронные документы фактически будут выступать только как заменители бумажных носителей, не имеющих юридической силы.

3. Для полноценного применения электронных документов, использующих электронную цифровую подпись, требуется внесение соответствующих изменений и дополнений в Закон "Об электронном документе", в частности, необходимо ввести в Закон понятия "сертификат открытого ключа" и "удостоверяющий центр", являющиеся общепризнанными в мировой практике использования электронных документов, подписанных ЭЦП. В Законе же присутствует только понятие "карточка открытого ключа проверки подписи", создаваемая в виде бумажного документа, подписываемая владельцем личного ключа и распространяемая им лично либо уполномоченным им лицом среди заинтересованных лиц.

ФОРМАТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ КАК ЭЛЕМЕНТ ЗАЩИТЫ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Е.А. ЦЫНКЕВИЧ

В докладе рассматриваются критерии оценки форматов электронных документов (ЭД), а также процедур формирования ЭД и проверки соответствия ЭД определенным в системе форматам.

При определении правомочности поступившего в систему электронного документа одной из основных является проверка соответствия документа определенным в системе форматам. Важность данной проверки состоит в том, что соответствие электронного документа определенному формату обеспечивает наличие в документе реквизитов, значения которых назначают ему установленную в секторе действенности роль, в соответствии с которой этот электронный документ имеет право “требовать” от системы совершения определенных действий. Исполнение таких действий на основе ошибочных либо специально сформированных злоумышленниками электронных документов может нанести пользователям этих систем ощутимый ущерб.

При решении данной задачи используется проверка выполнения требований, предъявляемых к процессу формирования электронных документов, в ходе которой необходимо:

определить множество реквизитов, входящих в состав электронных документов, значения которых будут использоваться при подтверждении правомочности ЭД;

установить ограничения на процесс формирования их значений;

определить местонахождение данных реквизитов в составе ЭД и установить признаки, обеспечивающие их распознавание, т. е. описать формат создаваемого документа.

Таким образом, защита автоматизированных систем электронного документооборота должна содержать схемы синтаксического и семантического контроля поступающих электронных документов, включая сопоставительный анализ значений реквизитов ЭД с установленными для них ограничениями, а также определять четкие правила обработки документов установленных форматов, для каждого из форматов.

САПР ДЛЯ ПРОЕКТИРОВАНИЯ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ В ПРОЦЕССЕ ЕЁ ПРОЕКТИРОВАНИЯ И ЭКСПЛУАТАЦИИ

С.В. ПОЛАЖЕНКО

Современные автоматизированные системы (АС) сложны и многообразны: в них используется множество программно-аппаратных комплексов различных производителей, которые реализуют те или иные модели правил разграничения доступа (ПРД); на каждом вычислительном узле (ВУ) определено несколько учётных записей (УЗ), обладающих различными полномочиями; каждый пользователь обладает несколькими УЗ на нескольких ВУ и т.д. При этом сама АС постоянно модифицируется: меняются пользователи и их УЗ, меняется категория обрабатываемой информации, меняется множество объектов на конкретном ВУ и т.д. Число ПРД, которые должны учесть все возможные комбинации объектов, субъектов, типов доступов и т.д., растёт в комбинаторном порядке.

В результате администратор ИБ в АС не имеет возможности представить полную картину реализации ПРД в АС и не может быть уверен в том, что текущие ПРД корректны для данной АС. Для самостоятельной разработки ПРД администратору ИБ необходим испытательный стенд, повторяющий конфигурацию самой АС, где он может экспериментальным путём настроить новые ПРД и проверить их корректность.

В работе предлагается разработать СППР для проектирования ПРД в АС в процессе проектирования самой АС и в процессе её эксплуатации. Предлагаемая СППР должна обеспечить возможность: построения описания ПРД в АС, модификация уже имеющегося описания ПРД, автоматизированный поиск уязвим остей, вызванных неправильным определением ПРД в АС.

СЕКЦИЯ 6. ПРОБЛЕМЫ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КАДРОВ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ "ВЛИЯНИЕ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ НА ОРГАНИЗМ ЧЕЛОВЕКА"

К.Д. ЯШИН, В.В. КУЗНЕЦОВ, Л.Е. ПАРИМСКАЯ

Целью работы явилась разработка виртуального лабораторного практикума "Экранирование электромагнитных полей". Последнее время в связи с высоким ростом информационных технологий происходит глобальное внедрение компьютерной техники. Спектр охватываемых прогрессом областей очень широк. Одной из них является образование. В сфере обучения разработаны и применяются различные электронные учебники, справочные пособия, системы контроля знаний и виртуальные лабораторные работы. Преимущества виртуальной работы очевидны. Это отсутствие изнашивающегося и нуждающегося в переналадке оборудования, безопасность выполнения лабораторной работы. Следует также выделить информативность. В реальной лабораторной работе сами электромагнитные поля увидеть нельзя, а применение компьютерных технологий позволяет их визуализировать. Выбор Macromedia Flash в качестве средства разработки позволяет предоставить обучаемому более дружеский интерфейс и привлечь его внимание к работе.

Актуальность лабораторного практикума вызвана тем, что с электромагнитными полями студенты сталкиваются ежедневно. Радиочастотный диапазон электромагнитных излучений 300 МГц–300 ГГц (1 м–1 мм) относится к СВЧ-диапазону. Основными источниками СВЧ-излучений на производстве являются: антенны радиопередающих устройств, отверстия и щели в фидерных линиях и фланцевых соединениях волноводов, неплотности и отверстия в экранирующих устройствах генераторов, открытые выходы генераторов и др. Для человека такое излучение опасно своими негативными последствиями: увеличение общего теплообразования в организме человека, нагрев тела и отдельных органов. Особенно подвержены облучению ткани и органы, у которых терморегуляция выражена слабо (глаза, мозг). Также облучение влияет и на нервную систему, результатом являются головные боли, повышенная утомляемость, нарушение сна, повышение раздражительности, ослабление памяти и др. Более длительное воздействие электромагнитного излучения может вызвать рост онкологических заболеваний, утрату репродуктивной функции, иммунитета. Более чувствительны к облучению больные люди, дети и лица пожилого возраста. Для снижения интенсивности поля в рабочей зоне применяются: экранирование излучателей, помещений или рабочих мест; уменьшение плотности потока энергии в рабочей зоне за счёт уменьшения мощности источника и использования ослабителей (аттенюаторов) мощности; применение средств индивидуальной защиты. При экранировании используются такие явления, как поглощение электромагнитной энергии материалом экрана и её отражение от поверхности экрана. Поглощение электромагнитного излучения обуславливается тепловыми потерями в материале за счёт индукционных токов и зависит от электромагнитных свойств экрана (электрической проводимости, магнитной про-

ницаемости и т.д.). Отражение обуславливается несоответствием электромагнитных свойств среды, в которой распространяется электромагнитная энергия, и материала экрана (прежде всего, волновых сопротивлений). Для изготовления экранов применяются любые тонкие металлические листы (сталь, алюминий, медь или их сплавы) либо металлические сетки, т.к. обладая хорошей электромагнитной проводимостью и низким волновым сопротивлением, они обеспечивают хорошее экранирование, как за счёт поглощения, так и за счёт отражения. Толщина экрана должна быть больше глубины проникновения электромагнитной волны в толщу экрана и не менее 0,5 мм.

АНАЛИЗ КВАНТОВЫХ ОПТИЧЕСКИХ КАНАЛОВ СВЯЗИ

И.Р. ГУЛАКОВ, А.О. ЗЕНЕВИЧ

В телекоммуникационных системах нового поколения широко используются сигналы оптического диапазона, транслируемые по волоконно-оптическим линиям связи (ВОЛС). Это связано с тем, что по оптическим каналам связи можно передавать достаточно большой объем информации, и иногда необходимо обеспечить конфиденциальность сообщаемой информации. Однако в местах соединений и подключения кабельных сегментов, оптических усилителей и регенераторов ВОЛС наиболее вероятное подсоединение несанкционированного пользователя (нарушителя). Поэтому возникает необходимость в надежных способах защиты информации.

Одним из способов защиты информации, предаваемой по ВОЛС от несанкционированного пользователя, является уменьшения мощности передаваемого сигнала уровня единичных фотонов [1]. В этом случае каждый бит двоичной информации кодируется различными состояниями фотона. Для кодировки информации используются различные поляризации фотонов либо производится модуляция их фазы [1]. Наиболее дешевое и простое в реализации является кодирование информации при помощи различных поляризаций фотонов, поскольку она не требует использование такой дорогостоящей аппаратуры как интерферометры Маха-Цендера, которые необходимы для модуляции фазы фотона.

В настоящее время это один из наиболее надежных способов защиты информации, поскольку он базируется на законах квантовой механики. Нарушитель не может отвести часть сигнала с передающей линии, так как нельзя поделить квант оптического излучения на части. Любая попытка вмешаться в процесс передачи приведет к резкому увеличению уровня числа ошибок регистрации, что не может остаться не замеченным. Степень надежности в данной методике выше, чем в случае применения алгоритмов с парными ключами (например, RSA). В нашем случае ключ может генерироваться во время передачи по совершенно открытому оптическому каналу. По существу квантовая криптография может заменить алгоритм Диффи-Хелмана, который в настоящее время часто используется для пересылки секретных ключей шифрования по каналам связи.

При передаче данных отдельными фотонами возникают сложно решаемые задачи, связанные с обеспечением достаточно большой скорости и дальности передачи данных. Скорость передачи данных отдельны-

ми фотонами в основном ограничена быстродействием фотоприемника, и как показали наши исследования для самого быстродействующего режима работы фотоприемника она составляет около 1 Мбит/с[2]. Максимальное расстояние, на которое можно передать информацию, будет определяться свойствами волоконно-оптического кабеля и чувствительностью фотоприемника. При распространении оптического излучения в волокне фотон может быть поглощен волокном или обратно рассеян на оптических неоднородностях волокна. Наименьшее затухание оптического излучения наблюдается для одномодовых волокон 0,22–0,25 дБ/км для длины волн 1550 нм, для многомодовых волокон 0,50–0,60 дБ/км для длины волны 1300 нм [3]. При 100 % квантовой эффективности регистрации фотоприемника вероятность обнаружения одного фотона при длине одномодового кабеля 15 км составит около 0,5. Для многомодового волокна та же вероятность соответствует 6–7 км. Поскольку ни один фотоприемник, использующийся в режиме одноквантовой регистрации, не обладает 100% квантовой эффективностью регистрации, то приведенные данные для 0,5 вероятности регистрации необходимо скорректировать. Наибольшая квантовая эффективность регистрации фотоприемника в режиме одноквантовой регистрации составляет 75 % [4] при охлаждении фотоприемника до температуры жидкого азота и ниже. Использование фотоприемников охлаждаемых до столь низких температур в ВОЛС затруднено и приводит к значительному удорожанию системы. Для фотоприемников, работающих при температурах близким к комнатной, квантовая эффективность для различных типов может изменяться от 1 до 5 %. Использование таких фотоприемников приведет к значительному снижению протяженности линии связи.

На основании проделанного анализа можно сделать вывод, что на настоящий момент возможна разработка и создание квантовых оптических каналов связи, по которым информация предается посредством отдельных фотонов. Максимальная скорость передачи данных при этом не будет превышать 1 Мбит/с, а протяженность линии не превысит нескольких километров.

Литература

1. Килин С.Я. / Успехи физических наук, 1999, Т. 169. № 5. С. 507–526.
2. Гулаков И.Р., Зеневич А.О., Козлов В.Л. // Доклады БГУИР. 2004. № 5. С. 31–32.
3. Убайдуллаев Р.Р. Волоконно-оптические сети. М., 1998.
4. Гулаков И.Р., Холондырёв С.В. Метод счета фотонов в оптико-физических измерениях. Мн., 1989.

ПОДГОТОВКА СТУДЕНТОВ В ВЫСШЕМ ГОСУДАРСТВЕННОМ КОЛЛЕДЖЕ СВЯЗИ ПО ВОПРОСАМ БЕЗОПАСНОСТИ

Л.М. НОВИКОВА

Подготовка студентов уровня высшего и среднего специального образования в Учреждении образования "Высший государственный колледж связи" включает преподавание дисциплин производственной, почтовой, радиационной безопасности, а также защиты населения и хозяйственных объектов в чрезвычайных ситуациях. Обязательность такого обучения вызвана реальностью современного мира, в котором к существующим издавна угрозам стихийных бедствий все больше добавляются опасности техногенного, антропогенного и социально - политического харак-

тера. Непременным атрибутом 21 века становится почтовый и электромагнитный терроризм, представляющий угрозу для систем управления и различных видов связи. Поэтому нормальное функционирование государства и безопасность населения во многом определяется превентивными мерами и подготовленностью соответствующих служб и граждан к действиям в чрезвычайных ситуациях.

В целях повышения качества получаемых знаний по вопросам профилактики почтового и электромагнитного терроризма, психологии и правил поведения в экстремальных ситуациях, безопасности на рабочих местах студентами ВГКС подготовлено более 10 докладов для участия в международной научно-практической конференции "Обеспечение безопасности жизнедеятельности: проблемы и перспективы", проводимой в Командно-инженерном институте МЧС Республики Беларусь в мае 2005 г.

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО РАДИОЭЛЕКТРОННОЙ ЗАЩИТЕ ИНФОРМАЦИИ

В.Н. ЛЕВКОВИЧ, С.Б. САЛОМАТИН, Р.Г. ХОДАСЕВИЧ

На кафедре радиотехнических систем БГУИР с 1 сентября 2005 г. начата подготовка инженеров по специальности "Радиоэлектронная защита информации".

Первые три года студенты изучают общеуниверситетские дисциплины социально-гуманитарного, общенаучного и общепрофессионального блоков. В блок специальных дисциплин включены курсы: "Методы и устройства формирования, приема и обработки радиосигналов", "Теория кодирования и защита информации", "Обработка информации в каналах с помехами", "Методы и средства радиоэлектронной защиты информации", Радиоэлектронные системы защиты информации", "Защита информации в социотехнических системах", "Проектирования цифровых систем на ПЛИС", "Системы компьютерного проектирования" и др.

В процессе обучения студенты изучают основные физические и технические принципы процесса получения информации путем приема и анализа электромагнитных излучений, методы комплексного использования различных методов и средств защиты на радиоэлектронном уровне (сигналов сложной формы, адаптивных методов их обработки в пространственно-временной и частотных областях, быстродействующей цифровой техники, современной технологии, организационных мер). Решают задачи системной радиоэлектронной защиты, радиоэлектронного противодействия и наблюдения, управления радиоэлектронными средствами защиты информации систем локации, навигации и передачи информации.

О МАТЕМАТИЧЕСКОМ ОБЕСПЕЧЕНИИ КУРСА ЗАЩИТЫ ИНФОРМАЦИИ

ЛИПНИЦКИЙ В.А., ЛИПНИЦКАЯ В.А.

В различных вузах Республики Беларусь читается сравнительно новый образовательный курс "Защита информации". Вопросы, обсуждаемые в данной учебной дисциплине относятся прежде всего к защите данных, информации, при их передаче по каналам связи от несанкциониро-

ванного доступа. Это одна из древнейших проблем цивилизации. В настоящее время курс защиты информации является высоко математизированной дисциплиной, использующей идеи, результаты и алгоритмы теории чисел, теории групп, теории колец и полей, теории полей Галуа и многое другое. Следовательно, качественное чтение курса защиты информации требует соответствующей математической подготовки слушателей. К сожалению, названные разделы современной математики отсутствуют в классическом курсе высшей математики во ВТУЗах.

Сейчас лишь начинается решение возникшей проблемы, причем в отдельных вузах. Так, в Белорусском государственном университете информатики и радиоэлектроники читается короткий семестровый специальный курс "Современная прикладная алгебра", посвященный изучению отмеченных разделов современной алгебры. К сожалению, читается он лишь для студентов дневной формы обучения специальностей "Информатика" и "Сети телекоммуникации".

Подобный семестровый курс читается и Белорусском национальном техническом университете для студентов специальности "Информационные технологии". Следует отметить, что похожий курс с упором на теорию групп уже более 10 лет читается на факультете прикладной математики БГУ, а с недавнего времени - на механико-математическом факультете БГУ для студентов специальности "Компьютерная матматика".

ОСОБЕННОСТИ ВНЕДРЕНИЯ РЕШЕНИЙ БУХАРЕСТСКОЙ ВСЕМИРНОЙ ПОЧТОВОЙ СТРАТЕГИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л.М. ЛЫНЬКОВ, В.В. СОЛОВЬЕВ, А.М. ПРУДНИК, С.В. ЖДАНОВИЧ

Бухарестский конгресс Всемирного почтового союза, проведенный осенью 2004 г. определил следующие цели развития отрасли:

1) универсальная почтовая служба;

2) качество службы и эффективность почтовой сети;

3) рынки и удовлетворение потребностей клиентов;

4) почтовая реформа устойчивое развитие;

5) сотрудничество и взаимодействие участвующих сторон и деятельности почтового сектора.

Кроме того, развиваются системы электронной почтовой марки для того, чтобы почта могла передавать сообщения, заверенные электронной цифровой подписью.

Для реализации перечисленных целей, предполагается осуществление следующих мероприятий:

– улучшение защиты почты и усиление борьбы с терроризмом и отмыванием денег с помощью почтовой сети;

– решение о модернизации и развитии почтовых финансовых услуг с использованием современных технологий;

– принятие предложения о придании юридической силы электронному почтовому штемпелю;

–определение мер по сохранению и защите окружающей среды.

СИСТЕМА АВТОМАТИЗАЦИИ КОНТРОЛЯ ЗНАНИЙ УЧАЩИХСЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В.А. БОГУШ, А.В. ДОДУ, М.З. ТИЛЛАЕВ

Широкое использование вычислительных систем обработки информации в организациях и на предприятиях, увеличение электронного документооборота, информатизация общества и постоянно увеличивающаяся стоимость информации обуславливает актуальность проблем защиты информации, создания в рамках службы безопасности специальных подразделений по технической защите. Подготовка специалистов по защите информации связана не только с получением специальных навыков и знаний, но также должна обеспечивать высокий уровень базовой подготовки в области телекоммуникаций и радиоэлектроники, что связано с динамикой развития современных средств доступа к информации и методов защиты информации.

Кафедра защиты информации Учреждения образования "Белорусский государственный университет информатики и радиоэлектроники" обеспечивает подготовку специалистов в области защиты информации в телекоммуникационных системах с использованием перспективных методов и средств обучения. Гибкость учебного процесса и его адаптация к современным требованиям обеспечивается за счет автоматизации учебного процесса. Для выполнения лабораторно-практических занятий работ активно привлекаются современные вычислительные системы и элементная база.

Разработан методический комплекс лабораторных работ для обучения (методическая часть) и проверки знаний студентов (тестовые задания и расчетная задача) по дисциплинам в области защиты информации.

Основные требования к комплексу включают наглядность, соответствие современному виду операционных систем, невысокие требования к аппаратной части, что позволяет использовать имеющийся парк машин, возможность использования манипулятора «мышь», легкость понимания и изучения.

При выборе среды разработки учитывалось несколько факторов. Основным из них была объектная ориентированность языка программирования, что на данный момент наиболее полно соответствует требованиям, предъявляемым к программным продуктам. Неоспоримым плюсом объектно-ориентированного программирования является понятность и наглядность программного кода, что, безусловно, ощутимо облегчает доработку программы, как ее автору, так и группе разработчиков, занимающейся модификацией приложения впоследствии.

В качестве языка программирования использовался Microsoft Visual C++ 6.0, обладающий следующими преимуществами: пониженный размер результирующего бинарного файла при равной функциональности приложений, написанных в других средах разработки; более низкие аппаратные требования и отсутствие необходимости установки дополнительного программного обеспечения, совместимость с широко используемой в учебном процессе операционными системами семейства MS Windows.

Приложение представлено двумя исполняемыми файлами, один из которых предназначен для преподавателей и предусматривает возмож-

ность редактирования базы данных, в которой хранятся вопросы и правильные ответы на них, а второй – предназначен для проверки знаний учащихся. Он включает в себя два раздела: теоретическая информация, необходимая для выполнения данной лабораторной работы, и вопросы и задача для контроля. Введенные данные считываются и передаются в класс-хранилище. Хранить их в своем классе не представляется возможным по той причине, что класс, который отвечает за представление и считывание информации, уничтожается при переходе к следующему вопросу. Время жизни класса-хранилища равно времени жизни программы. Введенные данные сравниваются с правильными ответами, хранящимися в базе данных. На основании сравнении этих данных выносится решение о правильности ответа на вопрос и результата решения задачи. Итог выполнения задания используется преподавателем при оценке знаний студентов.

ОРГАНИЗАЦИЯ ПОДГОТОВКИ ИНЖЕНЕРНЫХ КАДРОВ ПО НОВОЙ СПЕЦИАЛЬНОСТИ "ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ"

В.А. БОГУШ, В.Ф. ГОЛИКОВ, В.К. КОНОПЕЛЬКО, Л.М. ЛЫНЬКОВ

В настоящее время в области телекоммуникаций происходят значительные изменения, связанные с разработкой и совершенствованием технологий информационной безопасности (электронная цифровая подпись, инфраструктура идентификации, защита сетевых протоколов, антивирусная защита, фильтрация содержания и многое другое). Для информационно-коммуникационных сетей составной и неотъемлемой частью обеспечения их защищенности является сбалансированность интересов потребителей, операторов и органов государственного управления. Развиваются службы, основным видом деятельности которых на предприятиях, учреждениях и офисах является обеспечение безопасности, которая реализуется различными методами и средствами, в том числе с применением конкретной аппаратуры, компьютерных программ, технических, организационно-правовых и методологических средств. Особая актуальность подготовки специалистов данного профиля связана с совершенствованием систем электронной коммерции и развитием современных платежных систем.

В Учреждении образования "Белорусский государственный университет информатики и радиоэлектроники" введена новая специальность "Защита информации в телекоммуникациях". Содержание трудовой деятельности инженера по данной специальности включают исследование, разработку и сопровождение специальных и технических средств защиты и обработки информации в телекоммуникационных системах, моделирование технической защиты информации в телекоммуникационных системах, построение и анализ защищенных систем и сетей передачи информации, эксплуатацию специальных технических и аппаратно-программных средств защищенных телекоммуникационных систем, выполнение оперативных заданий, связанных с обеспечением контроля технических средств и механизмов системы защиты информации, проведению аттестации и сертификации объектов, помещений, технических

средств, программ и алгоритмов на предмет соответствия нормативным требованиям технической защиты информации.

Предполагается, что введение двойной квалификации: специалист по защите информации, инженер по телекоммуникациям, будет способствовать повышению интереса абитуриентов.

Учебный план специальности «Защита информации в телекоммуникациях» включает новые специальные дисциплины, посвященные правовому и нормативному обеспечению защиты информации, криптографической защите информации, защите речевой и видеоинформации, защищенным сетям радиодоступа и системам подвижной радиосвязи, компьютерным сетям, защите информации в банковских технологиях, методам и средствам защиты объектов связи от несанкционированного доступа, защите программного обеспечения и баз данных в сетях телекоммуникаций.

Созданная в прошлом году кафедра Защиты информации БГУИР обладает достаточной компьютерной и специальной аппаратурной базой, имеет в своем составе квалифицированных преподавателей (5 профессоров, докторов наук, 8 доцентов, канд. наук), что позволяет обеспечить высокий уровень подготовки инженеров по специальности.

На кафедре проводятся госбюджетные и хоздоговорные научные исследования и опытно-конструкторские работы по проблемам создания теоретических основ, методов и средств защиты информации в сетях телекоммуникаций, защиты речевых сообщений, электромагнитной информационной безопасности (данная деятельность лицензирована Государственным центром безопасности информации РБ). Осуществляется подготовка магистров, кандидатов и докторов наук.