ДОКЛАДЫ

БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

ЭЛЕКТРОНИКА
МАТЕРИАЛЫ
ТЕХНОЛОГИИ
ИНФОРМАТИКА

Российско-белорусская научно-техническая конференция

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Минск-Нарочь 19-23 мая 2003 года

Том 1 № 2/1
2003

ДОКЛАДЫ

БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Выходит четыре номера в год

Научный журнал основан в 2002 году

Адрес редакции:

220027, Минск, ул. П. Бровки, 6, к. 401

239-89-39

Компьютерная верстка А.М. Прудник

Подписано в печать 8.05.2003. Формат 60×84 1/16.
Печать ризографическая. Усл. печ. л. 7,84. Уч. изд. л. 7,1. Тираж 100 экз. Заказ .

Напечатано с оригинал-макета заказчика в типографии "Бестпринт". ЛВ № 260 от 11.09.2000.
220027, г.Минск, ул. Фабрициуса, д. 5, к. 1.
Унитарное предпрятие "Бестпринт".
220027, г.Минск, ул. Фабрициуса, д. 5, к. 1.

Издатель: Учреждение образования "Белорусский государственный университет информатики и радиоэлектроники"
Свидетельство № 1954 от 3.12.2002.

ОРГАНИЗАТОРЫ КОНФЕРЕНЦИИ
Министерство образования Республики Беларусь
Государственный центр безопасности информации РБ
Гостехкомиссия при Президенте 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

Российско-белорусская научно–техническая конференция

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

19 мая – 23 мая
2003
Минск — Нарочь

Материалы докладов и краткие сообщения

СОДЕРЖАНИЕ

Секция 1 Организационно-правовое и методологическое обеспечение

Секция 2. Защита информации в компьютерных и телекоммуникационных сетях

Секция 3. Технические средства обнаружения и подавления каналов утечки информации

Секция 4. Проблемы подготовки и переподготовки кадров

СЕКЦИЯ 1. ОРГАНИЗАЦИОННО–ПРАВОВОЕ И МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

АКТУАЛЬНЫЕ ЗАДАЧИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

В.Ф. ГОЛИКОВ

Многие важные процессы, протекающие сегодня в нашем государстве в сфере политики, экономики, безопасности, науки и техники связаны с необходимостью создания, передачи и хранения больших объёмов информации. Для решения этих задач всё шире используются современные системы, позволяющие автоматизировать работу с информационными ресурсами. Важнейшей характеристикой информационных объектов является их защищённость или в более широком смысле информационная безопасность. Обеспечение информационной безопасности объектов, как правило, комплексная проблема, включающая в себя создание правовой базы, нормативно-методических документов, комплекс организационных мер, технических средств, научно-исследовательские и опытно-конструкторские работы.

Становление системы технической защиты информации в Беларуси происходило на фоне разрыва связей с традиционными организационными и научно-техническими центрами в области информационной безопасности, оставшимися на территории Российской Федерации, а также бурного развития информационных технологий в развитых странах. Поэтому анализируемая сфера деятельности оказалась в положении постоянно догоняющей. И хотя на сегодня, благодаря существовавшему в республике научно-техническому потенциалу в области информационных технологий, некоторая часть дистанции успешно пройдена, тем не менее, проблем остаётся немало. Рассмотрим некоторые из них.

Научно-исследовательские работы. Актуальной темой исследований, на наш взгляд, остаётся исследование технических каналов утечки информации современных технических систем и средств создания обработки и передачи информации. Таких как: системы связи, автоматизированные системы управления критичными объектами, средства оргтехники и т.д. Задача этих исследований выявить реальный уровень опасности существования технических каналов. Так как недооценка их существования грозит серьёзным ущербом, связанным с утратой конфиденциальной информации, а переоценка — с ущербом за счёт неоправданных затрат на защиту. Ситуация здесь усугубляется тем, что, с одной стороны, развитие технических средств обработки информации идёт по пути снижения габаритов, материалоёмкости, потребляемой энергии, использования малоизлучающих проводников и эффективных экранов, сложных сигналов, т.е. всего того, что в конечном итоге значительно уменьшает уровень побочных электромагнитных, акустических, виброакустических, оптических и других сигналов, а также их информативность. С другой стороны, постоянно улучшаются технические характеристики разведывательной аппаратуры, увеличивается вероятность их скрытой доставки к границам объектов. Ускоряется темп смены оборудования: результаты научных исследований быстро устаревают. Все эти факторы требуют осмысления как с точки зрения системной постановки исследований, так и с точки зрения отдельных специализированных работ по электродинамике, акустике, виброакустике, оптике и т. д.

Второй крупной задачей (а по масштабам наиболее важной) являются исследования защищённости современных информационных систем, основывающихся на компьютерных сетях, от несанкционированного доступа. Здесь можно выделить следующие актуальные задачи:

Обнаружение несанкционированных действий с целью нарушения конфиденциальности, целостности и доступности информации. Обеспечение такого обнаружения основывается на использовании различных признаков: попытках обойти установленные в сети правила доступа типовыми способами, подбор паролей, резким увеличением активности действий и т. д. Правильно поставленное обнаружение атак позволит вовремя принять меры по их отражению и сохранить информационные ресурсы сети в неприкосновенности.

Аудит уязвимостей компьютерных сетей. Решение этой задачи заключается в периодической проверке безопасности системы с использованием программных или аппаратно-программных средств. При этом могут быть выявлены некорректные настройки системы безопасности, ошибки программного обеспечения, несанкционированные программные или аппаратные средства.

Исследование программных и аппаратных средств на наличие не декларированных функций. Задача "отягощается" тем, что в стране используется большое количество средств иностранного производства, поставляемых как "чёрные ящики". Наибольшую проблему здесь составляет использование операционных систем для различных вычислительных систем, являющихся "непрозрачными" для анализа. Многие страны идут по пути создания национальных операционных систем на базе свободно распространяемых типа "Linux". Республика Беларусь, на наш взгляд, располагает возможностями решения этой задачи, для этого необходимо сосредоточение усилий всех заинтересованных организаций и в первую очередь государственных в рамках некой национальной программы.

Исследования в области криптологии. Работы в этой области ведутся достаточно давно и успешно. Можно сказать, что белорусские специалисты владеют основательными теоретическими знаниями в

области построения современных криптосистем, имеют самостоятельные разработки теоретического и практического характера, что позволяет сделать вывод о том, что республика на сегодня в сфере криптотехнологий является самодостаточной.

Разработка технических средств защиты информации. Основные работы в этом направлении сводятся к разработке программных и аппаратно-программных средств, встраиваемых в существующие информационные системы. Имеется ряд изделий: по управлению доступом в компьютеры и компьютерные сети, устройства для криптографической защиты компьютерной и речевой информации, антивирусные программные средства, устройства активного зашумления, программно-аппаратные средства аутентификации пользователей и другие.

УГОЛОВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Т.В. РАДЫНО

Говоря об информационной безопасности, следует сказать: всякое государство имеет уязвимые стороны в деятельности государственных структур, коммерческих банков, предприятий, их структур, притягивающих злоумышленников. Именно поэтому развитие и распространение компьютерных систем и сетей сопровождается ростом правонарушений, связанных с кражами, злоупотреблениями, модификацией и неправомочным доступом к данным, хранящимся в памяти компьютера и передаваемых по линии связи.

В связи с вышеизложенным, в РБ получили свое развитие принципиально новые аспекты защиты информации, которые раньше не были вызваны объективной необходимостью. Одним из таких средств защиты являются меры по защите прав собственника по владению, пользованию, распоряжению и управлению информационными ресурсами. Действенным методом борьбы с хищениями путем использования компьютерной техники является включение данной новеллы в новый Уголовный кодекс Республики Беларусь. Необходимо отметить, что в правовом пространстве Российской Федерации подобного закона нет, или, иначе говоря, УК РФ 1996 г. не предусматривает подобного состава.

Непосредственным объектом данного преступления являются отношения собственности, вред которым причиняется путем хищения предмета преступления — движимого или недвижимого имущества, но чаще всего безналичных денежных средств. Объективная сторона данного преступления предполагает два варианта компьютерных манипуляций с целью обогащения за счет чужого имущества: изменение компьютерных программ, когда от каждой денежной операции осуществляется отчисление в пользу виновного: изменение номера счета одного лица на номер счета другого лица, за которым следует переадресация денег. Обычно подобная подделка осуществляется через иллюзию выборки по системе случайности.

Сложности в практике правоприменения вызывает отграничение мошенничества от хищения путем использования компьютерной техники. Ключевым моментом в такой ситуации является выяснение цели использования компьютера.

УНИВЕРСАЛЬНЫЙ КОМПЛЕКС КОЛЛЕКТИВНОГО ПОЛЬЗОВАНИЯ "ЭКЗАМЕНАЦИОННЫЙ КЛАСС — ИЗБИРАТЕЛЬНЫЙ УЧАСТОК"

В.Ю. ЛИПЕНЬ

Известен ряд систем обучения и тестирования знаний, использующих режим интерактивного взаимодействия испытуемого с обучающей системой. Вместе с тем, следует отметить, что ряд организаций, включая и Республиканский Институт контроля знаний (РИКЗ) Минобразования РБ, вынуждены использовать ручные технологии, основанные на процедурах заполнения испытуемыми опросных листов (ОЛ) и транспортировки ОЛ в уполномоченный компьютерный центр. Ручные технологии применяются и при проведении таких массовых мероприятий как опросы населения, референдумы, выборы, выдвижение кандидатов и т.п.

Построение автоматизированных систем (областных, республиканских), реализующих при приемлемых затратах указанные функции, возможно, по мнению автора, за счет использования сети недорогих универсальных пунктов опроса респондентов. Каждый из таких пунктов должен представлять собой многотерминальный (до 32 терминалов) комплекс на базе сетевого компьютера. При этом терминал респондента представляет собой простейший ручной пульт с цифровой клавиатурой и индикатором, которые служат для ввода номеров ответов. Использование большого числа дешевых терминалов, управляемых одним сетевым компьютером, позволяет осуществлять опрос большого числа респондентов и передавать через сеть данные на сервер регионального компьютерного центра для регистрации итогов единого государственного экзамена, выборов и др.

КОМБИНИРОВАННЫЕ МЕТОДЫ ЗАЩИТЫ И КОНТРОЛЯ ДОКУМЕНТАЛЬНЫХ ДАННЫХ

В.К. ЕРОХОВЕЦ, В.Ю. ЛИПЕНЬ, Д.В. ЛИПЕНЬ

Утвержденная 27.12.2002 г. Государственная программа "Электронная Беларусь" предусматривает в своем составе ряд проектов, направленных на создание ведомственных и территориальных автоматизированных информационных систем (АИС), решающих задачу компьютеризации органов госуправления. Одной из таких задач является радикальное расширение сферы использования электронных документов, а также внедрение компьютерного контроля за оборотом выдаваемых гражданам и юридическим лицам бумажных документов (свидетельств ЗАГС, лицензий, справок о собственности) и пластиковых карт (водительских и служебных удостоверений, удостоверений личности и юридических лиц).

Основным отличием внедряемых документов от традиционных является компьютерный способ их изготовления на основе цифровых данных, хранимых в регистрах населения и юридических лиц, а также — в базах данных ведомственных АИС. Такие машинозаполняемые документы могут содержать как традиционные человекочитаемые изображения (текст, фотопортрет, графическое оформление), так и специальные машиносчитываемые маркеры, например, штрих-коды (ШК). Для подобных документов с машиносчитываемой маркировкой могут применяться комбинированные методы защиты и контроля данных. Последние могут включать как процедуры сличения с электронным оригиналом при обращении к базе данных организации-эмитента, так и процедуры автономной верификации, построенные с использованием криптопрограмм, реализующих дешифрирование специальных ШК. Докладчиком демонстрируются примеры бумажных и пластиковых документов с машиносчитываемой маркировкой.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ДАННЫХ В СИСТЕМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ДЕЙСТВИЯМ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

Е.В. НОВИКОВ

В рамках реализуемой Министерством по чрезвычайным ситуациям Республики Беларусь государственной научно-технической политики в области предупреждения и ликвидации чрезвычайных ситуаций разработана многоуровневая автоматизированная система управления действиями дежурного персонала в чрезвычайных ситуациях, связанных с авариями на химически опасных предприятиях.

Функционирование этой системы, являющейся многоуровневой сетью комплексов, обеспечивающей мониторинг состояния отдельных объектов и передачу данных в соответствующие территориальные подразделения МЧС, невозможно без наличия, кроме прочих компонент, развитых телекоммуникационных средств. В этой коммуникационной среде на каждом уровне генерируется своя информация, объем, и значимость которой возрастают при переходе от одной ступени мониторинга к другой, и вместе с тем растет риск внешних вторжений в деятельность предприятий и органов управления.

Для ликвидации возможных угроз концепция безопасности системы строится с учетом реализации следующих требований:

- обеспечение защиты информации на всех этапах её накопления, обработки и передачи по каналам связи;
- обеспечение защиты информации в каналах связи путем максимального сокращения объемов передачи (передача метаданных, а не полного объема информации) с применением криптографических методов;
- обеспечение целостности и подлинности информации на всех этапах ее хранения, обработки и передачи по каналам связи:
- обеспечение аутентификации сторон, обменивающихся информацией;
- обеспечение контроля доступа к информационным системам и базам данных; а также защита программных продуктов от внедрения программных "вирусов" и закладок.

Разграничение доступа обеспечивается путем использования возможностей операционной системы сервера и средств многопользовательских операционных систем. На всех уровнях разграничения доступа запрещаются все действия, кроме явно разрешенных.

ФОРМИРОВАНИЕ И ИСПОЛЬЗОВАНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ К ОБЪЕКТАМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

А.А. ГУЛЬКО, Т.С. МАРТИНОВИЧ

В докладе рассматриваются вопросы формирования пакетов функциональных и гарантийных требований безопасности на базе стандарта СТБ 34.101, а также порядок использования требований безопасности при сертификации средств реализации этих требований.

При формировании требований безопасности учитывается незавершенность большинства функциональных и гарантийных требований безопасности стандарта СТБ 34.101, ценность информации, архитектура объекта и способы обработки информации.

Для разработки нормативных документов "*Профиль защиты*" и "*Задание по обеспечению безопасности*" предлагается использовать набор детализированных требований безопасности, систематизированных с учетом привязки к объектам информационных технологий и к существующим классам требований СТБ 34.101.

Приводится пример формирования пакетов функциональных и гарантийных требований безопасности.

Описаны подходы при сертификации средств реализации требований безопасности на базе пакетов функциональных и гарантийных требований безопасности.

ФУНКЦИОНАЛЬНЫЕ И ГАРАНТИЙНЫЕ ПАКЕТЫ ТРЕБОВАНИЙ К СРЕДСТВАМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

С.К. ТУРБИН, М.А. ТАЛАЛУЕВА

Рассматривается задача формирования требований по управлению безопасностью в виде пакетов требований.

В практике имеются случаи, когда на ранних этапах разработки информационных систем нельзя четко описать объект, угрозы безопасности и на этой основе сформулировать задачи безопасности. В этих случаях целесообразно разрабатывать не профиль защиты (ПЗ), а пакеты функциональных и гарантийных требований.

По существу разработка пакета – первый шаг к созданию некоторого профиля защиты или семейства ПЗ, и к использованию в задании по обеспечению безопасности (ЗБ).

Опыт формирования пакетов весьма ограничен. На сегодняшний день практическими примерами пакетов являются уровни гарантии оценки, определенные в СТБ 34.101.3, которыми следует пользоваться для формирования гарантийных пакетов.

Пакеты, предназначены для многократного использования:

- потребителями в качестве пособия при обосновании требований к средствам управления безопасностью;
- экспертами (испытателями) при проверке соответствия представленных на сертификацию средств управления безопасностью заданным функциональным и гарантийным требованиям безопасности.

Эффект от использования пакетов состоит:

- в уменьшении стоимости разработки ПЗ и (ЗБ);
- в сокращении сроков и объемов работ при разработке ПЗ или ЗБ при выборе или определении требований к средствам управления безопасностью.

КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

С.К. ТУРБИН, В.К. ФИСЕНКО

Основными целями защиты информации являются обеспечение ее конфиденциальности, целостности и доступности. Поэтому целесообразно провести классификацию всего множества средств защиты по целевому назначению. С учетом того, что в соответствии с принципом суперпозиции сложная техническая система подразделяется на средства непосредственно исполнительные и средства, поддерживающие эффективное функционирование первых, установлено следующее множество классов средств защиты информации { A_i }:

A_1 — класс средств обеспечения конфиденциальности;

A_2 — класс средств обеспечения целостности;

A_3 — класс средств обеспечения доступности;

A_4 — класс средств контроля (аудита) безопасности;

A_5 — класс средств управления безопасностью.

Задача распределения средств защиты информации из заданного множества $\{S_j\}$ по классам $\{A_i\}$ решается путем логической проверки наибольшего соответствия совокупности признаков целевой направленности средства $(n_{1j},...n_{ij},...n_{Ij})$ классификационным признакам A_i – го класса $(r_{1i},...r_{mi},...r_{mI})$ – $max_{ji}\ (n_{ij} \Lambda\ r_{mi}) => S_j \in A_i$.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

А.В. ПРИБЫЛЬСКИЙ, Т.Г. ТАБОЛИЧ

В условиях рыночной экономики резко обостряется конкурентная борьба между производителями товаров и услуг за потенциальных заказчиков и потребителей. Большинство предприятий РБ пока не занимают лидирующих позиций в этой борьбе на белорусском и зарубежных

рынках. Одной из причин такого положения является доступность к информации предприятия, выпускающего конкурентную продукцию. Одним из путей выхода из такой ситуации могли бы стать мероприятия, направленные на усиление информационной безопасности предприятия, т.е. на защиту информации [1]. Защита информации на любом предприятии может быть представлена в виде трех уровней:

1. Защита от конкурентов технико-экономических показателей выпускаемой продукции или научно-исследовательских и опытно-конструкторских разработок, в особенности в перспективных направлениях.

2. Защита внутренней текущей информации предприятия, в том числе данных о себестоимости продукции, складских запасах, наличии технических проблем.

3. Защита информации или данных, которые в том или ином виде присутствуют в выпускаемых изделиях.

Первых два уровня относятся к организационно-техническим мерам обеспечения безопасности, и их реализация сводится в основном к следующим действиям [1]:

- организация пропускного режима и службы безопасности,
- отбор работников при приеме на работу,
- заключение контрактов с работниками, в которых отражается ответственность за передачу информации третьим лицам,
- защита информации в локальной вычислительной сети (ЛВС) предприятия; введение в штат сотрудников, отвечающих за безопасность информации внутри сети.

К третьему уровню защиты информации может относиться защита технологии изготовления изделия (например, микросхемы), которая может быть восстановлена при анализе изделия, а также защита информации, хранящейся в самом изделии. Примером изделий, содержащих нуждающуюся в защите информацию, являются выпускаемые НИРУП "ЦНИИТУ" электронные пластиковые карты (ЭПК). В настоящее время НИРУП "ЦНИИТУ" постоянно наращивает выпуск телефонных ЭПК, освоена первая опытная партия банковских ЭПК, планируется освоение ЭПК для других применений — в качестве пропусков для проходных, автостоянок, для автоматизации выдачи зарплаты на предприятиях и т.д. Важнейшим техническим показателем и необходимым условием востребованности на рынке для телефонных ЭПК является защищенность их от несанкционированной перезарядки, для банковских ЭПК — их защищенность от несанкционированного доступа к содержащимся в ЭПК платежным ресурсам. По данному показателю ЭПК НИРУП "ЦНИИТУ" соответствуют современному научно-техническому уровню [2].

Литература

1. Тимченко И.М. Организационно-технические меры обеспечения комплексной безопасности предприятия: методология, специальные технические средства//Конспект лекций научно-практического семинара для руководителей предприятий Министерства промышленности Республики Беларусь по теме: "Обеспечение безопасности хозяйственной деятельности предприятия в рыночных условиях" (Минск, 18-19 февраля 2003 года). - Мн.: Институт экономики НАНБ, 2003. – С. 45-49.

2. Вечер Д.В., Прибыльский А.В., Реуцкий В.С., Таболич Т.Г. Сравнение кристаллов пластиковых карт по степени защиты информации//В этом сборнике. – С.

ЗАЩИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАНЫ ПРИ РЕГУЛИРОВАНИИ ИНТЕЛЛЕКТУАЛЬНОЙ МИГРАЦИИ

М.В. АЗАРЕНКО, А.Г. ПАЦЕЕВА

Организация защиты информации предполагает наличие целого комплекса разноцелевых разработок, повышающих эффективность управления не только техническими процессами, но и человеческими факторами. С формальной стороны человеческие отношения и в этой области регулируются правовыми нормами, например, законом РБ "О государственных секретах". Законодательство РБ предусматривает защиту большого набора разнообразных видов тайн, которые объединяются общей категорией — конфиденциальностью [1]. Разрабатываются основные организационные принципы защиты информационных ресурсов страны.

При такой разработке целесообразно учесть один из важных источников утечки информации - миграцию научных кадров [2]. Действительно, основными создателями научного и научно-технического информационного продукта являются научные кадры. Результаты научной деятельности, как правило, принадлежат ученому или научному коллективу, их создавшему. В свою очередь, государство заинтересовано в том, чтобы практическая реализация этих результатов осуществлялась в пределах страны, где информационный продукт был создан. Правовое регулирование вопросов собственности на ту или иную информацию заложено в патентном праве. С другой стороны, большое количество информации, идей, разработок, технологических нововведений до официального оформления прав собственности принадлежат их создателям. В силу того, что человек считает более выгодным для себя реализовать свои инновации и права на них в условиях другой страны, эти информационные ресурсы теряются для стран-доноров. Для стран с переходной экономикой, какой является Республика Беларусь, это создаёт проблемную ситуацию — чем интереснее разработки ученого для мировой науки или для иностранных компаний, тем выше вероятность того, что он уедет в другую страну, с более благоприятными социально-экономическим условиями. Страна в этом случае терпит не только информационные, но и прямые

экономические убытки. Для прекращения утечки информации за рубеж путем научной миграции кадров в республике в настоящее время не существует надежных правовых и организационных норм.

Поэтому для глубокой проработки вопроса об информационной безопасности страны с учетом влияния человеческого фактора при миграции кадров необходимо создание временных коллективов разработчиков названных норм. В этот коллектив обязательно должны войти специалисты по вопросам защиты информации Государственного центра защиты информации, Комитета государственной безопасности, Министерства труда и социальной защиты, Государственного Таможенного Комитета, аппарата Совета Министров, Национальной Академии Наук Беларуси, министерства образования и других заинтересованных государственных органов управления и науки. Дополнить коллектив могли бы специалисты Центра мониторинга миграции научных кадров при НАН Беларуси, изучающего миграцию на постоянное место жительства и выезд по долгосрочным контрактам за рубеж.

Результатом работы такого коллектива могло бы стать создание правовой базы и организационных структур для государственного регулирования интеллектуальной миграции в части защиты информационных ресурсов страны. В дальнейшем данной работой могли бы заниматься научные организации в области защиты информации.

Литература

1. Азаренко М.В. Организация защиты государственных секретов в государственных организациях в соответствии с белорусским законодательством // Конспект лекций научно-практического семинара для руководителей предприятий Министерства промышленности Республики Беларусь по теме: "Обеспечение безопасности хозяйственной деятельности предприятия в рыночных условиях" (Минск, 18–19 февраля 2003 года). Мн.: Институт экономики НАНБ, 2003.
2. Мирская Е.З. Современные телекоммуникационные технологии в Российской академической науке // Науковедение. 2000. № 3. С. 48–56.

СЕКЦИЯ 2. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

ИНТЕГРИРОВАННАЯ СИСТЕМА ПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ АНАЛИЗА ДИНАМИКИ КЛАВИАТУРНОГО НАБОРА

В.Л. БАЛАЩЕНКО, Н.Я. РАДЫНО

Основным средством аутентификации при подключении к локальным или сетевым информационным ресурсам является парольная аутентификация. Мы предлагаем рассмотреть систему, позволяющую повысить надежность парольной аутентификации за счет анализа динамики клавиатурного набора пользователя.

Подсистема анализа динамики клавиатурного набора интегрирована с графической подсистемой идентификации и аутентификации пользователя интерактивной системы Winlogon. Разработанный модуль внедряется в процесс аутентификации защищенной службы Local Security Authority (LSA), перехватывая системные вызовы Winlogon. Система реагирует на вызовы функций WlxLoggedOutSAS, WlxLoggedOnSAS или WlxWkstaLockedSAS и запускает механизм перехвата нажатий клавиш в диалоговом окне Winlogon.

Далее система сравнивает полученные значения временных интервалов с эталонными. База эталонных значений содержит значения временных интервалов парольных фраз пользователей зарегистрированных в домене. Алгоритм аутентификации пользователя по динамике набора парольной фразы заключается в анализе относительного расстояния каждого временного интервала до группы эталонных значений. Алгоритм аутентификации прошел тестирование и обеспечивает необходимую точность аутентификации. Решение задачи аутентификации и более общая задача идентификации пользователя по набору фиксированной парольной фразы рассмотрена в работах [1, 2].

Указанная система является прозрачной для пользователя и незаметной для злоумышленника и позволит существенно повысить безопасность доступа к информационным ресурсам локальной вычислительной сети.

Литература

1. Радыно Н.Я. Алгоритм идентификации пользователя компьютера по набору фиксированной фразы на клавиатуре. Весці НАН Беларусі, 2002, № 3 ст. 70–76.
2. Балащенко В.Л., Радыно Н.Я. Задача идентификации пользователя компьютера по набору фиксированной фразы на клавиатуре. Материалы XIII Международной конференции "Проблемы теоретической кибернетики". Часть I. М: Издательство центра прикладных исследований при механико-математическом факультете МГУ, 2002, стр. 16

ТЕХНИЧЕСКИЕ СРЕДСТВА ДЛЯ СИНТЕЗА И ИДЕНТИФИКАЦИИ ГОЛОГРАФИЧЕСКИХ ЗАЩИТНЫХ ЭЛЕМЕНТОВ

В.К. ЕРОХОВЕЦ

Голографическая защита документов и ценных бумаг, упаковки продуктов питания и промышленных товаров считается на сегодняшний день одним из наиболее труднодоступных для подделки методов. Разнообразие информационных свойств голограмм определяет большое число степеней защиты, которое может составлять более десятка.

В докладе рассматриваются методы аналогового и компьютерного синтеза голографических защитных элементов (ГЗЭ). В первую очередь — это классические голограммы сфокусированных изображений (ГСИ) с использованием высокоразрешающего ввода через LCD-транспаранты цветоделенных изображений, а также "dot-matrix" и "line-matrix"технологии получения ГСИ. Последние технологии обладают широкими возможностями получения защитных микротекстов и графики. Однако анализ таких ГСИ возможен лишь в лабораторных условиях с применением относительно дорогих микроскопов.

В этой связи перспективным направлением является комбинирование технологий получения ГЗЭ с одним или несколькими скрытыми изображениями. Кодирование скрытого изображения, как правило, является "know-how" производителя ГЗЭ. Скрытые изображения оперативно воспроизводятся с помощью простых и дешевых приборов для идентификации ГЗЭ. Авторами разработаны ряд способов и технических решений по защите и идентификации голограмм.

Предложена дифракционная модель голограммы скрытого изображения, на основе которой разработана конструктивная теория расчета геометрических и энергетических параметров голографических идентификаторов.

ИСПОЛЬЗОВАНИЕ ТВЕРДОТЕЛЬНЫХ ФОТОПРИЕМНИКОВ В РЕЖИМЕ СЧЕТА ФОТОНОВ ДЛЯ КВАНТОВОЙ КРИПТОГРАФИИ

И.Р. ГУЛАКОВ, А.О. ЗЕНЕВИЧ, В.Л. КОЗЛОВ

В настоящее время для защиты информации, передаваемой по волоконно-оптическим линиям связи (ВОЛС), используют методы квантовой криптографии. Заключающей в том, если передача информации в ВОЛС осуществляется слабыми оптическими импульсами, содержащими десятки или сотни фотонов то любая попытка перехвата информации, будет обнаружена. Это связано с тем, что согласно квантовомеханической теории нельзя произвести измерения в системе, не изменив ее состояния. Тогда любая попытка перехвата информации приведет к появлению помех и обнаружению перехвата.

Для реализации такого квантового канала связи необходимо использовать фотоприемники способные регистрировать слабое оптическое излучение. В качестве таких фотоприемников для ВОЛС можно использовать лавинные фотодиоды (ЛФД), работающие в режиме счета фотонов. Поэтому целью данной работы являлась оценка возможности использования лавинных фотодиодов для методов квантовой криптографии.

В качестве объектов исследования были выбраны серийно выпускаемые кремневые лавинные фотодиоды ФД-115л и германиевых ЛФД-2.

Анализ схем включения ЛФД, реализующих режим счета фотонов показал, что для таких целей наиболее подходит стробирование фотодиода прямоугольными импульсами [1, 2]. Поскольку такое включение позволяет значительно понизить вероятность образования темновых импульсов за счет регулирования длительности импульса стробирования и обеспечивает достаточно высокое быстродействия.

На основании методики предложенной в работе [3], проведена оценка мощности оптического излучения P в максимуме чувствительности ЛФД (длина волны оптического излучения λ=0,84 мкм для кремния и λ=1,1 мкм для германия) необходимая для обнаружения импульса с вероятностью ошибки 10^{-5} и она составила P=0,3×10^{-9} Вт для кремниевых и 0,2×10^{-9} Вт для германиевых фотодиодов (это соответствует 300 фотонам). Скорость передачи данных при этом составит 2 Мбит/с. Расчет проведен для длительности импульса стробирования 250 нс, скорости счета темновых импульсов 100 с$^{-1}$ и квантовой эффективности регистрации 0,1.

Проведенные расчеты показали возможность использования кремниевых лавинных фотодиодов для методов квантовой криптографии.

Литература

1. Гулаков И.Р., Холондырёв С.В. Метод счёта фотонов в оптико-физических измерениях. — Минск: Университетское, 1989. 256 с.
2. Гулаков И.Р., Зеневич А.О. Приборы и техника эксперимента. 2001. № 4, С. 21-23.
3. Унгер Г. Оптическая связь. М.: Связь,1979. 264 с.

ШИФРОВАНИЕ ИНФОРМАЦИИ НА ОСНОВЕ МЕТОДА МОДИФИКАЦИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

К.Я. АВЕРЬЯНОВ, А.А. БОРИСКЕВИЧ

Предложен итерационный метод модификации псевдослучайных последовательностей (ПСП), основанный на формировании последовательности случайных сдвигов из исходной ПСП, сложении по модулю 2 исходной ПСП и ее копии, смещенной на величину первого случайного сдвига из выбранных. Процесс повторяется для каждого значения случайного сдвига из оставшихся с целью получения результирующей непериодической ПСП с хорошими корреляционными свойствами. Перед сложением исходная ПСП и ее сдвинутая копия дополняются нулевыми битами, количество которых определяется величиной случайного сдвига. Величина случайного сдвига не превышает значения 2^{n-1}, где n — количество бит, равное длине сегментов, на которые разбивается исходная ПСП.

На основе метода модификации ПСП предложен метод внесения информации в ПСП. Он состоит в разбиении последовательности данных на равные блоки длиной не меньше 2 бит, добавлении старших разрядов, содержащих единицы, ко всем ненулевым и нулевым блокам (или исключении нулевых блоков) последовательности данных и формировании последовательности случайных сдвигов. Двоичная информация, содержащая в блоках последовательности данных, задает величины случайных сдвигов. В остальном процесс шифрования аналогичен процессу модификации ПСП.

Ключами для извлечения информации является ПСП и длина блока разбиения шифруемой последовательности данных. Процесс расшифровывания заключается в сложении по модулю 2 ключевой ПСП с ПСП, содержащей информацию. Восстанавливаемая последовательность первых нулевых бит соответствует величине случайного сдвига. После отбрасывания данных нулевых бит процесс повторяется до тех пор, пока длина зашифрованной последовательности не достигнет длины ключевой ПСП. Образованная последовательность величин случайных сдвигов с помощью второго ключа, указывающего какой разрядности эти величины в двоичной системе, преобразуются в исходную последовательность данных, дополненную старшими разрядами, содержащими единицы (или нулевыми блоками, исключенными на этапе шифрования).

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ШИФРОВАНИЯ MPEG ВИДЕОДАННЫХ

А.А. БОРИСКЕВИЧ, И Ю. Г.КОЧУБЕЕВ

Сетевые приложения мультимедиа, такие, как Видео-По-Требованию, широковещательная передача видео и видеоконференции требуют проведения исследований в области безопасности мультимедиа. Из-за особенностей мультимедийных данных возникает необходимость в разработке специальных алгоритмов шифрования *MPEG* видеоданных, которые должны быть одновременно высокозащищенными, высокоскоростными и не ухудшать уровень сжатия.

Стандарт *MPEG* является одним из наиболее универсальных принятых международных стандартов для кодирования и передачи динамических видеоизображений. Предлагается следующая классификация современных методов шифрования *MPEG* данных:

1) методы, использующие особенности формата *MPEG*;

2) методы, основанные на статистических особенностях потока *MPEG*;

3) методы, использующие возможности кодирования при шифровании *MPEG* видеоданных.

Рассмотрен селективный алгоритм шифрования наиболее важных частей потока *MPEG* (*I*-кадров), относящийся к первой группе. Он обеспечивает четыре уровня защиты с разным объемом шифруемой информации. Представителем второй группы является алгоритм видео шифрования (*VEA*), использующий шифры с разной вычислительной сложностью и обеспечивающий высокое быстродействие (на 48 % быстрее прямого шифрования), высокую защищенность. К третьей группе относится алгоритм с изменяемой моделью адаптивного кодека (*ИМАК*), обеспечивающий высокую скорость, защищенность и не увеличивающий исходный поток данных. Он основан на применении для каждого байта не сжатой информации своей таблицы Хаффмана.

Из сравнительного анализа следует, что более предпочтительными по всем критериям являются алгоритмы *VEA* и *ИМАК*. Они обеспечивают высокую защищенность наряду с высоким быстродействием и малым размером зашифрованного потока *MPEG*.

МАГНИТНАЯ ЗАЩИТА НОСИТЕЛЯ ИНФОРМАЦИИ НА ОСНОВЕ ИМПУЛЬСНОГО МАГНИТНОГО МАРКЕРА

А.А. БОРИСКЕВИЧ, В.Я. КУЛИК

Метод защиты основан на имплантировании в материальный носитель информации маркера со специфической магнитной структурой, обеспечивающей эффект быстропротекающего перемагничивания вещества маркера. Данный эффект наблюдается в виде скачкообразного изменения намагниченности при помещении маркера в переменное магнитное поле. Магнитная структура маркера, представляющая собой два или больше доменов, намагниченных встречно, идентифицирует носитель. Под воздействием внешнего возбуждающего магнитного поля в направлении намагниченности одного из доменов при пороговом значении поля происходит спонтанное перемагничивание домена с противоположным полю исходным направлением намагниченности. Такой процесс повторяется при циклическом перемагничивании маркера.

При помещении считывающей обмотки вблизи маркера в момент его скачкообразного перемагничивания поместить в ней возбуждается импульс напряжения. Форма и другие характеристики импульса существенно зависят от материала маркера, его геометрии, способа и режимов его получения, обработки сигнала с выхода приемной катушки.

К достоинствам магнитной защитной маркировки на основе импульсного магнитного маркера следует отнести стабильность параметров регистрируемого импульса напряжения, технологичность получения и встраивания маркера в корпус носителя, высокую надежность, объективность и бесконтактность контроля подлинности.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА АТС

Д.В. ШИПОВАЛОВ

В докладе рассматривается некоторые аспекты обеспечения информационной безопасности *АТС*, которая должна достигаться с помощью системы комплексной защиты информации (*КЗИ*) от перехвата информации в каналах связи, несанкционированного доступа к информации, утечки информации по побочным каналам, внедрения специальных технических устройств перехвата информации, программно-технических воздействий и программ-вирусов. Исследуются вопросы защиты от наличия в составе программного обеспечения (*ПО*) возможных программных закладок (*ПЗ*), активация которых может дезорганизовать работу как отдельной станции, так и всей сети.

Рассматривается необходимость реализации на *АТС* ряда эксплуатационных правил, регламентирующих периодическое выполнение копирования на специально выделенный внешний носитель (*ВНН*) рабочих областей оперативного запоминающего устройства (*ОЗУ*), станционных управляющих устройств, а также областей *ОЗУ*, хранящих программы, текущие переменные и постоянные данные о ресурсах станции и системы.

В докладе предлагаются методы действия персонала при обнаружении признаков активации *ПЗ*.

Исследуется необходимость разработки, и внедрения технических средств познакового документирования всей вводимой с пультов информации с жестким непрерывным административным контролем регламента пультового времени.

Также в докладе рассматриваются аспекты защиты информации исключением передачи по *ОКС* № 7 от международного центра коммутации к станциям *АМТС* сообщений с нетелефонными функциями (для предотвращения активации *ПЗ*, форматов *TCAP* и *OMAP*). В докладе предлагается разработка и установка на международном участке специальных тестирующих устройств, обеспечивающих обнаружение и фиксацию всех случаев передачи нетелефонных сообщений четвертого уровня.

Рассматривается обеспечение защиты от несанкционированного доступа к передаваемой информации, которое может быть достигнуто обнаружением искажений в передаваемой информации, реализуемое, например, методом контрольных сумм.

Литература

1. Технические аспекты защиты информации в АТСЦ-90 // http://kiev-security.org.ua
2. Бобов М.Н., Конопелько В.К. Обеспечение безопасности информации в телекоммуникационных системах. Мн.: БГУИР, 2002, 164 с.

ВЫБОР СТРУКТУРЫ АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ВИДЕОКОНФЕРЕНЦИЙ

В.Е. САМСОНОВ, В.С. ШАРАК

В связи с широким распространением систем видеоконференций актуальной задачей является обеспечение защиты сетевого трафика в этих системах. Повышенные требования к пропускной способности сетевой инфраструктуры видеоконференций требуют аппаратной реализации криптографической защиты сетевого трафика.

В докладе изложены результаты экспериментальных работ по аппаратной реализации криптографической защиты информации на сетевом уровне стека протоколов TCP/IP для использования в системах видеоконференций.

Экспериментальный образец устройства выполняет все функции интерфейса PCI шины и управляется драйвером ядра ОС Windows NT, 2000.

Были исследованы такие параметры как скорость аппаратного шифрования одного, скорость преобразования одного IP-пакета, время выполнения передачи пакета в память ЭВМ в режиме DMA, время реакции на прерывания устройства в т.ч. по завершению DMA, а также различные варианты построения драйвера устройства в операционных системах Windows NT, 2000. На основании проведенных оценок выбрана оптимальная структура устройства и метод построения драйвера, позволяющих эффективно производить криптографическое закрытие информации в системах видеоконференций.

ВНЕДРЕНИЕ ВОДЯНОГО ЗНАКА В ПО НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СТАТИСТИЧЕСКИХ СВОЙСТВ ИСПОЛНЯЕМОГО КОДА

С.С. ПОРТЯНКО

Уже на протяжении многих лет компании, разрабатывающие ПО с целью его продажи, теряют значительную часть доходов из-за компьютерного пиратства. Для того, чтобы препятствовать незаконному тиражированию ПО и для идентификации своих продуктов с целью обеспечения возможности доказательства принадлежности ПО разработчику, чьей интеллектуальной собственностью оно является, используется ряд методик. К их числу относится использование программно-аппаратных ключей (Software Dongles), стеганографические методы, такие как внедрение водяных знаков (watermarks) и "отпечатков пальцев" (fingerprints).

Предлагаемый метод идентификации исполняемого кода приложения является адаптацией основной идеи метода Patchwork, предложенного в [1] применительно к графическим изображениям, к использованию её для внедрения в код программы некоторого признака, характеризующего её принадлежность тому или иному разработчику. Метод основан на использовании статистических свойств исполняемого кода программы, определяющихся частотами встречаемости той или иной команды при осуществлении их случайной выборки.

Проведённые экспериментальные исследования показали, что для конкретной программно-аппаратной платформы распределение инструкций в исполняемых файлах имеет определённый вид, незначительно меняющийся от приложения к приложению.

Непосредственно внедрение водяного знака в программу заключается в модификации вида распределения индексов команд для некоторого подмножества команд программы, полученного в результате случайной выборки, таким образом, что бы оно существенно отличалось от типичного распределения команд для исполняемых файлов для данной программно-аппаратной платформы.

Для того, что бы при статистическом анализе исполняемого кода перейти от символик либо кодов инструкций к числам, производится назначение каждому типу команды индекса.

При внесении изменений в исполняемый код программы, одни группы команд заменяются на другие, являющиеся эквивалентными, чем и достигается модификация частот встречаемости определённых команд, а значит и вида их распределения.

Оптимальное построение списка взаимозаменяемых групп команд обеспечивает наибольшую эффективность процедур замены команд.

В [2] предложен ряд способов трансформаций исполняемого кода программы, служащих для минимизации времени её выполнения, которые могут быть применены и для воздействия на частоты встречаемости определённых команд.

Литература

1. W. Bender, D. Gruhl, N. Morimoto, A. Lu Techniques for data hiding.
2. David F. Bacon, Susan L. Graham and Oliver J. Sharp Compiler transformations for high performance computing.

УСТРОЙСТВО ПОИСКА ДЛЯ СИСТЕМ ТРАЕКТОРНЫХ ИЗМЕРЕНИЙ И СКРЫТНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

И.И. АСТРОВСКИЙ, В.К. КОНОПЕЛЬКО

Применение в современных системах радиолокации, радионавигации и связи сигналов с большой базой требует решения сложных проблем, связанных с ускорением генерирования и обработки сигналов, обеспечением помехоустойчивости и скрытной передачи информации.

Наибольшие временные или аппаратурные затраты, как правило, приходятся на поиск по временному положению (задержке). Задержка обычно определяется либо величиной перестройки опорного генератора до получения синхронного положения опорного сигнала приемника со входным, либо временем рассогласования начала входного сигнала с условными моментами отсчетов эталонного времени. Требованиям практики не удовлетворяет как одноканальный обнаружитель из-за больших временных затрат, так и многоканальный из-за больших аппаратурных затрат.

В работах [1, 2] было предложено использовать для целей поиска бинарные псевдослучайные последовательности Велти [3], которые генерируются на основе функций Радемахера и имеют регулярную структуру. Начальные отрезки, длительность которых кратна степени двойки, регулярно повторяются в прямом или инверсном по знаку виде, что позволяет организовать дихотомический поиск, который требует вместо $N/2$ (в среднем) только около $\log_2 N$ вычислительных процедур, сходных с вычислением корреляционной функции.

В докладе предлагается дихотомическая процедура поиска на основе функции суммы модулей, которая вычисляется путем последовательного суммирования абсолютных значений коротких корреляционных функций отрезков входной и опорной последовательностей.

Обосновывается криптостойкость совмещенных систем траекторных измерений и скрытной передачи информации. Показано, что алгоритм построения последовательностей Велти аналогичен алгоритму построения древовидных свёрточных кодов. Причем длина и мощность кода пропорциональны степени двойки, а начальные комбинации регулярно повторяются в прямом или инверсном виде. При отсутствии информации о длине последовательности код приобретает свойство криптостойкости. Случайный перебор длин не решает проблемы.

Предлагается процедура дополнительной манипуляции по знаку исходной последовательности в соответствии с передаваемой низкочастотной информацией. Эта манипуляция не нарушает принципов используемых алгоритмов поиска, не ухудшает качественные характеристики предложенных ранее систем поиска.

Литература

1. Клюев Л.Л., Астровский И.И. Синхронизация приемных устройств по задержке при приеме Д-последовательности. — "Радиотехника и электроника", 1975, т. 20, № 1, с. 178–181
2. Астровский И.И., Клюев Л.Л. Устройство синхронизации псевдошумовых сигналов по задержке. А.С. СССР. № 520716. — "БИ",1976, № 25.
3. Велти. Четверичные коды для импульсного радиолокатора. — "Зарубежная радиоэлектроника", 1961, № 4.

ИСКАЖЕНИЯ ЭЛЕКТРОДИНАМИЧЕСКИХ ПАРАМЕТРОВ СИГНАЛОВ В РАДИОКАНАЛЕ НАД АНИЗОТРОПНЫМ ВКЛЮЧЕНИЕМ

П.М. КАТЛЕРОВ, Д.В. ГОЛОЛОБОВ

Одной из основных причин частичного или полного искажения информационных параметров сигнала в реальном радиоканале без искусственных помех являются процессы электродинамического взаимодействия электромагнитной волны (ЭМВ) с естественными или искусственными неоднородностями. В общем случае неоднородности, возникающие в радиоканале, следует считать анизотропными, описываемыми тензорами диэлектрической и магнитной проницаемости.

Данная проблема может возникнуть в транкинговых системах связи, компьютерных радиосетях, радиорелейных линиях связи, которые работают в различных диапазонах частот на дальних расстояниях.

Проведена оценка электродинамических параметров ЭМВ при распространении по радиотрассе с естественным анизотропным включением, образованным за счет подмагниченного электронно-ионного потока в среде с потерями.

Результаты аналитических и экспериментальных исследований свидетельствуют о следующем:

заметная потеря информации на анизотропном включении может произойти за счет дисперсионных свойств среды;

в отдельных диапазонах частот происходит расщепление поверхностной ЭМВ на набор волн с различными фазовыми и групповыми скоростями, свидетельствующими об изменении поверхностного импеданса неоднородности;

на возникающей нерегулярности наблюдается трансформация поляризационной характеристики.

Данные результаты следует учитывать при планировании, прокладке радиотрасс над естественными или искусственными неоднородностями, следует уменьшать вероятность ошибки за счет повышения соотношения сигнал/помеха, либо применять системы с передачи информации, устойчивые к такого рода помехам.

В задаче выделения неоднородностей в радиоканале обозначенные признаки приобретают практический смысл, способствуя повышению точности регистрации границ анизотропной неоднородности.

При решении задачи идентификации естественных и искусственных объектов на фоне подстилающей среды по известному радиопортрету учет вышеобозначенных признаков повышает уровень достоверности распознавания.

Разработана модель неоднородной анизотропной среды, которая способна дополнить существующие модели радиоканалов.

СОВРЕМЕННАЯ ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ В СРЕДЕ ИНТЕРНЕТ

В.М. КОЛЕШКО, А.А. КОЛБ

Взрывообразное развитие глобальных сетей существенно осложнило проблему защиты информации в корпоративных сетях, использующих среду Интернет. Это обусловлено основными свойствами сети Интернет — демократичностью, открытостью, доступностью, глобальностью. Эти свойства сыгравшие, несомненно, положительную роль для быстрого развития этой сети, делают неэффективным использование традиционных методов защиты информации в корпоративных сетях — закрытой архитектуры, административного регулирования, многоэтапности доступа и т.д.

Происшествие с безопасностью — событие, которое нанесло или может нанести вред работе сетей, последствием которого могут быть мошенничество, потеря или разрушение собственности организации или информации.

Хотя при защите соединения с Интернетом в основном защищаются от внешних угроз, неправильное использование соединений с Интернетом внутренним пользователем часто тоже является значительной угрозой. Использование распределенных систем привело к появлению большого числа уязвимых мест, и поэтому недостаточно просто "закрыть двери и запереть их на замки". Требуются гарантии того, что сеть безопасна — что "все двери закрыты, надежны, а замки интеллектуальны".

В работе рассмотрены современные особенности построения структуры и логистика безопасности в корпоративных сетях, использующих среду Интернет, даны конкретные рекомендации по эффективной защите сетей, приведены примеры конкретной реализации на опыте многолетней работы в системе "Нетворк системс".

ЛОГИСТИКА И ЗАЩИТА ИНФОРМАЦИИ ТОРГОВОЙ СЕТИ ГИПЕРМАРКЕТОВ

В.М. КОЛЕШКО, Е.В. ПОЛЫНКОВА, В.Ю. ПОЛЫНКОВ

В разветвленной системе гипермаркетов обращается огромное количество товаров и финансовых документов. Серьезной проблемой является защита экономических интересов акционеров от мошеннических действий наемных работников. По данным Интерпола более 90 % экономических преступлений в субъектах хозяйствования (акционерных обществах) совершается при прямом или косвенном участии наемных работников этих же обществ. Анализ совершенных преступлений показывает, что наиболее уязвимым местом является документооборот товаропотоков и финансовых потоков. Разработанная электронная система логистики над документооборотом, товарооборотом и финансовыми потоками гипермаркетов и их филиалов включает интеллектуальный интерфейс и специальные программы логистики, имеет многоярусную радиально-узловую структуру, в ней используются индектифицированные протоколы обмена и защиты информации и электронные ключи.

Глобальный контроль над документооборотом, товарооборотом и финансовыми потоками основан на новой (защищенной патентами) компьютерной технологии защиты документов от подделки. Это позволяет повысить эффективность работы гипермаркетов, получить акционерам дополнительную (независимую) информацию о финансовой деятельности и улучшить их управляемость и рентабельность.

Интеллектуальная прогнозирующая система позволяет с высокой точностью предсказать ожидаемый спрос на различные товары в краткосрочный и долгосрочный перспективе, минимизировать складские затраты, существенно сократить требуемый объем оборотных средств, минимизировать расходы на рекламу и максимизировать прибыль торгового предприятия.

Корпоративная компьютерная система защиты материальных объектов, контроля и интеллектуального управления торговой сети гипермаркета защищена патентами на изобретения.

АРХИТЕКТУРА СИСТЕМЫ КОНТРОЛЯ ДОСТУПА LPS ЗАЩИЩЕННОЙ ОС BASTION

Д.С. КОЧУРОВ

Unix-подобные ОС с открытым кодом (Linux, FreeBSD и т.д.) с точки зрения безопасности имеют ряд существенных недостатков, которые невозможно преодолеть только грамотным администрированием и настройкой системы.

По этой причине пользователи таких ОС вынуждены применять дополнительные системы защиты, которые в свою очередь либо сложны в настройке и эксплуатации, либо ориентированы на отдельные частные случаи.

Для решения приведенных проблем с организацией защиты и построения защищенной ОС Linux (Bastion) применена система LPS (Linux Protection System), являющаяся разработкой кафедры ЭВМ БГУИР.

LPS имеет модульную структуру, причем каждый модуль реализует свою собственную модель защиты. Окончательное решение о предоставлении доступа или отказе в нем получается как суммарное после обсуждения этого вопроса всеми модулями.

Основа защиты в LPS — мониторинг поведения процессов, в частности, перехода процессов от одного пользователя к другому.

Система LPS разграничивает полномочия администратора системы и администратора безопасности. Администратор системы занимается обеспечением корректности функционирования системы, а администратор безопасности — обеспечением конфиденциальности данных. Такое разделение позволяет разграничивать ответственность и выполнять требование по обязательному присутствию нескольких лиц при принятии ответственных решений.

Такой универсальный подход позволяет защитить не только конфиденциальные данные, но и данные ОС, добавляя дополнительный уровень защиты. Для того чтобы преодолеть механизмы защиты LPS, необходимо получить и права администратора системы и права администратора безопасности, притом, что каждый из них контролирует действие другого.

ОЦЕНКА ПАРАМЕТРОВ СЛОЖНЫХ СИГНАЛОВ С ПОМОЩЬЮ ПРЕОБРАЗОВАНИЯ ГАБОРА В СИСТЕМАХ РАДИОКОНТРОЛЯ

С.Б. САЛОМАТИН, Д.Л. ХОДЫКО

Современные средства радиоконтроля несанкционированных источников передачи информации по радиоканалу внутри здания сталкиваются с необходимостью быстро и точно оценить параметры сложных псевдослучайных сигналов в условиях априорной неопределенности и многолучевого распространения.

Одним из подходов к решению такого рода задач является применение частотно-временных преобразований Габора.

Модель сигнала. Принимаемый сигнал $y(t)$ имеет вид:

$$y(t-\Delta t)=\sum_{i=1}^{M} s_i(t-\tau_i)+n(t),$$

где $s_i(t-\tau_i)$ — i-ый луч радиосигнала $i=1\ldots M$, Δt — задержка суммарного сигнала $y(t)$, $s_i(t-\tau_i)=\xi(t)\,A(t)\,sin[\omega(t-\tau_i)+\psi_i]$, $\xi(t)$ — множитель, определяющий затухание сигнала в среде распространения, $A(t)$ — кодовая огибающая радиосигнала, $\omega=2\pi f$.

Преобразование Габора. Используя преобразование Габора с окном $g(t)$ обрабатываемый сигнал можно представить в следующем виде[1]:

$$y(t)=\sum_{m,n=-\infty}^{\infty} C_{m,n}\,g(t-n)\,exp(j2\pi mt),$$

где $C_{m,n}=D_{m,n}-exp(-\lambda)D_{m,n-1}$ — коэффициенты Габора, m,n — отсчеты по частоте и времени соответственно, $m,n=0..N-1$, λ — параметр, контролирующий эффективную ширину окна.

Алгоритм оценки параметров. Входной сигнал $y(t)$ разбивается на N частей, каждая — длины L. Обработка осуществляется на длине L, с шагом $1/L$, начиная с $1/(2L)$. В процессе

обработки вычисляются коэффициенты $C_{m,n}$. Оценка частоты f производится по параметру m, оценка длительность сигнала $\widehat{T}$ определяется как разность $\Delta n = n_2 - n_1$, где n_1, n_2 начало и конец i-го луча. Оценка задержки $\Delta \widehat{t}$ определяется параметром n. Точность оценки зависит от λ_{opt}, которое является оптимальным для каждого из параметров.

Литература

1. B. Porat, B. Friedlander, Detection of transient signals by the Gabor representation IEEE Trans. Acoust., Speech, signal processing, Vol. 37, No. 2. February 1989.

СТАТИСТИЧЕСКИЙ АНАЛИЗ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

С.Б. САЛОМАТИН

Стеганографические методы защиты объектов используют в качестве скрывающих спектральные и корреляционные широкополосные преобразования данных. При этом возникает задача оценка стойкости стегосистем к обнаружению факта передачи скрываемых сообщений [1].

Для анализа стойкости стеганографических систем удобно использовать статистические методы распознавания образов.

Модель стеганографического процесса. Стегосообщение y представляется в виде аддитивной суммы стегошума n и скрываемых данных x. Стегошум характеризуется вероятностной функцией:

$$v[n] = p(y - x = n),$$

гистограмма стегосообщения может быть вычислена через свертку гистограммы скрываемых данных и вероятностной функции стегошума.

В качестве характеристических функций используются дискретные преобразования Фурье от соответствующих гистограмм и вероятностных функций.

Схема обнаружения. В условиях априори известного метода стеганографических преобразований анализатор строится на основе многомерного Байесовского классификатора, использующего линейную разделяющую функцию.

Дискриминантная функция задается в виде [2]

$$S_{ll'}(\vec{k}) = -\frac{1}{2}\vec{k}^T \Sigma^{-1}\vec{k} - \frac{1}{2}\vec{\mu}^T \Sigma^{-1}\vec{\mu} + (\Sigma^{-1}\vec{\mu})^T \vec{k} - \frac{1}{2} ln|\Sigma|,$$

где Σ^{-1}-общая ковариационная матрица классов l и l', $\vec{\mu}$ — вектор средних значений.

В условиях априорной неопределенности типа стегопреобразования, но в рамках анализа классов с многомерным нормальным распределением, которые отличаются лишь средними значениями, критерий оценки адекватности набора признаков использует понятие расстояния Махаланобиса:

$$\varphi = (\vec{\mu}_l - \vec{\mu}_{l'})^T \Sigma^{-1} (\vec{\mu}_l - \vec{\mu}_{l'}).$$

Для снижения вычислительной сложности алгоритма используется метод выбора "лучшего признака" [3].

Литература

1. Грибунин, Оков И.Н., Туринцев И.В. Цифровая стеганография. М., 2002.
2. Harmsen J.J, Pearlman W.A. Stegaanalysis of additive noise modelable information hiding. Center for ImageProcessing Research, Troy, NY.
3. Верхаген К.,Дейн Р., Грун Ф., Йостен Й., Вербек П. Распознование образов: состояние и перспективы. М., 1985.

О ФОРМИРОВАНИИ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

О.А. КАЧАН, И.В. МИТЯНОВ, В.К. ФИСЕНКО

В общем случае модель нарушителя определяется совокупностью признаков, характеризующих квалификацию C, мотивацию M и ресурсы R нарушителя, представленные в виде множеств (подмножеств).

Элементы множеств C, M и R также могут задаваться в виде подмножеств. Это позволяет сформировать вложенную систему подмножеств признаков и элементов. Достаточность глубины детализации и полноты охвата оценивается экспертным путем.

Множества C, M и R характеризуют различные аспекты процесса НСД. При этом:

C={c_1, c_2, c_3}, где c_1 — способности нарушителя, определяемые уровнем его подготовки; c_2 — степень информированности нарушителя о характеристиках объекта информатизации (ОИ); c_3 — статус нарушителя;

M={m_1, m_2, m_3, m_4}, где m_1 — ошибочные действия; m_2 — любознательность; m_3 — попытка взлома; m_4 — корыстные цели;

$R=\{r_1, r_2, r_3\}$, где r_1 — вариант реализации средств; r_2 — расположение средств; r_3 — функции средств.

Предлагается в одном из подмножеств отразить социально-психологические качества потенциального нарушителя: замкнутость или общительность, воля или нерешительность, авантюризм, прагматизм, карьеризм и др. Это позволит создать гипотетическую модель наиболее опасного нарушителя и выделить так называемую "группу риска".

Синтез моделей проводится с использованием аппарата логики высказываний.

Расширение номенклатуры классифицирующих признаков позволит детализировать модель нарушителя и получить более достоверные оценки вероятного направления, характера и риска возможного несанкционированного доступа.

ЗАДАЧА ИДЕНТИФИКАЦИИ АТАК В СРЕДСТВАХ АУДИТА БЕЗОПАСНОСТИ

Е.П. МАКСИМОВИЧ

В соответствии со стандартом СТБ 34.101.2-2001 (ИСО/МЭК 15408-2) средства аудита безопасности должны обнаруживать возможные нарушения безопасности на основе идентификации определенных правил, знаковых событий; известных сценариев проникновения; несоответствия текущей деятельности пользователя ранее применяемому профилю использования системы. Правила, знаковые события и профили стандартного поведения представляют собой некоторые шаблоны или экспертные правила, каждому из которых соответствуют нечеткое слабо формализуемое множество возможных реализаций. В таких условиях возникает нетривиальная задача идентификации наблюдаемых действий, выраженных в некоторых низкоуровневых сигналах относительно заданных эталонных описаний.

Один из возможных подходов к решению указанной задачи идентификации состоит в использовании распознавания с обучением.

Каждая атака представляется выборкой возможных реализаций, которые образуют один или несколько кластеров близких (в смысле заданной функции) ситуаций. Идентификация ситуации сводится к оценке ее возможной принадлежности одному из полученных кластеров. Если расстояние ситуации до ближайшего кластера меньше заданного порогового значения, то принимается решение о реализации соответствующей атаки. Для определения значения порога можно использовать контрольную выборку. В качестве критерия близости предлагается использовать правило типа "ближайшего соседа" либо близость к эталону кластера, заданному, например, в виде дизъюнктивной нормальной формы.

РАНДОМИЗАЦИОННЫЕ ПРЕОБРАЗОВАНИЯ С АЛФАВИТОМ БОЛЬШОЙ МОЩНОСТИ

В.В. ЗАХАРОВ

Известно, что одним из приемов, разрушающих частотные свойства исходного текста является рандомизация. В процессе рандомизации буквам алфавита исходного текста случайным образом ставятся в соответствие буквы алфавита рандомизированного текста. При этом если мощность алфавита рандомизатора незначительно превышает мощность алфавита исходного текста, то такой шифр может быть легко вскрыт.

Доклад посвящен синтезу и анализу рандомизационных преобразований с большой мощностью алфавита рандомизатора.

Показано, что такие рандомизаторы при мощности алфавита рандомизации $L \to \infty$ обеспечивают бесконечную энтропию криптограммы и, соответственно, полную статистическую независимость криптограммы от исходного текста. При этом возможно получение различной степени приближения к полной статистической независимости исходного и зашифрованного текстов путем использования рандомизатора с ограниченным, достаточно большим полем рандомизации.

Дана численная оценка мощности алфавита рандомизатора, при которой достигается практическая статистическая независимость исходного текста и криптограммы.

Приведена методика синтеза рандомизаторов с большой мощностью алфавита рандомизации на основе кусочно-линейных разрывных функций. Показаны возможные подходы к анализу стойкости таких рандомизаторов.

МЕТОД МНОГОКАНАЛЬНОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ И ЕГО ПРИМЕНЕНИЕ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Ю.В. ВИЛАНСКИЙ

В 1999 году в заявке PCT /BY99/ 00005 был предложен метод преобразования данных, в котором исходный текст преобразуется в два или более выходных потока. Особенностью метода является циклический характер получения составляющих выходных потоков, что позволяет распределять их совокупности, каналам передачи или использовать как дополнительные степени свободы в различных системах. При этом, по крайней мере, один из выходных потоков можно сделать достаточно малым.

Благодаря свойствам предложенного метода появляется возможность создания новых технологий защиты информации.

В докладе рассматривается один из вариантов реализации данного метода на основе функций с переменной длиной образа и некоторые возможные его применения.

Одним из таких применений, является технология для реализации безопасных телекоммуникационных связей между абонентами по открытым каналам (например, Интернет), которая обеспечивает контроль целостности передаваемой информации, идентификацию отправителя и аутентификацию сообщений.

УЯЗВИМОСТИ MICROSOFT INTERNET EXPLORER

А.Л. ГАРЦУЕВ, И.Н. ОБЕРНИХИН, А.В. БОРЗЕНКОВ

Благодаря своей популярности Microsoft Internet Explorer привлекает к себе внимание многочисленных хакеров, а также профессионалов по компьютерной безопасности.

Существует несколько типов уязвимостей, касающихся браузера Internet Explorer.

1. Уязвимости, приводящие к нестабильной работе браузера или его "зависанию".

2. Межсайтовый скриптинг (cros-site scripting). Злонамеренный сайт в интернете может узнать содержимое ваших "cookie"-файлов. Полученная информация может быть использована для выяснения таких личных данных пользователя, как адрес его электронной почты или, например, точных сведений о покупках, совершенных им на каком-либо сайте. Эти уязвимости также позволяют читать и выполнять локальные файлы на системе клиента, то есть те файлы, которые уже находятся (предустановлены) на копьютере.

Существует универсальная уязвимость, связанная с методом showHelp(). Последний патч от Microsoft (6 февраля 2003 г.), который должен был справиться с этой проблемой, все варианты использования не покрывает. Возможности: чтение cookie, чтение произвольных файлов, запуск файлов.

3. Выполнение произвольного кода, загруженного с сервера.

Используя уязвимость с showhelp(), можно запускать программы с параметрами. К примеру вставить в качестве запускаемой программы "mshta.exe" (для работы с активными web-страницами) и передать ей параметр — ссылку на активную html-страницу (name.hta). Эта страница в свою очередь может содержать код vbscript, который имеет права на чтение/запись/запуск любых файлов.

Литература

1. Абашин В.В., Бокун Н.В., Борзенков А.В. Анализ угроз информационной безопасности и путей защиты от них// Известия Белорусской инженерной академии, 2002. Т. 1(13)/2, С. 159–161.

ИСПЫТАНИЯ ПРОГРАММНЫХ ПРОДУКТОВ НА ОТСУТСТВИЕ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ

Е.В. ШИПЕРКО, Л.И. КИРИЛЛОВА

Введение

В последние годы в Республике Беларусь значительно активизировалась работа по созданию системы сертификации в области защиты информации. Это можно объяснить тем, что происходящие в стране процессы существенно затронули организацию системы защиты информации во всех ее сферах – разработки, производства, реализации, эксплуатации средств защиты, подготовки соответствующих кадров. Исследование средств защиты информации (СЗИ), поступающих на рынок Республики Беларусь, затрагивает ряд актуальных проблем. Рынок СЗИ сегодня представлен продукцией, как зарубежных производителей, так и отечественных. Эта продукция должна быть сертифицированной. В докладе рассматриваются общие вопросы сертификации СЗИ и вопросы сертификации программных средств.

Состояние системы сертификации СЗИ

В Республике Беларусь действует Национальная система сертификации, созданная республиканским органом по стандартизации, метрологии и сертификации, и могут действовать созданные другими юридическими лицами системы сертификации продукции по показателям, по которым законодательством Республики Беларусь проведение обязательной сертификации не предусмотрено.

В Национальной системе сертификации проводится как обязательная, так и добровольная сертификация, могут быть созданы системы сертификации по видам продукции и по отдельным требованиям.

Система сертификации продукции имеют свои знаки соответствия.

Система сертификации и знаки соответствия подлежат регистрации в порядке, установленном республиканским органом по стандартизации, метрологии и сертификации.

Участниками обязательной сертификации являются республиканский орган по стандартизации, метрологии и сертификации, органы по сертификации, аккредитованные испытательные лаборатории, изготовители (продавцы) продукции.

До недавнего времени испытания СЗИ в Республике Беларусь проводились специалистами Государственного центра безопасности информации (ГЦБИ) в добровольном порядке, в связи с

отсутствием нормативно-методической базы. ГЦБИ аккредитован Госстандартом Республики Беларусь в качестве органа по сертификации средств и продукции по требованиям безопасности информации (аттестат аккредитации № BY/112 01.1.0.0062 от 15 октября 2000г.). Во взаимодействии с Госстандартом Республики Беларусь ГЦБИ проводит работы по созданию и аккредитации лабораторий, способных проводить сертификационные испытания СЗИ и продукции по требованиям безопасности информации.

Одной из таких лабораторий является лаборатория сертификационных испытаний, организованная на базе УП "Научно-исследовательский институт технической защиты информации". В настоящее время готовится доаккредитация этой лаборатории по следующим направлениям:

сертификационные испытания аппаратно-программных СЗИ от несанкционированного доступа (НСД);

сертификационные испытания на отсутствие компьютерных вирусов и вредоносных программ;

сертификационные испытания программного обеспечения (ПО) СЗИ на отсутствие недекларированных возможностей (НДВ).

В Республике Беларусь сертификационные испытания такого характера не проводились и должного внимания проблема недокументированных возможностей ПО не получила.

Белорусский рынок СЗИ представлен продукцией различных производителей. Многие поставщики СЗИ имеют экспертные заключения на свою продукцию. В основном это СЗИ, поставляемые российскими производителями. Испытания таких СЗИ имеют свои особенности.

В ходе сертификационных испытаний выявляется соответствие/несоответствие /программно-аппаратных СЗИ нормативных актов, конкретных стандартов или других нормативных документов по стандартизации, на территории Республики Беларусь.

Сертификационные испытания аппаратно-программных СЗИ проводятся на специализированных стендах, отвечающих требованиям нормативных документов и стандартов, согласно специальным методикам, утвержденным соответствующими органами.

Результаты испытаний фиксируются экспертами в протоколах, которые являются основанием для принятия сертификационной комиссией решения о присвоении сертифицируемым СЗИ знака соответствия.

Для большинства информационных систем аппаратное обеспечение, системное и прикладное ПО, коммуникационное оборудование и эксплуатационные средства должны быть сконфигурированы воедино и протестированы во время сертификации. Результатом сертификации должна является выдача документа, который устанавливает, соответствует ли система требованиям безопасности, описывает все известные уязвимые места и сообщает все эти сведения лицу или органу, уполномоченному принимать решение об утверждении.

Что дает сертификация СЗИ?

Определенная гарантия качества СЗИ (подтвержденная сертификатом) со стороны государства с точки зрения выполняемых функций по защите. Возможность аттестации информационной системы, в которой используются сертифицированные средства защиты.

Гарантия отсутствия программных закладок, заложенных производителем с целью НСД к защищаемым системам.

Маркетинговый ход, призванный увеличить привлекательность программного продукта и поднять престиж компании-заявителя, а также повысить доверие потребителя к сертифицируемому продукту.

В дальнейшем, говоря об испытаниях ПО на отсутствие НДВ, не будем останавливаться на особенностях механизма сертификации, а более полно опишем методы, используемые при испытаниях ПО СЗИ, поскольку, кроме того, что часто испытывается как законченное изделие, в ряде случаев является составной частью всех комплексов аппаратно-программной защиты информации.

Испытания ПО СЗИ на отсутствие НДВ

Что такое недокументированные (недекларированные) возможности?

Недекларированные возможности - это программа (подпрограмма) или логически законченный набор команд, преднамеренно разработанные и внедренные в ПО с целью реализации функций, выполнение которых потенциально возможно в процессе эксплуатации; в то же время не описано в достаточном для тестирования объеме ни в одном из документов из состава программной документации на ПО (описание программы или пояснительная записка, описание применения программы, исходный текст программы).

Реализацией НДВ, в частности, являются программные закладки.

Программные закладки – преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

Сертификация на отсутствие НДВ (программных закладок) ориентирована на специализированное ПО, предназначенное для защиты информации ограниченного доступа.

На сегодняшний день объем специализированного ПО, достаточно велик. Вопрос защиты информации актуален для организаций любой формы собственности. Потенциальными потребителями специализированного ПО являются как государственные, так и коммерческие структуры.

Сертификационные испытания ПО на отсутствие НДВ не относится пока к числу мероприятий, регулируемых Белорусским государством в интересах информационной безопасности, но с утверждением в системе сертификации Республики Беларусь проекта руководящего документа *"Защита от*

несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" они будут нести обязательный характер.

Сертификационные испытания на отсутствие НДВ предполагают глубокое исследование ПО и связаны с анализом, как исполняемого кода, так и исходного с целью установления факта отсутствия (либо наличия) в некотором программном решении функциональных возможностей, не документированных разработчиком.

Методы испытаний основаны на общих принципах анализа программ с учетом аспектов, связанных с информационной безопасностью. Теоретические и практические работы в данной области известны давно.

При проведении сертификационных испытаний, используются классические методы, применяемые в мировой практике сертификации качества ПО.

В основе проверок лежит возможность четко соотнести исходный и исполняемый код ПО, выявить и устранить избыточность представленного на испытания исходного кода (которая присуща многим проектам, особенно большим по объему и разработанным разными программистами), однозначно определить действия ПО в процессе начальной инсталляции и деинсталляции по отношению к системным областям операционной системы ЭВМ, получить ряд других характеристик ПО.

Метод установления факта наличия или отсутствия в программах недекларированных элементов основан на оценке модели воздействия закладного элемента программы.

Оцениваемая модель предусматривает наличие в программных модулях такого элемента, который до наступления определенного события (выполнения определенного условия) является неактивным (не получает управления), и активизируется (получает управление) после выполнения некоторого условия (события).

Действия, выполняемые активизированным недекларируемым элементом, не предусмотренным функциональным назначением программы, могут быть:

разрушительными, ведущими к нарушению требуемого алгоритма функционирования ПО средств защиты информационных ресурсов;

замедляющими ход вычислительного процесса в информационных системах без нарушения алгоритма функционирования проверяемого ПО;

отвлекающими пользователя (мерцание экрана, пятно на экране и др.) без нарушения нормального хода вычислительного процесса и логики функционирования ПО и др.

Метод установления факта структурно-логического соответствия реальных и декларируемых функциональных возможностей ПО основан на оценке устойчивости функционирования, работоспособности, полноты реализации, логической корректности программ.

Данный метод позволяет без исполнения программы в машинных кодах на ПЭВМ проводить символическое тестирование корректности обработки данных:

анализируются функции программ, записанных в символическом (на языке программирования) виде, связывающих наборы входных переменных программы и выходных переменных, и участвующих в исполнении программы по определенному маршруту;

области определения входных и выходных данных для конкретных маршрутов разбиваются на соответствующие им подобласти;

разрабатываются тесты таким образом, что каждому тесту ставится в соответствие определенный набор входных и выходных переменных с конкретными границами подобластей и указанием реализуемого маршрута;

устанавливается соответствие между областями определения наборов данных (входных и выходных) и маршрутами их обработки в программе.

Обработка программой данных считается корректной, если не обнаружено несоответствия маршрутов и данных.

Результаты испытаний могут быть использованы разработчиком для проведения углубленного анализа своего продукта, планирования и реализации корректирующих воздействий по отношению к ПО в части усовершенствования процессов его разработки и сопровождения.

Несмотря на то, что разработчика ПО, которое позиционируется как средство защиты конфиденциальной информации, никто не заставляет проводить сертификацию на отсутствие НДВ (она добровольна) тем не менее, такую сертификацию стоит проводить.

Предпосылки повышения актуальности испытаний на отсутствие НДВ

Во-первых, существенно вырос уровень возможностей разнообразных СЗИ, что сделало дорогостоящими и малоперспективными мероприятия по взлому систем защиты "в лоб", без знания их принципов построения и функционирования.

Во-вторых, неизмеримо возросла значимость и ценность защищаемой информации разной степени конфиденциальности.

В-третьих, потребитель информации в целом вник в суть проблемы и стал опасаться попыток НСД к своей информации не только со стороны так называемых хакеров, но и со стороны разработчиков ПО, фискальных органов и т.п.

Итак, мы имеем две стороны одной медали:

для получения НСД к информации злоумышленнику гораздо проще воспользоваться заранее подготовленными закладками в ПО;

потребитель хочет иметь гарантии того, что таким способом к его информации доступа нет.

Наличие у производителя или поставщика ПО сертификата, подтверждающего отсутствие в продукции программных закладок, позволяет учитывать последнее обстоятельство вместе с тем, к сертифицированной продукции существенно повышается доверие старых заказчиков, крупных корпоративных потребителей. В нынешних условиях это очень важно.

Технологическая операция по динамическому анализу ПО предусматривает его тестирование. Причем, такое тестирование является углубленным, учитывающим не только функциональные возможности исследуемого ПО, но и его технологические и структурные особенности.

Полезность для разработчика для разработчика такого исследования, выполненного независимой организацией, очевидна.

Кроме того, результаты тестирования могут быть использованы разработчиком при сопровождении своего продукта, а также разработке новых версий или новых программных продуктов.

Следующий важный момент – процесс испытаний на отсутствие НДВ объективно предполагает тесный постоянный контакт испытателя и разработчика, что зачастую позволяет разработчику оперативно улучшать функциональные и потребительские свойства ПО непосредственно в процессе испытаний.

При этом в интересах разработчика испытания могут быть выполнены на его производственной базе.

О потребительских или маркетинговых преимуществах можно сказать следующее:

Государственный документ – сертификат – с определенной степенью вероятности, зависящей от уровня проведенного контроля, подтверждает тот факт, что в проверенном ПО нет явных программных конструкций, использование которых предполагает возможность НСД, нарушения целостности защищаемой информации.

По результатам проведенных испытаний ПО приобретает четкий идентификационный признак – зафиксированные контрольные суммы исходных и исполняемых файлов, позволяющий осуществлять мероприятия по контролю целостности сертифицированного ПО на этапах эго разработки, тиражирования и эксплуатации.

Тот факт, что за доставку к потребителю именно сертифицированного ПО отвечает не только его разработчик, но и проводившая испытания сертификационная лаборатория, которой нормативными документами вменены соответствующие контрольные функции, также имеет немаловажное значение для маркетинга.

Кроме того, рассматриваемый вид испытаний подтверждается соответствующим актом установки именно сертифицированного ПО на объектах конечных пользователей.

Наличие сертификата на отсутствие НДВ является неоспоримым преимуществом для программных решений, претендующих и дальше позиционироваться на государственном рынке СЗИ, поскольку процедура подтверждения и пролонгации действия сертификата, основана на анализе соответствия сертифицированных свойств вновь представляемого на сертификацию продукта по отношению к аналогичным свойствам сертифицированного эталона.

Таким образом, еще раз можно подчеркнуть то, что, используя сертифицированное на отсутствие НДВ в ПО заказчик получает средства, которые с определенной степенью вероятности делают две простые вещи:

корректно и гарантированно выполняют функции по защите его информации;

не имеют встроенных механизмов, позволяющих нанести этой информации вред.

ПРОФИЛЬ ЗАЩИТЫ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ СЕРВЕРА ДЕМИЛИТАРИЗОВАННОЙ ЗОНЫ

А.И. МАТУК, С.Л. ПУГАЧ, Г.Д. ТОМИНА

1. Роль и место "Критериев оценки безопасности информационных технологий" в сфере защиты информационных технологий.

"Критерии оценки безопасности информационных технологий" ("Критерии") регламентируют все стадии разработки и квалификационного анализа продуктов и систем ИТ, отвечающих требованиям информационной безопасности. "Критерии" устанавливают метрики информационной безопасности и являются основой для создания и развития глобальной системы сертификации безопасности продуктов и систем ИТ. Согласно "Критериям" [1], безопасность ИТ может быть достигнута посредством применения предложенной в них технологии разработки и общей схемы сертификации продуктов и систем ИТ.

"Критерии" позволяют использовать множество независимых частных показателей безопасности и ранжировать требования безопасности по частично упорядоченному набору шкал. Отказ от единой шкалы ранжирования требований безопасности позволяет достичь адекватности реализации средств защиты объекта оценки (ОО) принятой политике безопасности организации, что свидетельствует о преобладании "качества" обеспечения защиты над "количеством" и позволяет потребителю не только приспособить требования к своим нуждам, но и оптимизировать выбор средств защиты по критерию качество/стоимость.

"Критерии" определяют множество типовых требований, которые в совокупности с механизмом Профилей защиты позволяют пользователям создавать частные наборы требований, отвечающие их нуждам. Разработчики могут использовать Профиль защиты как основу для создания спецификаций

своих продуктов. Профиль защиты и спецификации средств защиты составляют Задание по обеспечению безопасности, которое используется для оценки конкретных систем и продуктов ИТ.

Квалификация уровня безопасности является методом определения соответствия продукта или системы ИТ запросам потребителя. Запросы определяются в результате анализа рисков и выбранной политики безопасности организации.

Квалификационный анализ может осуществляться как параллельно с разработкой продукта или системы ИТ, так и после ее завершения.

Схема процесса квалификационного анализа включает три стадии [2]:

1. Анализ Профиля защиты на предмет его полноты, непротиворечивости, реализуемости и возможности использования в качестве набора требований для анализируемого продукта.

2. Анализ Задания по обеспечению безопасности на предмет его соответствия требованиям Профиля защиты, а также полноты, непротиворечивости, реализуемости и возможности использования в качестве эталона при анализе продукта или системы ИТ.

3. Анализ продукта или системы ИТ на предмет соответствия Задания по обеспечению безопасности.

Результаты квалификационного анализа влияют на повышение качества работы производителей в процессе проектирования и разработки продуктов и систем ИТ. В продуктах, прошедших проверку на соответствие уровням гарантии, вероятность появления ошибок, недостатков защиты и уязвимостей существенно меньше, чем в продуктах, не прошедших оценку. Применение "Критериев" позволяет упростить и стандартизировать формирование требований, разработку продуктов ИТ, их оценку и сертификацию.

Основными документами, описывающими все аспекты безопасности продуктов и систем ИТ, с точки зрения пользователей и разработчиков являются соответственно Профиль защиты и Задание по обеспечению безопасности.

2. Профиль защиты

Профиль защиты определяет требования безопасности к определенной категории продуктов и систем ИТ, не уточняя методы и средства их реализации.

Профили защиты распространяются на программные, аппаратные и аппаратно-программные средства обеспечения безопасности.

Профиль защиты определяет необходимый перечень функциональных и гарантийных требований безопасности, предъявляемых к продукту или системе ИТ, при обработке информации, представляющей ценность для собственника (в частности, применительно к Профилю защиты ОС сервера для использования в государственных органах управления – при обработке информации ограниченного распространения, не отнесенной к государственным секретам).

Настоящий Профиль защиты применяется к программным средствам безопасности ОС сервера отечественного и импортного производства при их использовании в демилитаризованной зоне.

Положение настоящего Профиля защиты предполагается сделать обязательным для применения расположенными на территории Республики Беларусь заказывающими органами (потребителями продуктов и систем ИТ), разработчиками таких продуктов и систем, и экспертами (испытателями) в качестве руководства при покупке, разработке, применении и оценке защищенных продуктов и систем ИТ в государственных организациях.

3. Особенности ОС сервера демилитаризованной зоны сети как продукта ИТ.

Объектом оценки, исследуемым в Профиле защиты является ОС сервера общего назначения устанавливаемая на компьютеры-сервера демилитаризованной зоны сети (ДМЗ), имеющей выходы во внешние сети передачи данных.

ОО служит платформой для сетевых приложений ДМЗ, поддерживает защищенную передачу через недоверенную внешнюю сеть при обработке информации ограниченного распространения и может включать специализированные пакеты (service packs, add-ons и т.д.) для расширения основных функциональных возможностей. Обеспечение защиты активов ОО и осуществление политики безопасности выполняет Комплекс средств обеспечения безопасности объекта оценки (КСБО), который представляет собой совокупность программных средств защиты, входящих в состав ОО. Все операции аудита производятся компонентами КСБО.

ОО поддерживает выполнение процессов, активируемых субъектами: исполняемым кодом программ сервисов-приложений, порождающих системные процессы, и пользователями. Пользователи и системные процессы учитываются при всех операциях ОО за счет применения механизмов порождения процессов, которые действуют или от имени конкретного пользователя, или от имени уникально опознаваемого системного процесса. Порожденный процесс запрашивает и использует ресурсы от имени уникального идентификатора, связанного с пользователем или системным процессом.

ОО предназначен для использования в сетевой среде и поддерживает протоколы различного уровня (канальные, сетевые, транспортные, прикладные) для обеспечения одного или более типов связи в сетях различных топологий.

ОО обеспечивает:

а) удаленный доступ к внешнему объекту ИТ через недоверенную сеть (т.е. механизмы, функционирующие в этой ОС, взаимодействуют с механизмами в других продуктах ИТ или с другой ОС для безопасного обмена информацией через недоверенную сеть);

б) доступ к внешнему объекту ИТ, функционирующему в среде объекта оценки;

в) разделяемые ресурсы, совместно используемые в сети, такие как сетевой диск, общие папки и т.д.;

г) виртуальный каталог, т.е. именованные точки подключения пользователя к сервисам-приложениям, функционирующим в среде ОО;

д) многопротокольную маршрутизацию для сетевых пакетов;

е) доступ к службе сетевой регистрации, т.е. именованную точку подключения к серверу регистрации;

ж) назначение уникального идентификатора каждому полномочному пользователю;

и) назначение уникального идентификатора каждому системному процессу, включая те, которые не выполняются от имени пользователя (например, процессы, стартовавшие подобно процессу "inetd" в Unix);

к) аутентификацию полномочного пользователя, прежде чем разрешить ему выполнить любые действия, отличные от установленных для открытого доступа набора безопасных операций (например, чтение с общедоступного Web-сайта);

л) проведение аудита для обеспечения подотчетности действий контролируемых пользователей, для обнаружения возможных нарушений политики обеспечения безопасности объекта оценки (ПБО) и реакции на них;

м) управление разрешением на доступ, т.е. инициализация, назначение и изменение прав доступа (например: чтение, запись, выполнение) к объектам, относительно:

1) имени логического объекта или членства в группе;

2) ограничений, накладываемых условиями эксплуатации (например, время суток и точка входа);

н) управление доступом к приложениям, функционирующим в среде ОО, по правилу: запрет или разрешение;

п) управление соединениями к серверам доверенной зоны по правилу: запрет или разрешение;

р) управление распределением ресурсов с целью воспрепятствовать исчерпанию ресурса;

с) обнаружение некоторых опасных состояний;

т) обеспечение надежного восстановления ОО, в случае системных сбоев, обнаружения опасных состояний;

у) поддержка автоматизированной инструкции для оказания помощи при проверке поставки, инсталляции, функционировании и администрировании ОО.

4. Требования безопасности к современным ОС сервера общего назначения для использования в демилитаризованной зоне корпоративной сети

Предполагается, что ОО не содержит явных недостатков и ошибок разработчиков, установлен и сконфигурирован в соответствии с техническими условиями (ТУ) и нормативно-технической документацией. Контроль корректности функционирования и конфигурации КСБО, а также общий контроль за соблюдением мер безопасности на объекте осуществляет администратор безопасности. ОО должен быть расположен в зоне контроля физического доступа. Профиль защиты рассчитан на два типа санкционированного доступа пользователей: открытый доступ и полномочный доступ. Считается, что технические возможности для осуществления попыток обхода КСБО существуют только при открытом доступе со стороны внешней сети, не контролируемой организацией, при открытом доступе со стороны доверенной зоны возможности обхода КСБО существенно снижаются за счет применения комплекса административных и технических мер защиты доверенной зоны.

ОО может применяться для защиты информации в распределенных информационных системах, используемых в коммерческом секторе и государственных органах.

При использовании в государственных органах ОО обеспечивает минимальные требования защиты:

– при обработке информации, представляющей ценность для собственника;

– при обработке информации ограниченного распространения.

При обработке информации ограниченного распространения, доступ к ней может быть разрешен только полномочным пользователям согласно предписанным ролям.

При использовании в коммерческом секторе ОО обеспечивает:

– базовые требования защиты при обработке информации, представляющей ценность для собственника;

– минимальные требования защиты при обработке информации ограниченного распространения. При обработке информации ограниченного распространения, доступ к ней может быть разрешен только полномочным пользователям согласно предписанным ролям.

При применении в государственных органах и коммерческом секторе ОО используется в информационных системах, в которых главную угрозу безопасности доверенной зоне и ДМЗ представляет внешняя сеть, поэтому главная задача КСБО – противостоять угрозе со стороны внешней сети. Угроза ОО со стороны доверенной зоны для обоих применений закрывается программно-техническими средствами защиты внешних объектов ИТ доверенной зоны. При применении в государственных органах угроза со стороны доверенной зоны закрывается дополнительно организационными мерами.

Профиль защиты обеспечивает следующие функциональные возможности:

– поддержку политики принудительного контроля доступа субъектов к объектам. Политики основаны на идентификации субъекта и разрешают или запрещают действия;

– формирование данных аудита;

– формирование данных, подтверждающих подлинность пользователя;

– просмотр данных аудита;
– ограничения на просмотр данных аудита;
– выборочный просмотр данных аудита;
– избирательный аудит;
– защита журнала данных аудита;
– действия в случае возможной потери данных аудита;
– ограниченное управление доступом;
– управление доступом на основе атрибутов безопасности;
– передача данных пользователя без атрибутов безопасности
– прием данных пользователя без атрибутов безопасности;
– ограниченная защита остаточной информации;
– базовая конфиденциальность обмена данными;
– целостность передаваемых данных;
– обработка отказов аутентификации;
– определение атрибутов пользователя;
– проверка секретов;
– выбор момента времени аутентификации;
– сочетание механизмов аутентификации;
– повторная аутентификация;
– аутентификация с защищенной обратной связью;
– выбор момента времени идентификации;
– связи пользователь-субъект;
– управление режимами работы средств безопасности КСБО;
– управление атрибутами безопасности;
– инициализация атрибутов безопасности;
– управление данными КСБО;
– ограниченный срок действия авторизации;
– роли безопасности;
– тестирование абстрактной машины;
– сбой с сохранением безопасного состояния;
– конфиденциальность передаваемых данных, обеспечиваемая КСБО;
– обнаружение модификации передаваемых данных КСБО;
– автоматическое восстановление;
– обнаружение подмены;
– невозможность нарушения политики безопасности ОО;
– разделение на области КСБО;
– базовая согласованность данных КСБО при взаимных обменах;
– тестирование КСБО;
– максимальные нормы;
– ограничение области применения атрибутов;
– базовое ограничение числа одновременных сеансов;
– блокирование сеанса связи КСБО;
– блокирование сеанса связи пользователем;
– завершение сеанса связи КСБО;
– установленные по умолчанию сообщения о доступе к ОО;
– хронология доступа к ОО;
– открытие сеанса связи с ОО;
– надежный канал передачи данных.

Профиль защиты не обеспечивает:
– поддержку политики контроля доступа, основанную на метках безопасности;
– защиту от преднамеренного злоупотребления полномочными пользователями предоставленными правами доступа;
– приемлемую защиту от сложных атак (например, атаки класса "отказ в обслуживании");
– достаточную защиту от ошибок при инсталляции и конфигурировании ОО и администрировании КСБО.

Уровень гарантии оценки (УГО) для рассматриваемого Профиля защиты выбран как УГО 2 " Структурно тестируемый" в соответствии с СТБ 34.101.3 с необходимыми усилениями (УГО-ДМЗ).

Уровень гарантии ПЗ выбран исходя из следующих соображений:

– УГО-ДМЗ соответствует уровню гарантий поставляемых на рынок серийных ОС серверов;
– затраты на проведение сертификационных испытаний по более высокому уровню гарантии оценки, производимые третьей стороной высоки и нецелесообразны

В то же время меры защиты ОС сервера с гарантиями УГО-ДМЗ достаточны для управления группами пользователей и обеспечивают защиту от простых атак.

Литература

1. СТБ 34.101.1-3 Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. 2001.

2. Common Evaluation Methodology for Information Technology Security. Version 0.6 11.01.97

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ХАОС-ПРЕОБРАЗОВАНИЙ

В.А. ЧЕРДЫНЦЕВ, А.Н. МОЛОСНОВ

Преобразование сообщений на основе нелинейных динамических систем (НДС) обеспечивает относительно высокую степень защиты информации в каналах связи. Рассматривается класс преобразований, использующих нелинейные дифференциальные уравнения и нелинейные отображения. Формулируются условия неискажённого воспроизведения сообщений, оценивается влияние мультипликативных и аддитивных помех на качество обобщённой синхронизации систем.

Даётся классификация методов модуляции хаос-процессов, порождаемых НДС: линейные и нелинейные. Линейные методы основаны на отображениях вида:

$$x_{n+1} = \lambda_n + F(x_n,...,x_{n-k}),$$

где λ_n – сообщение, x_n – преобразованное сообщение, $F(...)$ — нелинейная функция.

Нелинейные методы предполагают модуляцию параметров и начальных условий в отображении:

$$x_{n+1} = F(x_n,...,x_{n-k},\lambda_n)$$

Обсуждаются вопросы синхронизации прямых и обратных преобразователей в присутствии аддитивных и мультипликативных канальных помех. Формулируются условия обеспечения качественной синхронизации и выделения сообщений. Приводятся примеры построения систем передачи данных с хаос-процессами.

Показано, что простейшие НДС (1, 2-го порядков) обеспечивают эффективное хаотическое кодирование и декодирование данных. Приводятся результаты моделирования хаос-преобразователей.

Приводятся примеры построения псевдохаотических генераторов для криптографии, стойкость которых обеспечивается чувствительностью к начальным условиям и вычислительной непредсказуемостью одномерных отображений.

ПРЕОБРАЗОВАНИЕ ДИСКРЕТНЫХ СООБЩЕНИЙ В КАНАЛАХ С ЗАЩИТОЙ ИНФОРМАЦИИ

А.Н. МОЛОСНОВ, Ю.А. ТИХАНОВИЧ, П.В. ЛУЧЕНОК

Рассмотрены системы, описываемые нелинейными отображениями фрактального типа, обеспечивающие прямое и обратное преобразование сообщений в каналах с защитой информации:

$$x_{n+1} = k_1 F(x_n) + y_n$$

$$x_n = k_2 F(x_{n-1})$$

где x_n – преобразованное сообщение, $F(...)$ – нелинейная функция, y_n – сообщение.

Возможны два режима работы системы: генерация хаотических колебаний и нелинейное преобразование сообщения.

Выявлены условия, при которых возникает режим хаотических движений в системе. Показана возможность восстановления сообщений в случае действия аддитивных помех в канале передачи.

Обсуждаются вопросы синхронизации генераторов хаотических колебаний на передающей и приёмной сторонах, влияние канальных помех на качество синхронизации.

За счёт включения линейного фильтра с оптимальными характеристиками на выходе обратного преобразователя снижается вероятность ошибочного воспроизведения информационных символов y_n.

Приведены результаты моделирования системы. Приводятся трёхмерные отображения состояний системы при различных параметрах преобразований.

Показана возможность повышения качества криптозащиты информации за счёт использования комбинационного построения генераторов хаотических последовательностей.

ШИРОКОПОЛОСНАЯ СИСТЕМА СВЯЗИ С ЗАЩИТОЙ ИНФОРМАЦИИ

Д.А. ГОЛОВАЧ, Н.А. ДЕЕВ

Рассмотрена система передачи сообщений, использующая скремблированный ЧМ-сигнал $s(t)$ в качестве скремблирующих последовательностей, обеспечивающих расширение спектра ЧМ-сигнала, используется двоичная $\{\pm 1\}$ случайная последовательность (ДСП) $g(t)$ с тактовой частотой $f(t)$. Последовательностью $g(t)$ осуществляется фазовая манипуляция ЧМ-сигнала. Для обеспечения

энергетической скрытности системы ДСП $g(t)$ формируется как произведение двух двоичных последовательностей: псевдослучайной (ПСП) $g_1(t)$ и случайной $x(t)$, представляющей клиппированный физический шум; полоса спектра которого меньше полосы спектра ПСП $g_1(t)$:

$$s(t) = g_1(t)x(t)\cos[\omega_0 t + \psi(t,\lambda)]$$

Обработка фазоманипулированного сигнала сводится к операции дескремблирования в корреляторе с опорной ПСП $g_1(t)$, фильтрации в полосовом фильтре полученного сигнала $x(t)\cos[\omega_0 t + \psi(t,\lambda)]$, операции свёртки для получения ЧМ-сигнала и, наконец, выделению сообщения в частотном детекторе.

Обсуждаются вопросы помехоустойчивости системы при действии флуктуационных и полосовых помех.

Сравниваются два варианта свёртки сигнала: путём возведения в квадрат, и с помощью схемы с обратной связью по дискретному процессу $x(t)$. Доказывается, что второй вариант обеспечивает более высокое качество воспроизведения сообщения.

ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ, ВЫПОЛНЕННЫЕ МЕТОДОМ ВАКУУМНОГО НАПЫЛЕНИЯ

Е.А. УКРАИНЕЦ, Т.В. БОРБОТЬКО, А.В. ГУСИНСКИЙ, И.А. ВРУБЛЕВСКИЙ

Постоянное совершенствование специальной техники стимулирует появление новых, все более эффективных электромагнитных экранов, в том числе и для защиты от утечки информации по техническим каналам из специальных защищенных помещений, в частности, помещений для обработки шифрованной информации, комнат для ведения конфиденциальных переговоров, камер для настройки и испытаний специальной техники и т.д. А так же используемых для экранирования средств обработки информации для локализации ПЭМИН.

Для создания гибких конструкций электромагнитных экранов весьма перспективной является возможность применения технологии вакуумного напыления тонких пленок на машинно-вязаные основы.

Для изучения экранирующих свойств изготавливались образцы, на которые в натянутом состоянии методом магнетронного распыления наносилось металлическое покрытие из никеля, толщиной 0,1 нм.

После чего из этого полотна формировались конструкции с геометрическими неоднородностями. Одна из них представляла собой гребенчатую структуру с шагом гребня 1 см, вторая – имела поверхность псевдопирамидальной формы.

Экранирующие свойства материалов исследовали с помощью измерителя КСВН панорамного Р2-65, генератора РГ4-14 и индикатора Я2Р-70 в диапазоне частот 27-115 ГГц.

В результате исследований установлено, что использование машинно-вязаных полотен с геометрическими неоднородностями и напыленным никелевым покрытием позволяет уменьшить КСВН более чем в 2,5 раза в отличие от полотен с гладкой поверхностью.

Формирование геометрических неоднородностей на поверхности машинно-вязаных основ позволяет повысить их коэффициент ослабления (до 40 дБ) за счет поглощения ЭМИ в материале полотна (рис.).

Установленные особенности взаимодействия исследованных материалов с электромагнитным излучением позволяют использовать их при изготовлении гибких многослойных конструкций широкополосных экранов ЭМИ.

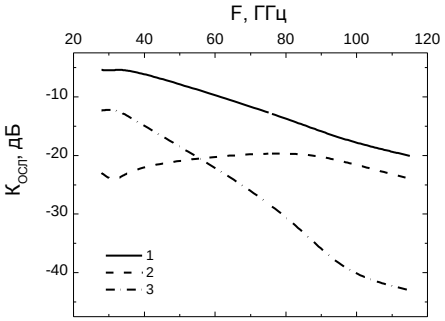

Рисунок. Зависимость коэффициента ослабления машинно-вязаных полотен с напыленным Ni от частоты: 1 — полотно гладкой формы, 2 —

полотно с гребенчатой поверхностью, 3 — полотно с поверхностью псевдопирамидальной формы

ГИБКИЕ КОНСТРУКЦИИ ПОГЛОТИТЕЛЕЙ ДЛЯ ЭЛЕКТРОМАГНИТНОЙ МАСКИРОВКИ НАЗЕМНЫХ ОБЪЕКТОВ

Л.М. ЛЫНЬКОВ, В.Е. ЧЕМБРОВИЧ, Т.В. БОРБОТЬКО

Актуальной проблемой на данном этапе развития науки и техники является снижение радиолокационной заметности наземных объектов.

Исследовались поглотители, выполненные на основе гибких уплотненных волокнистых материалов с жидкостным наполнителем. Для комплексной оценки эффективности поглощающих конструкций проводили их измерения в безэховой камере, что позволяет условия испытаний приблизить к реальным.

Образец № 1 представлял сбой гладкий слой из уплотненного волокнистого материала, на поверхности образца № 2 выполнены геометрические неоднородности псевдопирамидальной формы. Образцы № 3 и № 4 двухслойные: в первом случае поверх слоя уплотненного волокнистого материала закреплен слой машинно-вязаного полотна с рельефной поверхностью в виде мелких углублений, во втором случае использовано нетканое машинно-вязаное полотно с гладкой поверхностью. Образец № 5 аналогичен образцу № 1, но выполнен из нетканой машинно-вязаной основы.

Использовалось следующее измерительное оборудование: генератор Г4-109, приемник измерительный П5-34, позволяющий измерять мощность и отношение уровней мощности слабых гармонических сигналов. В качестве объекта использовалась прямоугольная алюминиевая пластина (цель), размер которой был выбран таким, чтобы длина волны была намного меньше размеров облучаемого объекта. Расстояние до объекта составляло 4 м.

Измерения проводились на частоте 10 ГГц (табл.). Уровни мощности измерялись относительно калибровочного уровня 10^{-12} Вт. Первоначально был измерен уровень отраженного сигнала от цели ($А_ц$), после чего алюминиевая пластина закрывалась исследуемым образцом, и фиксировался уровень отраженного излучения при закрытой цели ($А_{ц+э}$). Расчет дальности обнаружения выполнялся по формуле:

$$r_{обн.ц} / r_{обн.ц+э} = \sqrt[4]{P_ц / P_{ц+э}},$$

Соотношение $P_ц / P_{ц+э}$ вычисляется следующим образом:

$$P_ц / P_{ц+э} = anti\,lg\left(A_ц - A_{ц+э}/10\right),$$

Таблица

№	$А_ц$, дБ	$А_{ц+э}$, дБ	$r_{обн.ц} / r_{обн.ц+э}$
1	47	16	5,6
2	47	26	3,2
3	47	32	2,4
4	47	25	3,6
5	47	22	4,2

Таким образом, наиболее эффективными являются поглотители с малым значением КСВН (1,2-1,3) и коэффициента передачи.

ВЛИЯНИЕ ГЕОМЕТРИЧЕСКИХ НЕОДНОРОДНОСТЕЙ НА ЭЛЕКТРОМАГНИТНЫЕ СВОЙСТВА ЭКРАНОВ И ПОГЛОТИТЕЛЕЙ ЭМИ

В.Е. ЧЕМБРОВИЧ, А.В. ХИЖНЯК, Т.В. БОРБОТЬКО,
Н.В. КОЛБУН, И.С. ТЕРЕХ, В.А. НЕМЦЕВ

Промышленный шпионаж рано или поздно заставляет руководителя предприятия изучить аспекты защиты коммерческой тайны. Темпы развития рыночных отношений в стране превращают вопрос защиты от промышленного шпионажа в сложную проблему, к решению которой руководитель зачастую не готов.

Надежным гарантом защиты конфиденциальной информации может служить защищенное помещение, экранирование которого выполнено из гибких многослойных модульных широкополосных поглощающих материалов с геометрическими неоднородностями и жидкостным наполнителем.

Для исследований были изготовлены 11 образцов поглощающих конструкций из уплотненных волокнистых материалов.

Образцы №1-3 имели многослойную конструкцию: один, два и три слоя соответственно. Поверхность образцов №4-8 содержала геометрические неоднородности псевдопирамидальной формы шириной основания 35, 25, 20, 15, 10 мм. Высота образцов №9-11 составляла 9, 15 и 21 мм.

В качестве измерительного оборудования использовались: панорамного измерителя КСВН Р2-61 и генератора Г4-109. Калибровочным образцом служил слой органического стекла толщиной 3,5 мм. Измерения проводились на частоте 10 ГГц (табл.).

Таблица

№	КСВН	Кпрд, дБ
1	4,4	-14,1
2	4,3	-22,2
3	4,4	-35,4
4	1,9	-18,2
5	2,0	-20,1
6	2,4	-23,8
7	2,7	-26,7
8	2,8	-27,7
9	2,1	-20,1
10	2,0	-23,2
11	1,9	-28,4

С увеличением толщины поглотителя наблюдается уменьшение коэффициента передачи по причине увеличения доли потерь в объеме материала. Коэффициент же отражения образцов №1-3 остается практически постоянным, что объясняется периодическим характером зависимости коэффициента отражения от толщины слоя;

Коэффициент отражения от геометрических неоднородностей существенно ниже, чем от гладкой поверхности вследствие рассеянного отражения. По мере уменьшения размеров неоднородностей отражение приближается к зеркальному, и доля энергии, отраженной в направлении источника, увеличивается;

Увеличение высоты неоднородностей на поверхности уплотненных волокнистых материалов не приводит к существенному изменению коэффициента отражения, но заметно уменьшает коэффициент передачи.

МНОГОКАНАЛЬНАЯ СИСТЕМА ИССЛЕДОВАНИЙ ВИБРОАКУСТИЧЕСКИХ ПОЛЕЙ

И.Г. ДАВЫДОВ

Для исследования виброакустических полей широко применяются многоканальные системы сбора и обработки информации. В работе рассматривается структурное построение четырехканальной системы сбора данных, работающей в реальном масштабе времени. Система поддерживает подключение на четыре независимых канала датчиков в виде микрофонов или акселерометров. Данные, снимаемые в реальном масштабе времени с разрядностью в 16 бит и дискретизацией 44,1 кГц, передаются на компьютер по шине USB. Время накопления данных для последующей обработки ограничено только возможностями объема жесткого диска переносного компьютера.

Система включает в себя четыре независимых аналого-цифровых преобразователя, тактируемых от одного генератора, что обеспечивает одновременный съем информации. Данное решение позволяет применять для обработки ряд алгоритмов анализа, включая корреляционную обработку.

Предусмотрен режим программирования последовательности процесса накопления и обработки информации. Достоинством системы является высокая мобильность. Алгоритм построения позволяет использовать систему в самых широких областях.

МНОГОКРИСТАЛЬНЫЕ МОДУЛИ С ПОВЫШЕННОЙ УСТОЙЧИВОСТЬЮ К ЭЛЕКТРОМАГНИТНЫМ ПОМЕХАМ И ИЗЛУЧЕНИЯМ

В.А. СОКОЛ, В.М. ПАРКУН

Проблема защиты элементной базы от влияния электромагнитных помех (ЭМП) и излучений становится все более острой в связи постоянным ростом степени интеграции больших гибридных интегральных микросхем (БГИМС) и особенно многокристальных модулей (МКМ). При высокой степени интеграции современных интегральных микросхем энергия полезных сигналов устройств становится сравнимой с энергией ЭМП. Кроме того необходимо учитывать непрерывное повышение уровней мощностей (систем нагревания), а также усложнение современных радиопередающих устройств, состоящих из фундаментальных узлов, создающих помехи друг другу.

Потоки ВЧ большой мощности вызывают появление по внешних и внутренних цепях устройств наведенных напряжений и токов, которые могут привести к локальному выделению на некоторых

элементах схемы большого количества тепла и, как следствие, их расплавление (выгорание) и катастрофический отказ.

Помехи меньшей мощности могут вызывать ложные запуски и сбои в схеме, приводить к полному нарушению ее работы.

Существенного снижения воздействия ЭМП ВЧ-диапазона можно добиться различными конструктивно-технологическими методами, и прежде всего подбором высокоэффективного корпуса – экрана из материала с высокой проводимостью, обеспечением его непрерывности и электрогерметичности, рационально организованной системой заземления, позволяющей поддерживать элементы конструкции БГИМС при одном и том же потенциале, равном или близком к потенциалу "земли", и обеспечивать низкоомную нагрузку для опасных токов, которые по тем или иным причинам могут возникать в схеме устройства.

Организация заземления (соединение схемы с общим корпусом) также требует к себе самого пристального внимания, поскольку играет важную роль в уменьшении влияния ЭМП и излучений на нормальное функционирование схемы.

Широкие перспективы при разработке и создании МКМ с повышенной устойчивостью к ЭМП и излучениям открывает электрохимическая алюмооксидная технология (ЭЛАТ), позволяющая на едином технологическом оборудовании с использованием минимальной номенклатуры недорогих материалов изготавливать алюминиевые анодированные подложки (ААП), системы межсоединений высокой степени интеграции, пассивные элементы и корпуса МКМ.

Малый удельный вес, высокие коэффициент теплопроводности, электрические и прочностные свойства ААП наиболее полно удовлетворяют жестким требованиям, предъявляемым к массогабаритным характеристикам и тепловым режимам функционирования схем. Применение ААП при создании МКМ открывает возможность компоновки устройств без дополнительного основания. При этом ААП является одновременно подложкой схемы и основанием корпуса устройства. Герметизация осуществляется крышкой из сплава алюминия, припаиваемой к опорному контуру (рамки), сформированному по периметру подложки.

Для повышения электрической однородности корпуса и обеспечения надежного заземления схемы предложено создавать замкнутый электромагнитный контур между металлическим основанием, рамкой и крышкой корпуса, заземлять схему с помощью проводящих каналов, выполненных в изоляционном оксидном слое подложки.

Проводящие каналы формируются селективным пористым анодированием алюминиевой заготовки одновременно с формированием диэлектрического оксидного слоя на обеих поверхностях заготовки.

При работе микросборки в условиях интенсивного электромагнитного излучения с помощью вертикальных проводящих каналов создается электрический контакт между основанием, рамкой и крышкой корпуса, в результате чего вокруг рабочей части схемы образуется замкнутый электромагнитный контур, исключающий проникновение электромагнитного излучения внутри корпуса и возникновение помех при работе схемы. При этом земляная шина схемы связывается одним из проводников с рамкой, что исключает возникновение "плавающих емкостей" между элементами схемы и корпуса, и как следствие позволяет сохранить быстродействие устройства.

Проведенные испытания опытных образцов МКМ показали, что разработанные конструктивно-технологические методы позволяют в значительной степени повысить устойчивость интегральных схем к воздействию электромагнитных помех и излучений.

СРАВНЕНИЕ КРИСТАЛЛОВ ПЛАСТИКОВЫХ КАРТ ПО СТЕПЕНИ ЗАЩИТЫ ИНФОРМАЦИИ

Д.В. ВЕЧЕР, А.В. ПРИБЫЛЬСКИЙ, В.С. РЕУЦКИЙ, Т.Г. ТАБОЛИЧ

Одной из важнейших характеристик всех видов электронных пластиковых карт (ЭПК) (телефонных, банковских и других) служит степень защиты информации в них от несанкционированного доступа [1]. Процедура несанкционированного доступа злоумышленника к информации в карте обязательно должна включать операцию расшифровки (вскрытия, вычисления) индивидуального ключа карты, аналогичную процедуре аутентификации ЭПК в рабочем модуле безопасности таксофона или банкомата. Сложность процедуры расшифровки определяется сложностью алгоритма шифрования. Для шифрования информации в ключах ЭПК используются симметричные криптосистемы [2, 3], большинство из которых являются национальными или ведомственными стандартами (например, стандарт DES, США, 1975, криптосистемы IDEA, GOST и другие). В свою очередь ключи ЭПК характеризуются своей разрядностью (размером, длиной) – обычно от 40 бит и более.

В таблице [4] проведен сопоставительный анализ времени на расшифровку ключа и затрат на его вскрытие различными категориями злоумышленников, которых в совокупности удобно именовать атакующей стороной.

При этом в таблице обозначено:

ТВК СК — технология восстановления (дешифровки, взлома) ключа симметричной криптосистемы, (ASIC или FPGA),

ASIC — технология с использованием интегральных схем для конкретных приложений,

FPGA — технология с использованием программируемых пользователем логических матриц,

"надежный" ключ — ключ, на расшифровку которого злоумышленникам понадобится 1,5 года и более.

Из таблицы следует, что чем больше разрядность ключа, тем сложнее расшифровать содержащуюся в ключе информацию, и тем выше степень защиты информации в ЭПК. С другой стороны, при увеличении разрядности ключа возрастает сложность ЭПК и, соответственно, ее себестоимость.

Сопоставительный анализ времени на расшифровку ключа ЭПК и затрат на его вскрытие

Атакующая сторона	Затраты, тысяч USD	ТВК СК	Время расшифровки		Длина "надежного" ключа, бит
			Ключ 40 бит	Ключ 56 бит	
Хакер (индивидуальный злоумышленник)			Неделя	бесконечно	45
Малый бизнес	0,4	FPGA	5 часов	38 лет	50
	10	ASIC	12 минут	556 дней	55
Отдел корпорации	300	FPGA	24 секунды	19 дней	60
	300	ASIC	18 секунд	3 часа	60
Крупная компания	10 000	FPGA	7 секунд	13 часов	70
	10 000	ASIC	0,005 секунды	6 минут	70
Федеральное агентство	300 000	ASIC	0,0002 секунды	12 секунд	75

В подразделении НИРУП "ЦНИИТУ", занимающемся разработкой и производством ЭПК, было проведено сравнение по степени защиты информации различных кристаллов, используемых в ЭПК. Установлено, что в телефонном кристалле 4406 защита информации от несанкционированного доступа отсутствует, а в кристалле 4436 имеется ключ длиной 48 бит. Согласно [4] для расшифровки 56-битовых ключей с помощью суперкомпьютера Cray T3D (стоимость такого компьютера в 2000 году составляла 30 млн. долларов) понадобится 453 дня. В то же время длина ключа в телефонной и банковской ЭПК разработки НИРУП "ЦНИИТУ" составляет 256 бит. Это говорит о высокой степени защищенности информации в ЭПК разработки НИРУП "ЦНИИТУ", что в свою очередь свидетельствует о соответствии этих карточек по показателю безопасности информации в них современному научно-техническому уровню и современным тенденциям развития научно-технического прогресса в РБ и за рубежом.

Литература

1. Прибыльский А.В., Таболич Т.Г. Основные направления защиты информации на промышленных предприятиях // В этом сборнике. С.
2. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. Мн. 1999.
3. Харин Ю.С., Агиевич В.С. Компьютерный практикум по математическим методам защиты информации. Мн. 2001.
4. Калинцев Ю.К. Обеспечение безопасности информации в современных сетях связи//Электросвязь. 2000. N 12. С. 6–8.

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОИЗВОДСТВЕ И ЭКСПЛУАТАЦИИ ТЕЛЕФОННОЙ ЭПК

В.С. РЕУЦКИЙ, Д.В. ВЕЧЕР, А.В. ПРИБЫЛЬСКИЙ

Основные элементы действующей системы обеспечения информационной безопасности телефонной электронной пластиковой карты (ЭПК) НИРУП "ЦНИИТУ" — это криптозащищенная предоплаченная таксофонная карта и модуль безопасности (МБ). Карта изготавливается на основе кристалла российского производства, разработанного в ОАО "Ангстрем" в 1998 году и известного под маркой "Tay-98". Разработчики кристалла учли и устранили ошибки, допущенные при проектировании наиболее близкого аналога 4436 [1, 2].

ЭПК имеет достаточно большой потенциальный ресурс (до 29 тысяч тарифных единиц) и функцию защиты от прерванной записи. Каждая карта имеет индивидуальный ключ карты длиной 256 бит, зашифрованный по ГОСТ 28147-89 и хранящийся в области памяти, закрытой для чтения. Карта является автономным компонентом системы безналичных расчетов и может использоваться как самостоятельное платежное средство. Однако из-за жесткой логики работы ЭПК гарантировать высокую защищенности информации в ней нельзя.

Поэтому в качестве второго компонента системы предлагается использовать освоенный в производстве в НИРУП "ЦНИИТУ" модуль безопасности. Этот МБ представляет собой 8-разрядный микроконтроллер с RISK архитектурой, внутренней операционной системой и протоколом обмена T=0 по ISO 7816-3. Конструктивно МБ выполнен под разъем "PLUG IN" по GSM 11.11 и предназначен для установки в таксофон. В МБ могут храниться одновременно до 16 ключей, которые недоступны для

чтения, модификации или удаления. Основное назначение МБ в системе - аутентификация (удостоверение подлинности) кристалла на всех этапах производства и эксплуатации ЭПК. Ключи с течением времени могут сменяться, в том числе дистанционно, или одновременно могут действовать несколько ключей.

Важным элементом, обеспечивающим безопасность системы, является бесполезность такого занятия, как получение информации о ключах посредством логического анализатора — информация при очередном сеансе связи повторяться не будет и логику смены данных проследить невозможно.

Система организована так, что защита транспортного пути кристалла может производиться на ключах, которые не используются в системе. Таким образом изготовитель кристаллов не имеет возможности получить информацию о рабочих ключах. Смена транспортных ключей производится на каждой партии, и поэтому вероятная утечка ключевой информации не приведет к взлому системы.

Хищение МБ из таксофона или вместе с таксофоном также не позволяет взломать систему в целом из-за недоступности ключевой информации. Для защиты от имитации ЭПК, кроме традиционных методов в системе предусмотрена модификация индивидуального кода карты после каждого сеанса связи.

Для повышения стойкости системы к взлому в ней используются МБ с различными ключами на этапах изготовления и эксплуатации ЭПК. При изготовлении кристалла изготовителю передается МБ с транспортными ключами А1-А16. Изготовитель использует эти ключи для записи в кристалл зашифрованного транспортного кода и для создания транспортной карты, содержащей опять таки зашифрованный транспортный ключ. При этом для каждой партии кристаллов используются один из ключей А, а по истечении определенного времени может быть произведена полная замена ключей. Прочитать исходные ключи А в открытом виде и получить информацию о рабочих ключах Б изготовитель кристаллов не может.

После изготовления ЭПК транспортная карта и МБ с ключами Аi используются для входа в режим персонализации карты. Войти в этот режим можно только в случае, если зашифрованные транспортные ключи в кристалле и транспортной карте будут успешно расшифрованы и опознаны МБ с ключами А. Непосредственно для персонализации используется МБ с рабочими ключами Бi, которые также должны содержать МБ, установленные в таксофонах. По окончании персонализации транспортный ключ из карты удаляется, но в закрытую для чтения область памяти записывается индивидуальный ключ карты (ИКК) длиной 256 бит, зашифрованный на рабочем ключе Бi. Изготовителю таксофонов передается МБ с рабочими ключами Б1-Б16, также недоступными для чтения, модификации и удаления. При этом ему неизвестны транспортные ключи.

В настоящее время в системе используется лишь малая часть возможностей, предоставляемых МБ. Поэтому в случае внедрения система имеет дальнейшие перспективы развития, например в части шифрации информационного обмена между таксофоном и АТС, защиты от несанкционированного подключения к линиям связи и т.д.

Система в целом может использоваться и для других применений, где требуется использование предварительно оплаченного кредита. В настоящее время все компоненты системы освоены в серийном производстве в НИРУП "ЦНИИТУ" Научно-производственного объединения "Центрсистем" и прошли эксплуатационные испытания на телефонной сети Республики Беларусь. Результаты позволяют говорить о высокой степени защищенности и хорошем качестве ЭПК.

Литература

1. J. Glave. Pirate Cash in on Weak Chips // Wired News. 1998. N 218 (May).
2. Deutsche Telecom hit by Eurochip reload fraud //User Guide 99. P. 57.

СИНТЕЗ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А.А. ШАМШУР

В настоящее время генераторы случайных чисел получили широкое распространение благодаря применению в различного рода устройствах для защиты информации от несанкционированного доступа, в средствах встроенного самотестирования и т.д. Рост мобильности устройств выдвигает новые требования ко всем узлам, в том числе и к генератору случайных чисел. Основным требованием в мобильном устройстве является энергопотребление, поэтому на сегодняшний день актуальна проблема построения генератора случайных чисел с наименьшим энергопотреблением.

Известно несколько подходов к решению проблемы энергопотребления: изменение схемы устройства, исключение лишних узлов и т.д.; уменьшение частоты работы, что приводит, однако, к уменьшению производительности; изменение структуры блока.

В данной работе рассматривается внесение структурных изменений в широко распространенную схему генератора псевдослучайных последовательностей на основе сдвигового регистра с линейной обратной связью, известного в англоязычной литераторе как Linear Feedback Shift Register (LFSR). Весь регистр делится на две части, работающие на разных частотах, причем на самой большой частоте — частоте появления наборов на выходе схемы, работает только оконечная часть схемы, вся остальная часть работает на меньших частотах, за счет чего и достигается уменьшение энергопотребления.

Для генерирования выходной псевдослучайной последовательности высокой частоты используется несколько сдвигов одной и той же псевдослучайной последовательности меньшей частоты. После сложения двух последовательностей при помощи сумматора по модулю два, получается так же псевдослучайная последовательность, но уже большей частоты.

В работе излагается принцип построения генераторов псевдослучайных чисел, основанных на свойстве сложения псевдослучайных последовательностей со сдвигом по фазе. В результате были получены данные, характеризующие выигрыш в энергопотреблении в сравнении с классическими структурами.

Данный метод позволяет синтезировать менее энергоемкие генераторы без существенного увеличения аппаратных затрат, увеличивается только количество сумматоров по модулю два.

СТОЙКОСТЬ ЭЛЕКТРОННОГО ОБОРУДОВАНИЯ К ВОЗДЕЙСТВИЮ ЭЛЕКТРОМАГНИТНЫХ ИМПУЛЬСОВ

Л.М. ЛЫНЬКОВ, Г.И. ВЛАСОВА

Воздействие электромагнитного импульса, генерируемого при ядерных испытаниях, может привести к необратимому повреждению широкого спектра электрического и электронного оборудования, в особенности компьютеров и радио или радарных приемников, другого телекоммуникационного оборудования, а также вводимая в мире практика использования электронных бомб в экстремальных (военных) ситуациях для подавления информационных инфраструктур.

Основой технологической базы обычных (неядерных) электромагнитных бомб являются генераторы со сжатием потока с помощью взрывчатки, которые представляют собой устройство в компактной упаковке и производят электрическую энергию порядка десятков МДЖ.

Поражающее действие заключается в поглощении энергии через антенные комплексы ("парадный вход"), генерации больших переходных токов ("задний вход") на электрических кабелях или проводниках. Микроволновое оружие, функционирующее в сантиметровом и миллиметровом диапазонах, имеет дополнительный механизм проникновения энергии в оборудование через вентиляционные отверстия, щели между панелями и недостаточно экранированными интерфейсами.

Нацеливание электромагнитных бомб осуществляется методами обычной и технической разведки. Поскольку излучения от компьютерных мониторов, периферии, процессоров, источников питания различны по частоте и модуляции требуется соответствующая система пеленгации таких источников.

Основные методы обороны против электромагнитных бомб состоит в необходимости помещения оборудования в специальные электропроводящие клетки. Весьма существенным следует учитывать "мерцающие" неисправности, возникающие в полупроводниковых приборах, которые сложно диагностируются и ремонтируются.

Коммуникационные сети должны применять топологию с достаточной избыточностью и механизмами ликвидации сбоев, что не позволит пользователю электромагнитного вооружения вывести из строя данную сеть одной атакой.

Ограничения по применению электромагнитных систем вооружений:

- повышенная устойчивость лампового оборудования;
- трудности оценки повреждаемости субъектов из-за возможного затухания электромагнитного сигнала в атмосфере;
- возможность повреждения собственных электронных средств.

Представляется проблемным утверждение разработчиков электромагнитного оружия о "гуманном" воздействии на живые организмы, ведь может повреждаться сетчатка глаз человека, нарушаться излучения электромагнитных полей мозгом.

Для эффективной защиты человеческого организма от возможного контактирования с локальным импульсным электромагнитным воздействием необходима разработка специальных укрывных материалов, применяемых как средства индивидуальной защиты, так и средства для строительства, поглощающие электромагнитные поля.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИХ СИСТЕМ ПОЧТОВОЙ СВЯЗИ

С.В. ЖДАНОВИЧ, Т.Г. КОВАЛЕНКО

Основными направлениями деятельности по вопросам информационной безопасности информационно-технологических систем почтовой связи являются:

проведение научно-исследовательских работ и разработка нормативных и правовых документов в области информационной безопасности в сфере почтовых технологий;

подготовка технико-экономических обоснований по выбору, созданию, внедрению и развитию средств и систем информационной безопасности на предприятия почтовой связи;

разработка стандартов, технических требований в области безопасности для почтовой связи с учетом международных рекомендаций и стандартов;

разработка методов по совершенствованию деятельности предприятий почтовой связи в области информационной безопасности;

разработка программных продуктов по организации и осуществлению информационной безопасности для информационно-технологической сети почтовой связи и автоматизированных систем обработки информации;

проектирование и внедрение систем информационной безопасности на предприятиях почтовой связи;

организация технической учебы, повышения квалификации сотрудников предприятий почтовой связи в области информационной безопасности.

ВЫБОР КОДА ДЛЯ СИСТЕМЫ СВЯЗИ, ОБЕСПЕЧИВАЮЩЕЙ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

А.И. МИТЮХИН

Одним из требований, предъявляемых к современным системам связи является способность противостоять подслушиванию и преднамеренным помехам. Во избежание обнаружения кодированного сигнала несущего сообщение, передача в такой системе ведется с минимальным излучением мощности. Кодирование реализуется посредством использования кодов большой мощности $M=q^k$, где q и k основание и размерность кода соответственно. При этом период сигнала $T=n/f_т$ должен быть соизмерим со временем между сменами кодов ($f_т$ – тактовая частота в системе, n – значность кода).

Обнаруживающая способность подслушивающей стороны ограничивается отношением Q энергии $E_в$ (приходящейся на один бит сообщения) перехваченного сигнала к спектральной плотности мощности шума N_o. Возникает задача выбора класса кодов, определения его мощности, других его параметров, обеспечивающих минимальную вероятность ошибки декодирования $P_{ош}$ в основном канале при заданном минимальном отношении $Q=E_в/N_o$.

Пусть {G} является [n, k]-кодом над полем из q элементов. В системе используется M кодовых слов кода G. Для удобства назовем совокупность M действительных векторов $X=(x_1...x_n)$ множеством сигналов

$G=\{x^1,x^2,...,x^S,...,x^M\}$, $S\in\{1,2,...,M\}$.

Оптимальная процедура декодирования M сигналов на основе стратегии максимального правдоподобия заключается в нахождении номера S одного из M корреляторов с максимальным по абсолютной величине выходным сигналом. Декодирование сводится к сравнению входного вектора $Y=(x+E)$ с каждым словом кода G, где $Y=(y_0y_1...y_i...y_{n-1})$; $X=(x_0x_1...x_i...x_{n-1})$, $X\in G$; $E=(e_0e_1...e_i...e_{n-1})$ – вектор ошибок; $y_i,x_i,e_i\in\{0,1\}$. При условии, что все кодовые слова равновероятны, вектор Y декодируется в ближайшее по расстоянию Хэмминга кодовое слово. Это равносильно определению номера i, для которого вычисляется значение

$|F_i| = G\cdot Y^T$, для $i\in\{1,2,...,M\}$,

где $F_i=(f_0f_1...f_i...f_{n-1})^T$; G – матрица кодовых слов кода.

Если взаимное влияние сигналов отсутствует, то на величину вероятности ошибки декодирования $P_{ош}$ кодового слова X^S влияет только отношение сигнал/шум Q. Для того, чтобы в системе не было взаимного влияния сигналов должно выполняться условие

$R_{X^jX^S}(\tau)=0$ при всех $j\neq S$; $j, S\in\{1,2,...,M\}$.

Здесь $R_{X^jX^S}(\tau)=n-2wt(x^j+Д^\tau x^S)$, (1)

для $0\le\tau\le n-1$ — взаимная корреляционная функция; Д — оператор циклического сдвига последовательности X на одну позицию влево.

С точки зрения получения минимальной величины $P_{ош}$ или помехоустойчивого декодирования (приема в условиях воздействия организованных помех), множество сигналов {G} необходимо характеризовать коэффициентами ВКФ (1). Таким образом, оценка $P_{ош}$ для выбранного кода будет зависеть не только исключительно от отношения ($E_в/N_o$), но и корреляционной матрицы кодированных сигналов.

Рассмотрим, как можно осуществить реальный выбор кода для скрытной передачи информации. Будем исходить из того, что обнаружение подслушивателем передачи состоит в некогерентном накоплении энергии сигналов за период кодированных сообщений. В системе предусмотрена частая смена кодовых слов кода, затрудняющая правильное декодирование подслушивающей стороне. Такая тактика применения кодов требует тщательного анализа ВКФ больших множеств слов.

Известно, что большой совокупностью множеств слов кода G обладает двоичный симплексный $[2^k, k]$-код. К его достоинствам можно также отнести простоту формирования и относительно несложное декодирование. Недостатком симплексных кодов и их производных (Голда, Касами, ЛРД и др.) является сравнительно малое множество слов с хорошими взаимно-корреляционными свойствами. В качестве примера приведем М-код длиной 31. Всего существует 6 различных проверочных полиномов h(x) над полем GF(2) длиной 31. Полиномы h(x) запишем в восьмеричном представлении, в виде коэффициентов многочленов и в виде многочленов (см. табл.).

Примитивные многочлены степени 5

$h_1(x)$	45	100101	x^5+x^2+1
$h_2(x)$	75	111101	$x^5+x^4+x^3+x^2+1$
$h_3(x)$	67	110111	$x^5+x^4+x^2+x+1$
$h_4(x)$	51	101001	x^5+x^3+1

$h_5(x)$	57	101111	$x^5+x^3+x^2+x+1$
$h_6(x)$	73	111011	$x^5+x^4+x^3+x+1$

Выбор множеств пар М-кодов, кодовые слова которых обладают только определенными значениями ВКФ, основывается на следующем утверждении [1]. При всех $k \neq 0 \bmod 4$ существуют пары М-кодов с ВКФ, принимающими трехуровневые значения:

(-1), t(k), t(k)-2, (2)

где $t(k)=1+2^{\lceil (k+2)/2 \rceil}$, $\lceil \alpha \rceil$ — обозначает наибольшее целое число меньшее или равное α.

Пары примитивных многочленов, порождающие пары М-кодов с ВКФ, принимающими значения (2) образуют пары предпочтительных М-кодов. Для рассматриваемой системы связи важны не пары, а множества кодов с хорошими взаимно-корреляционными свойствами, в которых любая входящая в нее пара предпочтительна. Для приведенного выше примера М-кода значности 31 можно построить 8 различных множеств, в каждом из которых по 3 пары предпочтительных М-кодов. Распределение полиномов h(x) в множествах предпочтительных пар М-кодов выглядит так:

$M_3^1=\{h_1(x), h_2(x), h_6(x)\}$;
$M_3^2=\{h_1(x), h_2(x), h_3(x)\}$;
$M_3^3=\{h_1(x), h_3(x), h_5(x)\}$;
$M_3^4=\{h_1(x), h_5(x), h_6(x)\}$;
$M_3^5=\{h_2(x), h_4(x), h_6(x)\}$;
$M_3^6=\{h_2(x), h_3(x), h_4(x)\}$;
$M_3^7=\{h_3(x), h_4(x), h_5(x)\}$;
$M_3^8=\{h_4(x), h_5(x), h_6(x)\}$;

Заметим, что каждый предпочтительный многочлен h(x) входит в четыре из восьми множеств. Абсолютное максимальное значение коэффициента корреляции между всеми кодовыми словами каждого множества пар предпочтительных М-кодов M_3^i (j=1...8) равно (2)

$t(5)=1+2^{\lceil (5+2)/2 \rceil}=9$.

Относительное максимальное значение выбросов ВКФ не превышает величины 9/31 = 0,29. Выбранное для передачи множество M_3^i содержит $3\cdot(2^5-1)=93$ кодовых слов длиной 31. Если в системе предусматривается смена используемых множеств предпочтительных пар М-кодов, то количество применяемых слов для кодирования сообщений достигает величины

$M=8M_3^i = 8\cdot 93=744$.

Как видно, даже для малой длины кода можно построить сравнительно большое множество кодовых слов, удовлетворяющее основным требованиям скрытой системы: обеспечение заданной $P_{ош}$ декодирования для всех кодовых слов кода мощностью М.

Если переходить к большим значностям кода (n>100), когда число пар предпочтительных полиномов симплексного кода (его модификацией) увеличивается вместе с увеличением совокупности множеств M_r^j, эффективность защиты от подслушивания будет также расти. При низких отношениях Q и больших М для обнаружения слабых сигналов подслушивающей стороне потребуются значительные временные затраты во многих случаях несоизмеримые с реальным временем передачи информации по основному каналу.

Литература

1.Сарвате Д.В., Персли М.Б. Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей. ТИИЭР. 1980. Т. 68. № 5.

СОХРАНЕНИЕ КОРПОРАТИВНЫХ ДАННЫХ С ПОМОЩЬЮ СИСТЕМЫ АВТОМАТИЧЕСКОГО РЕЗЕРВНОГО КОПИРОВАНИЯ

Д.С. ПРИЩЕПА

Работа любой организации немыслима без создания надежной и удобной информационной системы, в которой должны находиться все корпоративные данные. При этом остро встает вопрос сохранности этих данных, так как их потеря может привести к остановке работы всего предприятия. Одним из самых надежных путей решения данной проблемы является резервное копирование.

Современные корпоративные СУБД представляют подобные сервисы [1, 2], однако доступ к такому инструментарию имеет лишь администратор СУБД, что приводит к усложнению процесса. Возможно также использование файлового копирования, предоставляемого сервисами ОС, но в таком случае требуется предоставить пользователю сведения об архитектуре распределенной БД, что является грубым нарушением политики безопасности. В данной работе реализован внешний по отношению к СУБД сервис, основанный на механизмах аутентификации, используемых для доступа к корпоративным данным. За основу взята технология DataSnap компании Borland Software Corp [3].

Разработанная система состоит из трех частей: сервер расписания, сервер копирования и клиентское приложение. Первый является дополнительным сервисом бизнес-уровня корпоративной сети и представляет собой DCOM-сервер, реализованный в виде службы NT. Сервер расписания выполняет следующие функции: посредничество между СУБД и пользователем (в том числе аутентификация), поддержка расписания (добавление, редактирование и удаление заданий), обработка таймера и запуск сервера копирования по появлению события задания. Сервер копирования является COM-сервером и

выполняет копирование и восстановление данных. Клиентское приложение предоставляет интерфейс пользователя.

Данная система позволяет осуществлять копирование и восстановление данных с помощью заданий, которые могут выполняться автоматически по расписанию. Возможны следующие режимы запуска: однократно, ежедневно, еженедельно, ежемесячно и ежегодно. При этом действует политика безопасности СУБД, так как сервера расписания и копирования подключаются к БД, используя учетную запись пользователя. Имеется возможность поддержания одновременно нескольких баз данных.

Литература

Луни К. Oracle 8. Настольная книга администратора. М. 1999.
Бобровски С. Oracle 8. Архитектура. М. 1998.
Елманова Н., Трепалин С., Тенцер А. Delphi 6 и технология COM. СПб. 2002.

СЕКЦИЯ 3. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

ДАТЧИК ОБНАРУЖЕНИЯ УТЕЧЕК ИНФОРМАЦИИ В КАНАЛЕ ОТКРЫТОЙ ЛАЗЕРНОЙ СИСТЕМЫ СВЯЗИ

К.В. МЕЛЬНИКОВ

Разработан датчик (широкополосное фотоприемное устройство с высокой чувствительностью) с параметрами, позволяющими использовать его в качестве устройства, обнаруживающего утечку информации в открытых каналах оптической связи.

Фотоприемник обладает чувствительностью порядка 20 нВт и полосой пропускания 25 МГц (35 Мбит/с) и может работать с оптическими излучениями в диапазоне длин волн 850–1570 нм.

В качестве оптоэлектрического преобразователя использован арсенидогаллиевый лавинный фотодиод фирмы *EG&G* типа C30662E с диаметром фоточувствительной площадки 200 мкм. Для повышения стабильности характеристик применена температурная стабилизация фотодиода на уровне +15˚C.

Устройство включает в себя входной каскад, каскад с регулируемым усилением (±40 dB), детектор уровня шумов, компаратор, выходной формирователь и схему термостабилизации.

Измерения проводились сравнительным методом. В качестве источника сигнала использовался лазерный диод фирмы *Siemens* SFH495P с рабочей длиной волны 980 нм. В качестве эталонных приемников использовались ФПУ-03Д НИИ *"Полюс"* (г. Москва) на основе германиевого ЛФД и Model 757-02 фирмы *Analog Modules* (США) на основе *InGaAs* PIN-фотодиода диаметром 300 мкм.

Результаты измерений показали уровень чувствительности разработанного устройства в диапазоне 20±5 нВт.

МИКРОВЗРЫВ В ПОРИСТОМ КРЕМНИИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПОПЫТКЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КРЕМНИЕВЫМ ЧИПАМ

А.В. ДОЛБИК, А.А. КОВАЛЕВСКИЙ, В.А. ЛАБУНОВ, С.К. ЛАЗАРУК, Д.Н. УНУЧЕК

С тех пор как появились первые чипы микросхем — появились и люди, взламывающие эти чипы. И точку в соревновании защиты и нападения, по-видимому, поставят не скоро. Учитывая, что подложка большинства микросхем кремниевая, то можно изготовить кремниевые чипы, которые бы саморазрушались при попытке их несанкционированного вскрытия. Недавно обнаруженная взрывная реакция в пленках наноразмерного пористого кремния может быть использована для этого случая, что обеспечит защиту информации, хранимой на чипе [1].

Явление взрыва пористого кремния инициируется механическим, электрическим либо химическим способом [2]. Микровзрыв, наблюдаемый при реакции окисления пористого кремния, обусловливается целым рядом химических реакций.

В связи с этим проведен анализ реакций имеющих место при окислении путём расчёта изобарно-изотермического потенциала ΔG. ΔG является оценочной величиной для расчёта количества теплоты, выделяемой в ходе реакции. Из проведённого расчёта определено, что такими реакциями являются реакции с участием групп силана *SiH*, SiH_2, SiH_3, водорода, кислорода. Также важны разрывы *Si-Si* связей. Хотя не исключены и другие реакции, характеризующиеся отрицательной величиной ΔG.

На основании проведенного анализа разработан технологический маршрут изготовления саморазрушающихся кремниевых чипов, обратная сторона которых покрыта слоем пористого кремния. Показано, что разрушение кремниевого чипа можно вызвать электрической искрой, локальным нагревом либо механическим воздействием.

Управляемый микровзрыв пористого кремния позволяет разработать микросистемы, обладающие принципиально новыми возможностями в плане защиты информации.

Литература

1. D. Kovalev, V.Y. Timoshenko, N. Kunzner, E. Gross,F. Koch, Phys. Rev. Lett. 2001, Vol. 87, p. 68301.
2. F.V. Mikules, J.D. Kirtland, M.J. Sailor, Adv.Mater. 2002, Vol. 14,p. 38.

ОПТИЧЕСКИЕ МЕЖСОЕДИНЕНИЯ КРЕМНИЕВЫХ ЧИПОВ, КАК СПОСОБ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

А.В. ДОЛБИК, В.А. ЛАБУНОВ, С.К. ЛАЗАРУК, Е.Л. ПЕТРОВИЧ, Д.Н. УНУЧЕК

Привычные в прошлом металлические линии связи все чаще обнаруживают свои недостатки в новом столетии. Современные технологии уже исчерпали их возможности в быстродействии, и, кроме

того, электрические соединения являются потенциальными источниками утечки информации. Оптические линии связи обладают рядом преимуществ, из которых особо выделим высокую степень защиты информации, так как оптическая развязка компьютерных чипов надежно предотвращает потери информации, что наряду с высокой помехоустойчивостью, информационной емкостью и возможностью работы с высокой тактовой частотой дает оптическим линиям связи преимущества перед электрическими.

Давняя проблема оптического передатчика, похоже, найдет свое решение в активно исследуемом направлении пористого наноструктурированного кремния. На сегодняшний день для светодиодов на пористом кремнии нами получены следующие параметры: пороговые напряжение и плотность тока при светоизлучении составляют 4 В и 0,02 мА/см² соответственно. Время нарастания светового импульса 2 нс. Частота 200 Мгц. Единственный параметр, не удовлетворяющий требованиям для оптических межсоединений — квантовая эффективность светоизлучения. При необходимых 10 %, получена величина около 1 %. Изготовлен прототип кремниевых оптических межсоединений, демонстрирующий возможность использования фотонов при передаче и приеме информации как внутри кремниевого чипа, так и между соседними кремниевыми кристаллами.

Показаны перспективы использования оптических межсоединений для совершенствования технологий по обработке и защите информации.

ОСОБЕННОСТИ ВЫБОРА СРЕДСТВ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ ИЗ КОМПЬЮТЕРОВ ПО СЕТИ ЭЛЕКТРОПИТАНИЯ

И.М. РУСАК, В.П. ЛУГОВСКИЙ.

Общеизвестно, что работа о защите информации является жизненно необходимостью, поскольку в современных условиях выигрывает тот, кто владеет информацией. В проблеме утечек информации пока еще недостаточно внимания уделялось внешне малоприметному каналу передачи данных через сеть электропитания. Сигналы, попавшие в сеть, могут распространяться на большие расстояния и, учитывая разветвленную структуру сетевых проводников, представляющих в целом двухпроводные, линии связи, могут быть доступны нежелательным пользователям. Спектр наводимых сигналов простирается вплоть до диапазона десятков и сотен мегагерц.

Одним из основных путей предотвращения утечек данных по сети электропитания является применение фильтров. Фильтры для подавления сигналов проводимости разрабатываются из учета работы в диапазоне от 0,15 до 300 МГц. Основным требованием является высокая эффективность работы фильтров в диапазоне от 0,15 до 20 МГц, из-за высоких уровней помех от импульсных блоков питания.

Исходя из этих требований, основное подавление утечек данных производится с помощью дросселей в проводах питания, включенных как синфазно, так и противофазно. Для работы высокочастотной области диапазона (от 10 до 300 МГц) применяют проходные емкости, устанавливаемые на входе и выходе фильтра. Сама конструкция фильтра должна исключать возможность наводки электромагнитного излучения на элементы фильтра. Установку фильтра в устройство рекомендуется осуществлять внутри общего экрана корпуса ПЭВМ. Подобный фильтр применяется, в основном, для подавления кондуктивных сигналов от импульсного блока питания. Для подавления сигналов от модулей ПЭВМ установку фильтров необходимо осуществлять непосредственно около разъемов питания модулей. Роль модулей, как генераторов сигналов с наиболее широкой полосой, накладывает определенные требования на фильтры, устанавливаемые на модулях устройства. Эти фильтры должны подавлять помехи в очень широкой полосе частот (от 10 до 300 МГц). Нижняя граница частоты среза для фильтров определяется конструкцией ПЭВМ, в частности, длиной кабелей питания и интерфейсов. Верхняя граница частоты среза определяется элементной базой, применяемой в ЭВМ. Основное требование-подавление помех в диапазоне от 60 до 300 МГц. Помехи с более низкой частотой могут подавляться фильтрами, установленными в блоках питания устройства.

Подобные фильтры должны быть выполнены с учетом требований на невосприимчивость к внешнему излучению": либо корпус фильтра должен экранировать фильтр, либо установка фильтра и его конструкция (конфигураций сердечника) должна исключать возможность наводки на него внешних помех. При применении фильтров необходимо учитывать падение напряжения на элементах фильтра (дросселей). Построенные таким образом фильтры подавляют сигналы по каналу проводимости и уменьшают вероятность возникновения наводок излучения от проводов питания, что является универсальным методом борьбы одновременно с двумя видами утечек данных.

ИНТЕЛЛЕКТУАЛЬНАЯ ТЕХНОЛОГИЯ И ОБОРУДОВАНИЕ ДЛЯ ЗАЩИТЫ ОТ ПОДДЕЛКИ МАТЕРИАЛЬНЫХ ОБЪЕКТОВ

В.М. КОЛЕШКО, Ю.Д. КАРЯКИН, В.Л. БУРШ

Технология, не имеющая аналогов в мировой практике, предназначена для защиты от подделки, подмены или фальсификации любых материальных объектов в различных областях деятельности человека. Технология и оборудование защищены патентами на изобретение.

Разработанное оборудование позволяет:

- защитить от подделки бумажные документы и занесенную на них информацию (банкноты, акции, облигации, векселя, банковские чеки, банковские гарантии, нотариальные документы, доверенности, завещания, паспорта, визы, удостоверения личности, водительские лицензии, документы на автомобили, таможенные документы, договора, контракты и т.д.);

- защитить от подделки и фальсификации произведения искусства и исторические ценности (картины, скульптуры, музейные экспонаты и т.д.);

- защитить от подделки и фальсификации драгоценности, украшения;

- защитить от подделки и фальсификации товары известных марок, лекарственные и косметические препараты, парфюмерные товары, спиртные напитки, продукты питания;

- защитить от подделки и фальсификации носители информации (магнитные пленки, диски, лазерные оптические диски и др.), что позволяет обеспечить защиту от несанкционированного копирования и несанкционированного использования музыкальных произведений, кинофильмов, компьютерных программ и информационных технологий;

- защитить каналы связи и передачи информации.

Потенциальные покупатели технологии и оборудования:

• полиграфические предприятия, специализирующиеся на производстве банкнот, ценных бумаг, документов,

• бумагопроизводящие предприятия, имеющие лицензию на производство специальных защитных сортов бумаги,

• банки, финансовые компании, криминалистические экспертные компании, подразделения полиции и безопасности, пограничные пункты паспортного и таможенного контроля,

• страховые компании, специализированные экспертные фирмы, ломбарды, нотариальные конторы,

• компании производители аудио- и видеофильмов и программных средств на CD-ROM,

• производители CD-ROM плейеров.

И самое главное данная технология и оборудование должны быть основным инструментом всех фискальных государственных организаций (в частности, налоговой инспекции, финансовой полиции, таможни, Госконтроля, Минфина и др.), что позволит резко сократить коррупцию и количество чиновников в госорганах и повысить благосостояние пенсионеров, студентов и малоимущих.

ВЫСОКОЛИНЕЙНЫЙ ЧИМ-МОДЕМ ДЛЯ ВОСП ТИПОВОГО АНАЛОГОВОГО МНОГОКАНАЛЬНОГО СИГНАЛА

А.А. ПИЛЮШКО

Автором уже было показано [1], что один из возможных путей модернизации корпоративных сетей связи (в частности сетей связи МО РБ) — это поэтапный переход от АСП, работающих по металлическим кабелям связи, к ЦСП, работающим по ВОЛС, с использованием на промежуточном этапе варианта, когда АСП будут работать по ВОЛС при условии наличия специализированных интерфейсов для их взаимного согласования. Ясно, что предложенный постепенный переход от АСП к ЦСП по ВОЛС потребует на первом этапе простых и дешевых методов преобразования типовых аналоговых многоканальных сигналов (ТАМКС) к виду, удобному для передачи по ВОЛС без ухудшения качества связи. Анализ показывает [2], что указанным требованиям наилучшим образом удовлетворяет ЧИМ. Однако, при использовании ЧИМ возникает много вопросов, на которые в известной литературе ответов не дано. В частности, рассматривались ЧИМ-модемы для ВОСП узкополосных и широкополосных одноканальных (ТВ) сигналов. Такие модемы из-за высоких требований к линейности модуляционной характеристики не могут быть использованы для передачи ТАМКС. В [3] приведены наиболее часто употребляемые варианты структурных схем преобразователей напряжения в частоту, лежащие в основе многих конкретных схем. Однако, такие преобразователи по совокупности параметров не удовлетворяют многим предъявляемым к ним требованиям, особенно в случаях, когда от них требуются предельные значения параметров.

В докладе отражены основные результаты работы по имитационному (с использованием САПР *Design Lab 8.0* [4]) и натурному моделированию ЧИМ-модема для ВОСП ТАМКС, рассматривается вариант повышения линейности модуляционной характеристики модулятора путем введения в схему ветви предискажения, построенной на биполярных усилительных звеньях по принципу кусочно-ломаной аппроксимации. Актуальность работы заключается в том, что предлагаемый в ней вариант построения ЧИМ-модема для ВОСП ТАМКС позволит: во-первых, избежать значительных единовременных капитальных вложений в реконструкцию аналоговых сетей связи МО РБ; во-вторых, уже сейчас значительно улучшить целый ряд тактико-технических характеристик сетей и линий связи МО РБ, таких как скрытность передачи информации, защищенность от внешних электромагнитных влияний, уменьшение времени развертывания, более выгодные массогабаритные показатели — и все это при денежно-трудовых затратах, сравнимых с теми, которые необходимы для выполнения традиционных работ по прокладке металлических кабелей связи.

Литература

1. Пилюшко А.А., Кириллов В.И. Состояние и перспективы развития ВОСП на сетях связи МО РБ./ Известия Белорусской инженерной академии, № 1(3)/1, 1997 г.

2. Кириллов В.И. Высокоэффективные системы информационного обмена для ПРТВК/ Мн.: ВШ, 1989 г.

3. Бабаян Р.Р. Быстродействующие преобразователи напряжения в частоту повышенной точности. Измерения, контроль, автоматизация. № 2 (74), 1990 г.
4. Радзевиг В.Д. Система сквозного проектирования электронных устройств *Design Lab 8.0*. Мн.: Солон, 1999 г.

ГЕНЕРАТОР РЕЧЕПОДОБНЫХ АКУСТИЧЕСКИХ ПОМЕХ ДЛЯ ПОДАВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

В.И. ВОРОБЬЕВ, А.Г. ДАВЫДОВ, Б.М. ЛОБАНОВ

Существующие методы создания маскирующих акустических помех (генераторы шумов, громкоговорящая работа радио или ТВ станции) не гарантируют полной защиты от несанкционированного прослушивания речевых сигналов, т.к. характеристики этих помех могут быть предсказаны и отфильтрованы соответствующими средствами. Для подавления акустических и радио каналов утечки информации о переговорах необходимо разработать технические средства создания маскирующих помех с характеристиками, максимально приближёнными к акустическим характеристикам реальных речевых сигналов и со случайным фонетическим содержанием, отражающим однако статистические закономерности естественной речи. Вероятность выделения такого рода случайных речеподобных сигналов очень низка, что обеспечивает высокую степень закрытия каналов утечки информации.

В докладе предложен и исследован алгоритм формирования акустических речеподобных сигналов (РПС), основанный на использовании статистики элементов речи русского языка (фоноабзацев, фраз, синтагм, слов, слогов и фонем) и предварительно созданной базы аллофонов. Обсуждаются структурная схема указанного алгоритма и результаты испытания реализующей его компьютерной модели. Рассмотрены вопросы реализации автономного синтезатора РПС на базе микроконтроллеров фирмы Atmel. Предлагаемое устройство позволяет оперативно изменять аллофонные базы и используемые статистические характеристики элементов речи с целью имитации РПС речи конкретного человека.

МЕТОД УДАЛЕНИЯ ШУМОВ И РЕВЕРБЕРАЦИИ В РЕЧЕВОМ СИГНАЛЕ ДЛЯ СИСТЕМ КОДИРОВАНИЯ

А.В. ШАДЕВСКИЙ

В настоящее время, активное развитие получили системы низкоскоростного кодирования речи. Они позволяют передавать кодированную речь со скоростью от 1 до 4,8 Кбит/с., при незначительной потере качества. Однако эти системы зависят от качества речи поступающей на ее вход. При наличии шума или реверберации качество восстанавливаемой речи значительно падает. Для корректной работы таких систем необходимо выполнить предварительную обработку речевого сигнала с целью устранения шума и реверберации. В последнее время был предложен ряд методов устранения шума, основанных на использовании свойств модуляционного спектра речи. Однако они либо удаляют только определенный вид шума, либо добавляют дополнительные искажения на выходе в случае поступления на вход чистой речи.

В данном докладе, рассмотрен метод, использующий свойства модуляционного спектра речи и позволяющий повысить разборчивость зашумленной речи. Предварительно, речь разбивается на 128 каналов, банком полифазных фильтров. Для повышения разборчивости используется адаптивная фильтрация спектральной огибающей в канале. При этом модуляционные фильтры независимо подстраиваются в каждом канале. Данный метод позволяет адаптировать работу алгоритма под изменяющееся акустическое окружение. Он удаляет реверберацию, а также большинство видов шумов.

Предложенный метод может использоваться для предварительной обработки систем кодирования речи.

БЕЗЭХОВЫЕ ЭКРАНИРОВАННЫЕ GTEM - КАМЕРЫ

О.Ю. КОНДРАХИН

Анализ состояния дел в области защиты информации показывает, что в промышленно развитых странах мира на сегодняшний день уже сформировалась достаточно устойчивая инфраструктура защиты информации в системах обработки и передачи данных. Но тем не менее, наблюдается устойчивая тенденция роста фактов технического шпионажа. Среди всех возможных каналов утечки информации, технические каналы представляют наибольшую опасность. Такое предположение основывается на следующих фактах:

наличие технически грамотных специалистов, знания и навыки которых не востребованы вследствие тяжелого экономического положения;

недостаточного внимания, а чаще всего просто игнорирования проблем безопасности информации;

наличие широко рекламируемых фирмами-производителями аппаратуры для технического шпионажа, которая до недавнего времени была под строгим государственным контролем и информация о достижениях науки в этой области была доступна только узкому кругу специалистов.

Среди многообразия существующих технических каналов утечки защищаемой информации особое место занимает канал утечки информации за счет побочных электромагнитных излучений. Традиционно считается, что перехват побочных электромагнитных излучений весьма трудоемкая задача и на первый взгляд может показаться, что этот канал действительно менее опасен, чем, например, акустический. Однако нельзя не забывать, что в настоящее время практически вся конфиденциальная информация обрабатывается и хранится в электронном виде.

С помощью современной специализированной радиоприемной аппаратуры перехвата, позволяющей осуществлять прием сигналов ниже уровней окружающих электромагнитных помех, информативные сигналы побочных электромагнитных излучений от средств вычислительной техники могут быть приняты и расшифрованы на значительных расстояниях (десятки, сотни метров и более). В этих условиях важной задачей является измерение уровней электромагнитных излучений радиоэлектронных изделий при проведении специальных исследований по требованиям информационной безопасности. Проведение указанных измерений, а также последующий расчет показателей информационной безопасности радиоэлектронных изделий сегодня уже не представляет собой весьма трудоемкий процесс. На смену ручных инженерно-исследовательских работ пришли автоматизированные комплексы такие, как "Навигатор", "Сигурд", "Зарница", "Легенда".

Представленные на отечественном рынке комплексы для проведения специсследований не обеспечивают высокой точности измерений. К сожалению, в настоящее время наблюдаются значительные расхождения в результатах измерений, получаемых измерительными комплексами и ручными измерениями. Причиной этому служат невысокие, как правило, уровни излучаемых информативных сигналов на фоне внешних электромагнитных помех, создаваемых различными работающими в данный момент времени промышленными электроустановками, бытовым электрооборудованием, электромагнитными процессами в атмосфере и космическом пространстве, а также работающими радио- и телевизионными станциями. Это приводит к существенному увеличению трудоемкости и сроков сертификационных испытаний в связи с ручной проверкой всех обнаруженных составляющих или необходимостью проведения радиоизмерений в отдельных диапазонах частот в вечернее и ночное время суток и в выходные дни. По результатам проведенного статистического анализа распределение уровня внешнего фона электромагнитного поля в диапазоне частот 9 кГц - 1000 МГц в дневное время суток в рабочие дни для центра г. Минска, можно сделать вывод, что в диапазоне 9 – 50 кГц уровень внешних ЭМП составляет в среднем от 50 до 70 дБ (мкВ/м). При этом сигнал ПЭМИ от низкочастотных технических средств, например, клавиатуры, частотой 10 кГц и длительностью импульса 50 мкс, создающий напряженность электрического поля 52 дБ (мкВ/м) может быть перехвачен на расстоянии 10 м, а для перехвата 5-й гармоники частотой 50 кГц на расстоянии 10 м достаточно, чтобы ее напряженность поля была не менее 45 дБ (мкВ/м).

Измерительные приемники, анализаторы спектра или автоматизированные комплексы, в отличие от специализированной аппаратуры перехвата, не позволяют обнаружить сигналы с уровнем напряженности поля ниже уровня окружающих электромагнитных помех. Все измерения, как правило, проводятся в два этапа. На первом этапе происходит сканирование частотного диапазона при выключенном тестовом режиме, т.е. анализ шумовой обстановки. На втором - исследуемое техническое средство переводится в тестовый режим и измеряются уровни всех сигналов, превышающих запомненные шумы на заданное значение порога. При этом сложность возникает в распознавании сигналов, несущих информацию, на фоне всех неинформативных и помеховых сигналов.

Вышеперечисленные проблемы, возникающие в процессе специальных исследований в реальных условиях, могут быть разрешены с помощью специальных программно-аппаратных комплексов, состоящих из экранированной безэховой камеры (GTEM-камеры) и комплекта измерительно-регистрирующей аппаратуры. Такая камера представляет собой четырехгранную пирамиду, лежащую на боковой грани. Камера является прямоугольной коаксиальной линией с плоским центральным проводником. В качестве нагрузки линии используется комбинация поглощающего материала с сосредоточенными сопротивлениями. Это позволит измерять побочное электромагнитное излучение различных электронных изделий в широком диапазоне частот в замкнутом экранированном пространстве, аналогично измерениям в свободном пространстве и в условиях защищенных от внешнего воздействия электромагнитных помех. При этом в созданном экранированном объеме отсутствуют многократные отражения, наблюдающиеся в обычных экранированных камерах или помещениях.

В западных странах подобные комплексы на основе GTEM-камеры нашли широкое применение в области испытаний по электромагнитной совместимости, как при измерении излучаемых побочных электромагнитных излучений, так и при испытаниях на устойчивость к внешним электромагнитным полям. Частотный диапазон зарубежных камер, например, GTEM 250, GTEM 500, GTEM 1250 лежит в пределах от 9 кГц до 18 ГГц (каталог “EMC TEST SYSTEMS”, Messelektronik, Berlin).

Республика Беларусь не производила аналогичных испытательных комплексов для проведения измерений уровней электромагнитных излучений по требованиям безопасности информации, что и затрудняло проведение соответствующих измерений. В связи с этим в рамках государственной научно-технической программы "Защита информации" реализуется проект по разработке испытательного комплекса, который позволял бы проводить сертификационные испытания изделий по требованиям

безопасности информации независимо от окружающей электромагнитной обстановки в частотном диапазоне, в данном случае от 9 кГц до 1000 МГц.

В настоящий момент разрабатывается программно-аппаратный комплекс для измерения побочных электромагнитных излучений, состоящий из экранированной безэховой коаксиальной камеры рупорного типа, настроенной на определенный тип колебаний, и комплекта автоматизированной измерительно-регистрирующей аппаратуры для тестирования рабочего объема камеры и проведения радиоизмерений объекта испытаний. Торцевая часть камеры будет выполнена из радиопоглощающего материала, который обеспечивает поглощение электромагнитных волн в широком диапазоне частот. Планируемая эффективность экранирования камеры не менее 60 дБ. При помещении в данную GTEM-камеру испытываемого радиоэлектронного изделия, измеряемое электромагнитное излучение от него будет представлять собой поперечную, так называемую ТЕМ-волну. Конструкция камеры обеспечивает однородность испытательного электромагнитного поля и практическое отсутствие высших типов волн. Комплект измерительно-регистрирующей аппаратуры с помощью разрабатываемого специализированного программного обеспечения позволит автоматически регистрировать и измерять параметры информационных сигналов от испытываемого радиоэлектронного оборудования.

В процессе работы программно-аппаратного комплекса будут использованы два режима:

режим контроля - для оперативного обнаружения излучаемых сигналов по определенным признакам и проведения непрерывного мониторинга электромагнитной обстановки внутри камеры. Для реализации данного режима работы предполагается использование сканирующего приемника типа AR-5000 (или его аналога) с персональным компьютером, с помощью которых осуществляется быстрый поиск, демодуляция, регистрация на жестком диске персонального компьютера частот и признаков обнаруженного сигнала, а также непрерывный контроль за электромагнитной обстановкой внутри камеры с целью обнаружения непостоянно излучающих радиоэлектронных закладок.

режим измерения - для определения физических параметров (напряженности поля, частоты излучения) электромагнитного излучения исследуемых электронных изделий.

Программно-аппаратный комплекс предполагает использование профессионального измерительного селективного приемника либо комбинированного измерительного прибора, совмещающего функции измерительного приемника и анализатора спектра, имеющих метрологические характеристики, соответствующие стандартам на приборы для проведения радиотехнических измерений и методикам для проведения специальных исследований.

В настоящее время в Российской Федерации действуют несколько федеральных системы сертификации средств защиты информации (в рамках Гостехкомиссии РФ, Минобороны и ФСБ). Во всех федеральных системах сертификации действуют или будут дополнительно создаваться испытательные лаборатории (центры). Только в системе сертификации Гостехкомиссии РФ уже имеется более 100 аккредитованных лабораторий (центров) по проведению сертификационных испытаний разнообразных радиоэлектронных изделий и технических средств защиты по требованиям безопасности информации.

Разрабатываемый комплекс помимо проведения сертификационных испытаний изделий по требованиям информационной безопасности может быть использован для оснащения испытательных центров и лабораторий Республики Беларусь, аккредитованных в области испытаний радиоэлектронных изделий народнохозяйственного назначения на соответствие требованиям по индустриальным радиопомехам и устойчивости к внешним электромагнитным излучениям.

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ЖИЗНЕОБЕСПЕЧЕНИЯ ЗДАНИЙ

Н.С. ОБРАЗЦОВ, А.И. ПИНАЕВ

Проблемы защиты информации предполагают определение возможных каналов ее утечки и решение комплекса задач связанных с их блокированием или нейтрализацией. Каналы утечки информации через элементы конструкций зданий, электрические, телефонные и коммуникационные сети хорошо известны и мероприятия по их выявлению и блокированию в достаточной степени проработаны и постоянно совершенствуются.

В то же время в большинстве зданий и сооружений имеются хорошо сконфигурированные каналы утечки информации которым не уделялось и не уделяется достаточного внимания. В первую очередь это касается систем противопожарной сигнализации и автоматики. Особенность этих каналов утечки состоит в том, что их информационные линии проходят через все помещения и зачастую выходят за пределы охраняемых территорий. Это позволяет установить внутри пожарных извещателей устройства считывания информации и производить ее съем в любом доступном месте, кроме того, некоторые типы пожарных извещателей обладают микрофонным эффектом, что обеспечивает прослушивание помещения без дополнительных устройств. Поскольку основная масса систем противопожарной сигнализации и автоматики работает на постоянном токе, это позволяет использовать в качестве считывающих устройств пассивные элементы, которые не обнаруживаются традиционными техническими средствами контроля.

Предлагается комплекс технических и организационных мероприятий, обеспечивающих противодействие возможным каналам утечки такого рода. В плане пассивных технических средств может использоваться постоянно работающие в линиях связи генераторы белого шума или "речеподобных" сигналов, усложняющие аппаратно-программные средства распознавания и воспроизведения речи. Параметры сигналов помехи не должны влиять на нормальное функционирование технических средств. В

более сложных системах необходимо применение анализаторов речевых или высокочастотных сигналов и соответственно устройства формирования соответствующих помех при их наличии. Предлагаются конфигурации структурных схем различных технических средств защиты такого рода.

Рассмотрены системы аналогичного назначения, использующие свои линии передачи данных, которые могут использоваться для несанкционированного съема информации. К такому оборудованию относятся комплексные системы безопасности, включающие системы доступа, охранной сигнализации, управления устройствами жизнеобеспечения зданий и т.п.

Предложен комплекс организационных мероприятий, предполагающих конфигурирование систем подобного назначения и выбор оборудования с учетом возможного несанкционированного доступа к их линиям связи.

СРЕДСТВА ИДЕНТИФИКАЦИИ В СИСТЕМАХ КОНТРОЛЯ И ОГРАНИЧЕНИЯ ДОСТУПА

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

Средства контроля и ограничения доступа все чаще применяются не только автономно, но и в составе комплексных систем безопасности. В сферу их применения попадает не только функции идентификации личности и инструмента подтверждения прав доступа, но и учет рабочего времени персонала, определение местонахождения сотрудников на предприятии и т.п. В качестве устройств идентификации личности в системах контроля доступа основное распространение получили электронные ключи TOUCH MEMORY, пластиковые магнитные карты, пластиковые чип-карты, бесконтактные PROX-карты, системы идентификации на основе интегральных считывателей отпечатков пальцев.

Рассмотрены устройства идентификации с точки зрения долговечности, удобства использования, информативности, скрытности идентификационной информации, стоимости.

Наиболее простыми и дешевыми являются пластиковые магнитные карты, они технологичны, позволяют использовать внешнюю поверхность для нанесения дополнительной информации. К отрицательным характеристикам магнитных карт, можно отнести низкую долговечность, сложность устройств считывания и низкую информативность. Проанализированы технологические особенности этих карт с точки зрения их долговечности и трудоемкости изготовления.

Все большее распространение получают бесконтактные PROX-карты, практически это единственные устройства, позволяющие вести корректную обработку рабочего времени персонала и определение местонахождения сотрудников. Основным недостатком PROX-карты является низкая скрытность идентификационных параметров и возможность простой симуляции кода карты за счет несанкционированного бесконтактного считывания ее кодов. Рассмотрены параметры и условия применения этих карт.

Традиционно распространенными устройствами идентификации являются электронные ключи TOUCH MEMORY. Они обладают высокой надежностью и долговечностью, имеют высокую степень скрытности информации. Их основным недостатком является низкая информативность.

Самым современным средством для широкого применения считаются системы идентификации на основе интегральных считывателей отпечатков пальцев. Несмотря на видимые преимуществами и удобство, по функциональному назначению и области применения они фактически идентичны наиболее простым из серии электронных ключей TOUCH MEMORY. Серьезный недостаток систем на их основе — необходимость сложных и дорогостоящих аппаратно-программных средств обработки информации.

Рассмотрены особенности применения средств идентификации в зависимости от решения конкретных задач, определяемых требованиями к степени контроля и ограничения доступа, характера предприятия, численности персонала, дополнительных функций и т.п.

ПРЕДПРОЦЕССОРНАЯ ОБРАБОТКА СИГНАЛА В УГЛОВОЙ ОБЛАСТИ В МОБИЛЬНЫХ СИСТЕМАХ КОДИРОВАНИЯ РЕЧИ

А.Л. ЛАВРИНЕНКО

В настоящее время существует проблема подавления динамически меняющихся шумовых компонент в системах кодирования речи в средствах связи на автотранспорте. В данной работе предлагается метод подавления компонент, амплитуда которых зависит от угла поворота движущихся элементов автомобиля, например, таких как колеса, вал двигателя, коробка передач. Для обработки этих шумовых компонент требуются методы для перевода сигнала из временной области представления в угловую и обратно.

Для перевода сигнала из временного представления в угловое требуется специальный метод временно-угловых преобразований. Метод должен на основании данных от канала тахометра и канала дискретизации акустического сигнала сформировать сигнал в угловом представлении с минимальными погрешностями. В данной работе предложен метод перехода на основе интерполирующего фильтра в порядковой области. Такой фильтр при изменении частоты вращения оси объекта плавно перестраивает частоту среза в частотной области, в порядковой же области частота среза фильтра является постоянной. Плавная перестройка частоты среза уменьшает шумы и обеспечивает более высокий динамический

диапазон. В угловой области представления сигнала для обработки шумовых компонентов можно использовать методы обработки сигнала применяемые во временной области, например спектральное вычитание.

Исследования алгоритма показали, что метод обеспечивает стабильность амплитуды и положение спектральных линий в угловой и порядковой области вне зависимости от режима работы автомобиля (разгона или торможения). Тем самым обеспечивается точность удаления шумовых составляющих зависящих от скорости.

ИСПОЛЬЗОВАНИЕ ГРУППОВОЙ ИНТЕРВАЛЬНОЙ ГИСТОГРАММЫ В ЗАДАЧАХ КОМПРЕССИИ И КОДИРОВАНИЯ РЕЧИ

Д.С. ЛИХАЧЁВ

В данной работе изложены основные принципы построения вокодерных систем с синусоидальным представлением речи и моделью слуха человека на основе кохлеарной модели и EIH (Ensemble Interval Histogram) — групповой интервальной гистограммы.

Согласно предлагаемому подходу речь, как на вокализованных, так и на невокализованных участках, представляется в виде набора синусоидальных компонент.

В процессе анализа входного речевого сигнала в кодере с помощью модели слуха человека на основе EIH выделяются несколько наиболее "критичных" для слуха человека частотных компонент, для каждой из которых определяется амплитуда, частота и фаза. Для передачи по линии связи найденные в процессе анализа параметры соответствующим образом квантуются и кодируются. Процедура восстановления речи в декодере сводится к синтезу необходимых синусоидальных компонент с принятыми по линии связи параметрами и их суммированию.

Проведённые эксперименты позволяют утверждать, что используя данный подход речевой сигнал с достаточно хорошим качеством можно представить 5–12 синусоидальными составляющими.

Предлагаемая система обладает относительно невысокой алгоритмической сложностью (не требуется определения частоты основного тона и разделения речевого сигнала на вокализованные и невокализованные отрезки). Кроме того, восстановленная речь обладает хорошей разборчивостью и узнаваемостью диктора.

СУБГАРМОНИЧЕСКИЙ АНАЛИЗ В СИСТЕМАХ КОДИРОВАНИЯ РЕЧЕВОГО СИГНАЛА

А.Н. ПАВЛОВЕЦ

При параметрическом кодировании речевого сигнала одним из важнейших выделяемых параметров является частота основного тона. Данная характеристика определяет качество голоса, интонации, эмоциональность речи и т.д.

Как в нормальной речи, так и в некоторых типах патологического голоса смежные вокальные циклы могут различаться амплитудой или периодом. В таких случаях определение частоты основного тона затрудняется, поскольку неясно, следует ли рассматривать каждый вокальный цикл либо два соседних цикла как один период основного тона.

В исследуемом методе определение частоты основного тона речевого сигнала осуществляется в частотной области с использованием понятия отношения субгармоники и гармоники.

Субгармоникой считается любая целая часть частоты основного тона. При определении отношения субгармоники и гармоники использовалось отношение спектров сигнала, сжатых по чётному и нечётному порядку.

В ходе исследования строился контур частоты в диапазоне от 80 до 300 Гц. Над сигналом производился кратковременный анализ Фурье. В дальнейшем линейная шкала частот подвергалась логарифмическому преобразованию, а результаты интерполировались методом кубических сплайнов. По значению отношения субгармоники и гармоники определялось, достаточен ли уровень субгармоники для того, чтобы считаться гармоникой.

Результаты показали, что алгоритм имеет достаточную точность и устойчивость в присутствии шума.

ТЕХНОЛОГИЯ КОНФИДЕНЦИАЛЬНОГО ПРОИЗВОДСТВА БЕЗОПАСНОЙ ЭЛЕМЕНТНОЙ БАЗЫ ЭЛЕКТРОННЫХ СИСТЕМ

И.Л. БАРАНОВ

Ведущие зарубежные электронные фирмы освоили серийное производство микропроцессоров и схем памяти с 0,13 мкм топологическими нормами, некоторые приступили к опытному производству ИС с 0,09 мкм нормами. У нас в республике на НПО "Интеграл" освоена 0,8 мкм технология и только

планируется переход на 0,5 мкм уровень. Ликвидация такого отставания требует колоссальных затрат. Так современный завод-мегафаб на проектные нормы 0,13 мкм стоит 1,5–3,0 млрд. долларов.

Очевидно, что наше государство не может позволить себе такие затраты, а поиск зарубежных инвесторов оказался безуспешным.

Поэтому для изготовления изделий, требующих уровня глубокого субмикрона, придется ориентироваться на зарубежные "кремниевые мастерские", мирясь с необходимостью передачи им разработок наших дизайн-центров. В этом случае необходимо разработки доводить до уровня топологии, не останавливаясь, как принято сейчас у системщиков, на модели RTL-уровня. В противном случае нет гарантий защиты наших дизайн-центров от несанкционированного использования представленной модели, ее самого ценного — идеи. Кроме того, возникают опасения – не будут ли при изготовлении ИС встроены в них так называемые "закладки", в частности, взрывающийся пористый кремний, которые в час "Ч" способны нарушить нормальное функционирование систем, нанося значительный ущерб государству.

Разработку, выполненную на уровне топологии, а еще лучше представленную комплектом фотошаблонов, изготовленным в соответствии с требованиями выбранного производства ИС, проще защитить, она не воспроизводится. После изготовления пластины должны обязательно тестироваться у себя. Тогда изготовителю даже сложно узнать, что за функциональное устройство он сделал, все ноу-хау остаются у разработчика, становится трудно вписать "закладки".

Тем более, что изготовление фотошаблонов даже для глубоко субмикронной технологии можно организовать в республике. Концерн "Планар" производит для этого самое современное оборудование.

Для полного обеспечения секретности, сокращения сроков разработок таких, как "система на кристалле", "система на пластине", требующих глубокого субмикрона, рассмотрена технология, использующая функционально законченные, многократно используемые IP-блоки в сочетании с элементами собственных, имеющих ноу-хау блоков, которые изготавливаются на пластинах в зарубежных кремниевых мастерских. Данные блоки не соединены металлизацией в систему, что исключает понимание ее функционирования. Специализация выполняется на своем относительно недорогом гибком производстве — минифабрике, с использованием бесшаблонной фотолитографии для формирования 1–2 уровневой металлизации, соединяющей эти блоки в систему. Для этого достаточно 0,5–1,0 мкм технологии, которая реализуется лазерным генератором изображений ЭМ-5299 концерна "Планар".

Исключение фотошаблонов и малые сроки (3–4 часа) программирования одного слоя снижает до минимума утечку информации о разрабатываемых устройствах.

МОДЕЛЬ ОЦЕНКИ ПОСЛЕДСТВИЙ АТАК НА ЦЕЛОСТНОСТЬ И ДОСТУПНОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В.И. НОВИКОВ

В информационном обществе доминирующим катализатором и движущей силой социально-экономического развития становятся информационные ресурсы ***(R).***. Более того, в информационном обществе они выступают как интегральный вектор направления его развития. Развивающиеся информационные ресурсы порождают позитивное развитие общества, а их деградация приводит к застою в обществе, социально-экономическим потрясениям и кризисам.

Поэтому в комплексе задач создания, получения, хранения, использования и передачи информационных ресурсов как важнейшей социально-экономической категории информационного общества проблема доступа и защиты выдвигается на первый план.

Информационный ресурс ***R*** не изменяется сам по себе. Проблемный ресурс общества ***P***, постоянно взаимодействуя с информационным ресурсом, всегда как при воздействии внешней среды, так и вне зависимости от внешней среды создает новые знания и реструктурирует информационный ресурс в результате процессов объединения и трансформации, отрицания и старения.

Механизмом и средством взаимодействия ресурсов является информационная среда общества ***S***.

Под интеллектуальным потенциалом общества ***I*** будем понимать способность общества в соответствии с проблемным ресурсом ***P,*** средствами и механизмами информационной среды общества ***S,*** в том числе за счет "живого" знания, путем активизации и всестороннего анализа информационного ресурса ***R*** находить решения проблемных ситуаций в соответствии с целями общества в направлении его развития, создавая новые знания ***R****, новые цели и проблемы ***P****, информационную среду ***S**** и интеллектуальный потенциал ***I****[1].

Классификация всех видов ресурсов может быть выполнена по ряду признаков.

По признаку отношения к определенным общественным группам такая классификация в нисходящей последовательности включает ресурсы: мировые; национальные; государственные; общественные; отраслевые; профессиональные ресурсы личности, команды.

Дадим общее для этих уровней определение интеллектуального потенциала в терминах ресурсов.

Интеллектуальный потенциал ***Ii(t)*** некоторого иерархического уровня ***i*** общества в данный момент развития ***t*** определим как способность этого уровня общества к объединению средствами информационной среды ***Si(t)*** информационного ***Ri(t)*** и проблемного ***Pi(t)*** ресурсов для создания (развития) ***Ri(t+t*), Pi(t+t*), Si(t+t*), Ii(t+t*)*** в процессе разрешения проблемных ситуаций из ***Pi(t)*** в соответствии с целями развития данного иерархического уровня общества.

Или **I** есть отображение

$$I: (R,S,P) \rightarrow R^*,S^*,P^*,I^*. \quad (1)$$

Таким образом, ***R,P,S*** *и* ***I*** составляют основу национального достояния общества в информационной стадии развития и, как следствие, представляют предмет атак, производимых с экономической, политической и другими целями.

Атака на доступность информационных ресурсов предполагает нарушение временных характеристик доступа (отказ, частичный доступ), искажение целей доступа (нарушение алгоритма поиска), подставка неадекватной информации. Атака на целостность ресурсов предполагает искажение (снижение) их точности и достоверности, разрушение структуры баз и т.д.

В модели развития ресурсов эти процессы можно представить как искажение информационного ресурса **R**

$$\Delta R = R^a - R, \quad (2)$$

где $\mathbf{R^a}$ – искаженный в результате атаки информационный ресурс.

Разность ΔR определяет меру внесенных в результате атак искажений, последствия которых могут быть оценены только в результате выполнения отображения (1), где исходным является искаженный ресурс R^a

$$I: (R^a,S,P) \rightarrow R^a*,S^a*,P^a*,I^a*. \quad (3)$$

Рассмотрим частный случай, когда отображение (1) может быть представлено в стандарте IDEF0 описания бизнес процессов [2]. Методология IDEF0 предполагает построение иерархической системы диаграмм, описывающих бизнес процессы. На верхнем уровне строится контекстная диаграмма, описывающая взаимодействие бизнес процессо й.

Семантика IDEF0 применительно к йствия ресурсов трактуется следующим образом. Отображение ***I*** представляет содерж (activity), искаженный информационный ресурс R^a - как входные да t), проблемный ресурс ***P*** - как функциональные задачи, правила, стандарты на входе управлен обесп ode механизмы (рис. 1).

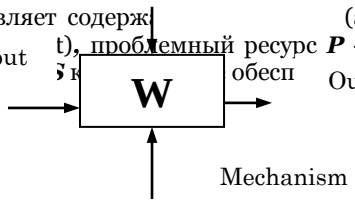

Рис. 1. Базовый блок IDEF0

Упростим модель, исключив влияние среды ***S*** . Тогда (3) может быть представлено в виде

$$I: (R^a,P) \rightarrow R^a*,P^a*,I^a, \quad (4)$$

а выход IDEF0 модели описан как $C=W(R,P)$ в идеальном случае, и как $C^a = W(R^a,P)$ в случае атаки на входной ресурс.

Рассмотрим, каким образом механизм декомпозиции контекстной модели влияет на последствия атаки на информационный ресурс.

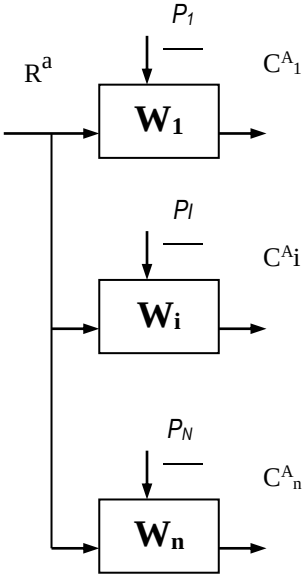

Рис. 2 Несвязные функциональные задачи

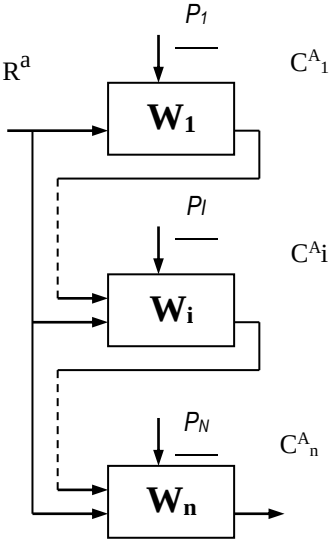

Рис. 3. Доминирование функциональных задач

Если задача P может быть представлена множеством несвязанных функциональных задач $P=(P_1 P_2 \ldots P_N)$, то декомпозиция работ может быть представлена N несвязными работами $W=(W_1W_2\ldots W_N)$ (рис.2).

Последствия атаки являются аддитивными и вычисляются как сумма погрешностей, вносимых в каждую конкретную работу

$$\Delta Ci = Ci^a - Ci. \quad (5)$$

Однако в большинстве случаев декомпозиция контекстной модели приводит к сильно-связанной модели доминирования работ (рис. 3)

Последствия атаки являются мультипликативными, так как конечный результат выполнения работ $C^A = C^A_n$ и воздействие атаки учитывается многократно.

$$\Delta Ci=Wi(R^A, C^Ai\text{-}1,Pi) - Ci. \quad (5)$$

Полученная модель положена в основу программного комплекса минимизации влияния атак на информационные ресурсы. В функции от последствий влияния атаки на конкретные работы ΔCi он позволяет синтезировать алгоритм декомпозиции работ с минимальными последствиями атаки.

Литература

1. Кривцов В.Н, Новиков В.И. Управление информационными ресурсами — перспективное направление образования // Тез. докладов IIV международной конференции "Комплексная защита информации" Мн, 2003.С. 186–188.
2. Маклаков С.В. Bpwin, Erwin. CASE-средства разработки информационных систем. М. 2000.

ОБНАРУЖЕНИЕ АКУСТИЧЕСКИХ СИГНАЛОВ НА ФОНЕ РЕЧИ

В.И. ВОРОБЬЕВ, Г.В. ДАВЫДОВ, Д.В. ЛЕЩЕНКО

Рассмотрены методы обнаружения сигналов на фоне речи, включая тональные сигналы, шумовые сигналы и частотно-манипулированные с использованием кодов Баркера. Такие методы применяются для автоматизации обнаружения несанкционированных технических средств съема акустических сигналов в выделенном помещении путем автоматического сканирования радиочастотного диапазона и анализа демодулированных сигналов.

Задача обнаружения заключается в принятии решения: в данном помещении присутствуют технические средства съема речевой информации и передачи ее по радиоканалу или указанные средства в помещении отсутствуют. При этом предполагается, что средства съема информации используют для её передачи радиопередающее устройство с амплитудной, частотной и другими видами модуляции и имеют ненаправленную антенну. Алгоритм обнаружения включает формирование и излучение в выделенном помещении тестового акустического сигнала и поиск этого сигнала в частотном спектре радио излучений в заданном диапазоне частот.

Для обнаружения технических средств съема речевой информации активным методом в качестве тестового сигнала представляется целесообразным использовать частотно-манипулированный сигнал со сменой частоты в соответствии с кодами Баркера. Корреляционная функция такого сигнала имеет четко выраженный пик, а спектральный состав обеспечивает борьбу с замираниями в условиях наличия в помещении явления акустической реверберации.

Рассматриваются наиболее распространенные критерии обнаружения и вопросы выбора оптимального критерия для решения поставленной задачи.

Для оценки эффективности представленного алгоритма обнаружения приводятся результаты моделирования. Оценены вероятность правильного обнаружения и вероятность ложной тревоги при различных значениях порога и отношения сигнал/шум. В качестве модели шума использовался случайно выбранный сигнал речи достаточно большой длительности.

ВИБРАЦИОННЫЕ ПРЕОБРАЗОВАТЕЛИ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Г.В. ДАВЫДОВ, А.В. ПОТАПОВИЧ, В.А. ПОПОВ

В настоящее время для защиты речевой информации широко используются вибрационные преобразователи. Основные электроакустические параметры различных вибрационных преобразователей систем защиты речевой информации не нормируются и отсутствуют методики оценки их эффективности.

Целью работы является исследование амплитудно-частотных характеристик вибрационных преобразователей и разработка методики измерений и сравнение основных электроакустических параметров вибрационных преобразователей.

Вибрационные преобразователи систем защиты речевой информации преобразуют электрические колебания в силовые воздействия на присоединенные конструкции и являются устройствами инерционного принципа действия. Преобразователи, работающие в системах защиты речевой информации, должны иметь достаточно широкую частотную полосу, соответствующую полосе речевого сигнала. Кроме того, их параметры не должны существенно изменятся в рабочем или заданном диапазоне температур и во времени.

В работе излагается методика измерения выталкивающей силы вибрационных преобразователей, по которой можно сравнивать эффективность различных типов преобразователей и оценивать их

изменение параметров в процессе эксплуатации. Приводятся амплитудно-частотные характеристики вибрационных преобразователей электромагнитного типа и пьезоэлектрических.

ЭКРАНЫ ЭМИ НА ОСНОВЕ МАТРИЦ ИЗ ПРОПИТАННЫХ ЖИДКОСТНЫМ НАПОЛНИТЕЛЕМ ВОЛОКНИСТЫХ МАТЕРИАЛОВ

Н.В. КОЛБУН, И.С. ТЕРЕХ, Д.В. АНДРЕЕНКОВ

В современных условиях возрастающей интенсивности использования электромагнитного излучения большое внимание необходимо уделять защите информации. Развитие методов и средств перехвата информации повышает требования к средствам обеспечения ее безопасности.

Для восстановления информационного сигнала из ПЭМИН достаточно уровня всего в 3 мкВт [1]. При взрыве электромагнитной бомбы мощный импульс электромагнитного излучения выводит из строя все электронное оборудование, включая системы хранения и обработки информации. Основным средством защиты от перечисленных явлений является экранирование.

Вода является хорошим поглотителем электромагнитного излучения СВЧ, однако ее применение ограничено конструктивными сложностями, связанными с теплоотводом и фиксацией жидкости в определенном объеме [1]. Эта задача может решаться как созданием жестких конструкций, заполненных водой, так и применением гибких материалов.

Одним из направлений создания гибких экранов ЭМИ является пропитка материалов, имеющих капиллярно-пористую структуру, различными растворами на основе воды [1].

Удержание воды в материале происходит за счет капиллярных сил, которые зависят от формы связи жидкости со скелетом материала, особенностями его структуры и термодинамическими условиями взаимодействия тела с окружающей средой [2]. Структура капиллярно-пористых сред представляет собой совокупность капилляров различной длины и радиуса, однако для упрощения расчетов и моделирования процессов, связанных с капиллярными силами, чаще всего используют совокупность сквозных цилиндрически капилляров одинакового радиуса. Данная модель применяется чаще всего для описания процессов впитывания жидкостей в такие анизотропные среды, как фильтровальная бумага, ткани, древесина, пористые элементы тепловых труб, и др. [3].

Трикотажные полотна и нетканые волокнистые материалы, представляющие собой переплетение натуральных или химических нитей являются анизотропными капиллярно-пористыми телами [2]. Волокна и нити, в молекулах которых имеются сильнополярные группы, создающие на поверхности волокон значительное силовое поле, обладают большой способностью поглощать жидкости и называются гигроскопичными. Наиболее гигроскопичны волокна натуральные шерсти, шелка, джута, хлопка. Среди химических волокон наилучшими сорбционными свойствами обладают целлюлозные волокна белкового происхождения — вискозные, полинодные; наихудшими – волокна из синтетических волокнообразующих полимеров [4].

Таким образом, применение матриц из волокнистых материалов позволяет за счет капиллярности последних сформировать распределенную структуру воды в виде капель жидкости различного размера, разделенных воздушными промежутками, которые образуются в порах материала и промежутках между отдельными нитями или волокнами.

Отражение ЭМВ от границы раздела сред обуславливается различием волновых сопротивлений этих сред. Формирование распределенной структуры воды позволяет получить большое количество границ раздела сред воздух – жидкость и материал – жидкость, тем самым, увеличивая количество переотражений ЭМВ в материале экрана.

С другой стороны, изменяя электрические свойства воды путем введения в нее различных примесей, можно изменять величину отражаемой и поглощаемой энергии.

Проводилось экспериментальное исследование зависимости величины ослабления энергии ЭМИ и коэффициента отражения от формы поверхности подложки экрана и состава растворного наполнителя.

Исследования проводились с помощью блока индикаторного Я2Р-70 и волноводной измерительной линии с двумя рупорными антеннами. В качестве генераторов использовались в диапазоне 27–36 ГГц измеритель КСВН панорамный Р2-65 (ГКЧ), а в диапазоне 78–115 ГГц — генератор РГ4-14. Образцы полотен закрепляли между рупорными антеннами после предварительной калибровки тракта.

Для эксперимента в качестве основы экрана использовались: уплотненный волокнистый нетканый материал, машинно-вязаное полотно повышенной плотности и машинно-вязаное полотно с рельефным рисунком.

В качестве пропитывающих жидкостей использовались следующие растворы:

№ 1 — водный раствор соли пищевой 10 г/л (NaCl – 68,4%, KCl – 26,3%, $MgSO_4$ – 5,3%);

№ 2 — водопроводная вода с добавлением этиленгликоля (100 мл воды, 50 мл этиленгликоля);

№ 3 — водный раствор соли с добавлением этиленгликоля (800 мл водного раствора соли, 50 мл этиленгликоля).

Исследования проводились в диапазоне частот 27–36 ГГц и 80–115 ГГц. Полученные результаты представлены в таблице.

Ослабление ЭМИ, вносимое капиллярно-пористыми материалами с разными наполнителями

Капиллярно-пористый материал	Растворный наполнитель	Частота, ГГц							
		27		36		80		115	
		$К_{осл}$, дБ	КСВ	$К_{осл}$, дБ	КСВ	$К_{осл}$, дБ	КСВ	$К_{осл}$, дБ	КСВ
Уплотненный волокнистый материал	№ 1	32	3,4	33,8	3,6	43	3	43	2,2
	№ 2	31,5	3,5	32,5	3,8	30	3,5	33	3
	№ 3	32,3	3,8	33,4	4	31	3,5	35	3
Машинно-вязаное полотно повышенной плотности	№ 1	5,5	1,9	5,5	1,6	5,1	2,3	5,2	1,7
	№ 2	10,5	2,2	10,2	2,7	14,5	2,3	16	1,8
	№ 3	9,4	2,5	9,2	2,2	13	1,6	15	1,6
Трикотажное полотно с рельефным рисунком	№ 1	35	1,5	35	1,3	43	1,9	43	1,8
	№ 2	12,5	1,4	12,3	1,4	20	1,9	25	1,8
	№ 3	8	1,5	7,8	1,4	12	1,4	15	1,4

Из полученных результатов видно, что экраны на основе матриц из волокнистых материалов обеспечивают ослабление ЭМИ порядка 30…40 дБ. Введение дополнительных примесей в воду изменяет ее диэлектрические свойства. Добавление в воду пищевой соли NaCl приводит к изменению ее электропроводности, а следовательно, и коэффициента отражения электромагнитной волны. Введение в раствор этиленгликоля уменьшает ослабление сигнала, однако и величина отраженного сигнала уменьшается. Анализ полученных данных показывает, что наибольшее ослабление электромагнитного сигнала достигается при использовании материалов с большей удельной пористостью, но коэффициент отражения таких материалов выше. Формирование геометрически неоднородной поверхности матрицы позволяет снизить коэффициент отражения ЭМИ, сохраняя при этом значение ослабления сигнала.

Литература

1. Гибкие конструкции экранов электромагнитного излучения / Л.М. Лыньков, В.А. Богуш, В.П. Глыбин и др. / Под ред. Л.М. Лынькова. Мн. 2000.
2. Прудник А.М., Борботько Т.В., Колбун Н.В., Ходыко Н.Г., Власова Г.И. Особенности пропитки анизотропных капиллярно-пористых материалов для экранов ЭМИ. Известия Белорусской инженерой академии. №2(14)/2. 2002. С. 162-165.
3. А.В. Кузьмич, В.И. Новикова. Особенности кинетики капиллярного впитывания жидкости. Препринт № 10. Институт тепло- и массообмена им. А.В. Лыкова АН БССР. Минск, 1988
4. Прокопович Д.Н., Богуш В.А., Лыньков Л.М. Влияние состава и концентрации растворных наполнителей на характеристики гибких радиопоглощающих покрытий. Известия Белорусской инженерой академии. №1(11)/3. 2001. С. 137-140.

СЕКЦИЯ 4. ПРОБЛЕМЫ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КАДРОВ

ЗАЩИТА ИНФОРМАЦИИ В ФАЙЛОВОЙ СИСТЕМЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

В.Т. ПЕРШИН

В связи с расширением практики дистанционного обучения возникают проблемы, связанные с организацией защиты от несанкционированного доступа к файлам, содержащим информацию о результатах экспертных оценок успеваемости студентов. Это наиболее уязвимая часть всей системы дистанционного обучения, так как именно она представляет наибольший интерес для опытного программиста, который может сломать защиту и изменить содержащуюся в файле информацию.

На примере создания электронного учебника по курсу "*Основы радиоэлектроники*" рассмотрены возможности надежного перекрытия доступа к файлам о результатах тестирования. Осуществлена защита памяти с помощью кода, находящегося внутри программы. Этот код ограничивает доступ к областям памяти, выделенным управляющей программой для хранения информации об успеваемости студентов.

Рассмотрен также способ размещения информации о результатах тестирования на сервере с защитой его от несанкционированного доступа системными средствами сервера.

Отмечаются преимущества предложенного способа защиты информации, заключающиеся в простоте используемых средств для его реализации, упрощении протокола взаимодействия программ, обеспечивающих размещение защищаемой информации и организацию доступа к ней нескольких пользователей разного уровня.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ДИСТАНЦИОННОМ ОБУЧЕНИИ

Д.А. МЕЛЬНИЧЕНКО, А.П. МОРОЗОВ

В настоящий момент все большее распространение получает дистанционное обучение — новая форма образования, которая сочетает в себе открытость с его интенсификацией за счет применения электронных учебников, компьютерных обучающих программ, информационных баз знаний и данных. Такой вид обучения не представляется возможным без активного использования WEB–технологий. Системы, в которых информация передается по глобальной сети особенно уязвимы: компьютерные вирусы могут распространяться моментально от системы к системе, засоряя память или разрушая программы и данные. Для систем дистанционного образования очень важно, что часть данных (личные сведения о студентах, результаты контроля знаний и т.д.) являются конфиденциальными и подлежат защите. Поэтому, создание системы информационной безопасности – необходимое условие надежного и эффективного функционирования технологии дистанционного обучения.

Обеспечение безопасности системы в целом достигается за счет обеспечения безопасности на каждом ее уровне: внешнем, сетевом, системном и на уровне приложений.

Для обеспечения надежной работы системы на каждом уровне должен быть разработан комплекс организационно–административных, технических и технологических мер по предотвращению угроз разрушения и уничтожения информации, а также устранению их последствий.

Соблюдение всех этих принципов позволит обеспечить безопасную среду для бесперебойной работы всей системы дистанционного обучения.

ОСОБЕННОСТИ ПОДГОТОВКИ ИНЖЕНЕРОВ СВЯЗИ ПО ВОПРОСАМ ПОЧТОВОЙ БЕЗОПАСНОСТИ

В.М. БУРАЧЕНКО, Л.М. ЛЫНЬКОВ, В.В. СОЛОВЬЕВ, Н.Д. ЮШКЕВИЧ

В последнее время отрасль почтовой связи осваивает большое количество новых нетрадиционных услуг, современные технологии, в том числе и в финансово-кредитной сфере. Поэтому наряду с проблемами физической безопасности персонала и объектов почтовых учреждений появляется необходимость дальнейшего совершенствования и расширения преподавания дисциплины "Почтовая безопасность" учащихся и студентов Высшего государственного колледжа связи и системы переподготовки почтовых служащих.

Для этого в рабочую программу по данной дисциплине включены новые направления, такие как, элементы банковских услуг (правоотношения, операции, инкассация, кризисные ситуации), обеспечение финансовой безопасности, включая систему международных финансовых телекоммуникаций SWIFT и электронную пересылку посредством POST * Net, новые аспекты информационной безопасности, обеспечение коммерческой тайны и некоторые другие.

Все это позволит будущим инженерам связи определить свою роль в системе почтовой безопасности и тем самым защитить интересы предприятия от источников внешних и внутренних угроз, предотвратить правонарушения, причины и условия их порождающие, а также возникновение чрезвычайных ситуаций.

ОБРАЗОВАТЕЛЬНАЯ КОМПЬЮТЕРНАЯ СЕТЬ ПЕРЕПОДГОТОВКИ СПЕЦИАЛИСТОВ

Л.П. ГАНЧАРИК

Как показывает мировой опыт, существенное повышение эффективности образовательного процесса для переподготовки специалистов в области защиты информации может быть достигнуто путем внедрения системы постоянно действующего дистанционного обучения. Академия управления при Президенте Республики Беларусь создала образовательную дистанционную телекоммуникационную среду, позволяющую решить задачу формирования интегрированного образовательного пространства для **широкомасштабной переподготовки кадров** по разным направлениям, включая специалистов в сфере защиты информации в компьютерных и телекоммуникационных сетях.

Телекоммуникационная среда основана на WaveTop технологии ИНТЕРНЕТ, не требующей использования дорогостоящих каналов связи для проведения одновременной и постоянной переподготовки **практически каждого специалиста** в области защиты информации. При этом осуществляется как дистанционное обучение специалистов, так и их массовое информирование, что обеспечивается оперативной трансляцией и актуализацией учебных WEB-сайтов по существующим телевизионным каналам непосредственно на компьютеры обучающихся. WaveTop технология ИНТЕРНЕТ имеет **самую низкую** из всех существующих сетей себестоимость доставки и актуализации данных, осуществляя передачу информации каждому конкретному абоненту через адресную систему телевизионных модемов.

Предусматривается параллельное функционирование совместно с системой дистанционного обучения Академии управления других учебных центров, оснащенных унифицированным дистанционным программно-техническим комплексом, что позволяет сформировать в республике интегрированную образовательную сеть переподготовки специалистов в области защиты информации в компьютерных и телекоммуникационных сетях.

Учебный процесс осуществляется на основе международного образовательного стандарта IMS.

ЭФФЕКТИВНОСТЬ И БЕЗОПАСНОСТЬ В ДИСТАНЦИОННОМ ОБУЧЕНИИ

А.С. БОНДАРЕНКО

В настоящее время широкое распространение получила система непрерывного обучения как комплекс мер, дающих возможность получать образование и повышать квалификацию специалистам на протяжении всего периода их практической работы. Реализация этих задач возможна на основе внедрения эффективных информационных технологий, удовлетворяющих мировым образовательным стандартам, к которым относится в частности система дистанционного обучения и консалтинга. В рамках этих образовательных технологий можно проводить дистанционную подготовку и переподготовку кадров, оказывать им повседневную консультационную помощь, предоставлять доступ к распределенным базам данных и знаний научно - технической и учебно-методической информации.

Основу образовательного процесса в дистанционном обучении составляет целенаправленная, контролируемая, интенсивная и самостоятельная работа обучающегося, который может учиться в удобном для себя месте, по индивидуальному расписанию, имея при себе комплект специальных средств обучения и согласованную возможность контакта с тьютором.

Реализация технологий дистанционного обучения вызывает необходимость учета следующих аспектов:

эффективность дистанционного обучения (ввиду территориальной распределенности обучаемых и тьюторов);

информационно-психологическая безопасность слушателей и информационная безопасность обучающих центров, поскольку учебная информация и методики обучения, как правило, имеют конфиденциальный, оригинальный или коммерческий характер.

Первая проблема решается разработкой учебных материалов нового поколения с использование цифровых компьютерных технологий (в том числе мультимедиа) — электронных учебников, пособий, справочников, лабораторных работ и практических заданий, тестирующих мультимедиа комплексов.

Учебные и методические материалы могут располагаться на CD ROM и DVD – дисках, Internet и Intranet – сайтах, локальных компьютерах обучаемых с использованием различных каналов обновления и актуализации информационных ресурсов — Internet, E-mail, Телеинтернет и др.

Решение второй проблемы возможно на основе внедрения общесетевых методов безопасного обмена привилегированной учебной и учебно-методической информацией в прямом и обратном канале информационного взаимодействия.

Внедрение эффективных технологий безопасного дистанционного обучения возможно на основе освоения тьюторами современных безопасных компьютерных и телекоммуникационных технологий, реализующих ассиметричную информационно-криптографическую систему.

Решение задачи обеспечения информационной безопасности как задачи ситуационного компьютеризированного планирования безопасного обмена электронными учебными материалами между учебными центрами и обучаемыми в территориально-распределенных сетях представляет собой выполнение тьютором или отдельным обучаемым (под контролем администратора безопасности учебного центра дистанционного обучения) логически взаимосвязанной совокупности специальных функциональных алгоритмов.

Литература

1. Гринберг А.С., Горбачев Н.Н., Бондаренко А.С. Прикладные системы обработки информации в управлении. Часть IV, Политика и программа информационной безопасности. Учебное пособие. Минск, 2000.
2. Бондаренко А.С. Вопросы взаимодействия информационных систем в рамках теории защитных оболочек; Национальная безопасность: управленческие и информационные технологии обеспечения. Материалы межведомственной научно-практической конференции, Минск, 10–11 июля 1999.
3. Бондаренко А.С. Реализация обратного канала в сети дистанционного обучения Академии управления при Президенте Республики Беларусь; Образовательные технологии в подготовке специалистов, Сборник научных статей, Минск, 2003.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО КУРСУ "ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ"

Л.М. ЛЫНЬКОВ, А.М. ПРУДНИК

В настоящее время одной из главных задач подготовки специалистов в области телекоммуникаций является необходимость преподавания предметов, рабочая программа которых предполагает получение знаний о современных банковских системах и способах защиты информации. С этой целью в Белорусском государственном университете информатики и радиоэлектроники на кафедре сетей и устройств телекоммуникаций проводится постановка лабораторного практикума по курсу "Защита информации в банковских технологиях".

Данный лабораторный практикум включает лабораторные работы: "Защита информации от утечки по каналам ПЭМИН", "Защита информации в интеллектуальных картах", "Защита информации в телефонных картах", "Международная телекоммуникационная сеть SWIFT".

Целью работы "Защита информации от утечки по каналам ПЭМИН" является изучение пассивных способов защиты информации от утечки по каналам побочных электромагнитных излучений и наводок.

Работы "Защита информации в интеллектуальных картах" и "Защита информации в телефонных картах" студенты будут изучать предназначены для изучения студентами систем обеспечения информационной безопасности при производстве и эксплуатации электронных пластиковых карт, алгоритмы защиты и процедуры аутентификации электронных пластиковых карт и структурную схему модуля безопасности. Для контроля знаний студентов будут использоваться компьютерные программы, содержащие информацию описательного характера и систему оценки знаний студентов (коллоквиумы).

В работе "Международная телекоммуникационная сеть SWIFT" студенты будут изучать пакет прикладных программ Turbo SWIFT, и язык сообщений системы SWIFT.