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