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