РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ ДЛЯ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Семенов С.Г., Боклаг Я.

Национальный технический университет «Харьковский политехнический институт», г. Харьков

Для проведения экспериментальных исследований статистических свойств сетевого трафика и обоснования практических рекомендаций по построению сетевых систем обнаружения и предотвращения вторжений разработана имитационная модель.

Разработанная имитационная модель содержит:

– блок генерации сетевого трафика, который предназначен для имитации потока данных в компьютерной системе (КС) как на подготовительном, так и на основном этапе функционирования;

– имитаторы захвата и фильтрации сетевого трафика – имитируют соответствующие процедуры сетевого анализатора, т.е. производят первичную обработку сгенерированных блоком генерации данных;

– блок статистической обработки, предназначен для анализа отфильтрованных данных и формирования на его основе статистических портретов;

– блок хранения данных, сберегает статистические портреты шаблонных данных;

– блок проверки статистических гипотез, предназначен для обработки статистических портретов шаблонных данных и потоков данных отдельных служб и сервисов КС;

– блок принятия решения, на основании результатов проверки статистических гипотез обобщает и принимает решение о наличии или отсутствии вредоносного сетевого трафика и соответствующего вторжения;

– блок формирования уведомлений и воздействий;

– на основании принятого решения (в блоке принятия решения) осуществляется формирование управляющих воздействий (в случае обнаружения вторжения) и формируется уведомление для системного администратора (оператора безопасности) о текущем состоянии системы;

– блок управления, осуществляет согласование работы остальных блоков имитационной модели и управление основными вычислительными операциями.

В докладе определено, что разработанная имитационная модель может адаптивно реагировать на текущую ситуацию и при необходимости блокировать подозрительный трафик и рассылать предупреждения соседним узлам сети, на рабочую станцию сетевого администратора, сервер протоколирования атак и т.д.