PROBLEMS OF INFORMATION PROTECTION IN SYSTEMS OF MODELING OF DYNAMIC OBJECTS

M.M. Karimov, S.M. Sagatova

The article is devoted to the protection of information in modeling systems. A multi-level hierarchical system is proposed to collect and analyze data on packet traffic in order to detect and repel intrusions and protect against unauthorized access to network resources in dynamic object modeling systems.

ДИНАМИК ОБЪЕКТЛАРНИ МОДЕЛЛАШТИРИШ ТИЗИМЛАРИДА АХБОРОТ ХАВФСИЗЛИГИ МУАММОЛАРИ

М.М. Каримов, С.М. Сагатова

Мақола моделлаштириш тизимларида ахборотларни ҳимоялашга бағишланган. Динамик объектларни моделлаштириш тизимларидаги тармоқ ресурсларига ҳужумларни аниқлаш ва қайтариш ҳамда рухсатсиз киришдан химоялаш мақсадида пакетли трафик тўғрисидаги маълумотларни йиғиш ва таҳлил этишга мўлжалланган кўп сатҳли иерархик тизим таклиф этилган.

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ МОДЕЛИРОВАНИЯ ДИНАМИЧЕСКИХ ОБЪЕКТОВ

М.М. Каримов, С.М. Сагатова

Необходимость решения вопросов защиты информации в системах моделирования динамических объектов требует перехода к качественно новым методам анализа сетевого трафика, включая анализ прецедентных данных, а также новым методам выявления и предотвращения вторжений и утечек конфиденциальной информации. Поэтому разработка методов защиты информации в компьютерных сетях нового поколения на базе многоуровневой модели обнаружения вторжений, обеспечивающей оперативный и долговременный анализ пакетного трафика, и на его основе блокирующей вторжения и неавторизованное обращение к информационным ресурсам, является актуальной задачей [1].

Внедрение обозначенных выше решений позволит разработать распределенные масштабируемые интеллектуальные программные системы комплексного обеспечения компьютерной безопасности, что значительно повысит эффективность и безопасность использования компьютерных сетевых

технологий в системах управления любого уровня.

Созданная модель обладает следующими преимуществами по сравнению с другими системами обнаружения вторжений: реакцией в режиме реального времени на известные и выявляемые вторжения; выявление скрытых или неизвестных сигнатур, методов или алгоритмов вторжений и фильтрацией последующих вторжений использующих эти методы или алгоритмы; возможность легкого масштабирования модели для предотвращения вторжений в различных сегментах сети; возможность применения различных алгоритмов для анализа данных; анализ данных в различных сегментах сети с целью выявления децентрализованных вторжений или несанкционированного доступа.

В заключение можно сказать, что новизна предлагаемых подходов заключается в методах, алгоритмах и средствах обнаружения и отражения вторжений, защиты от несанкционированного доступа к информации, обеспечивающих создание аппаратно-программного комплекса и анализа трафика на основе комплексного применения новых методов интеллектуального анализа трафика и скрытной фильтрации, таких как:

- метод полной скрытной фильтрации пакетного трафика по совокупности критериев, в том числе в сегментах виртуальных локальных вычислительных сетей (ВЛВС) для предотвращения утечек конфиденциальной информации и защиты информации от несанкционированного доступа;
- интеллектуальный анализ и самонастройка алгоритмов обработки трафика для выявления закономерностей в наборе прецедентных данных с целью автоматизированного формирования правил фильтрации и сигнатур обнаружения вторжений без участия экспертов.

Литература.

1. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях: 2-е изд., перераб. и доп. - М.: Радио и Связь, 2001.