СИСТЕМА ЦЕНТРАЛИЗОВАННОГО МОНИТОРИНГА И КОНТРОЛЯ СОСТОЯНИЯ УЗЛОВ КОМПЬЮТЕРНОЙ СЕТИ

Ю.М. Кротюк, Я.И. Кирилов

Система централизованного мониторинга и контроля состояния узлов компьютерной сети "Монитор" представляет собой многокомпонентную распределенную систему реального времени и призвана обеспечить интеграцию различных программных, аппаратных и аппаратно-программных средств и сервисов обеспечения безопасности корпоративной сети в единую информационную среду, реализующую унифицированные механизмы сбора, хранения и обработки оперативной информации о возникающих в процессе эксплуатации компьютерной сети событиях, например, таких как неудачная попытка аутентификации, ошибка репликации Active Directory, обнаружение вирусного заражения, отказ порта коммутатора и т.п. Вся информация о подобного рода событиях принимается соответствующим компонентом системы, аккумулируется в центральной базе данных, а затем выводится на консоль автоматизированного рабочего места администратора корпоративной информационной сети. Вывод информации сопровождается световой сигнализацией и звуковым оповещением.

"Монитор" способен взаимодействовать с электронной моделью корпоративной информационной сети, представляющей собой совокупность сведений о физической топологии сети, имеющихся узлах, каналах связи и их характеристиках. Электронная модель визуально представлена на плоскости в виде диаграммы размещения, например оформленной в соответствии с получившей широкое распространение графической нотацией, утвержденной стандартом унифицированного языка моделирования UML [1].

Все события, инициированные поставщиками, попадают в базу данных только после прохождения фильтра событий. Любое событие, хранящееся в базе данных, может находиться в одном из двух состояний — обработано администратором (не активно) или не обработано администратором (активно). Узел сети, для которого в базе данных зафиксировано хотя бы одно активное событие считается активным, иначе — не активным. Отображение активных узлов на диаграмме размещения сопровождается световой сигнализацией. Система обеспечивает возможность фильтрации событий в соответствии с устанавливаемыми правилами.

Литература

1. Леоненков А. Объектно-ориентированный анализ и проектирование с использованием UML и IBM Rational Rose. Москва, 2006.