

ЭКСПЕРИМЕНТАЛЬНАЯ УСТАНОВКА ДЛЯ ИССЛЕДОВАНИЯ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК КОРПОРАТИВНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Мишин Д.В., Щербин П.В.

ВГУ им. А.Г. и Н.Г. Столетовых, г. Владимир

В процессе исследования функциональных характеристик (ФХ) корпоративных сетей передачи данных (КСПД) современных предприятий, исследователь сталкивается с необходимостью проведения экспериментов, моделирующих информационные процессы (ИП) сети. Значительные затраты финансовых, технических и временных ресурсов на проведение подобных экспериментов актуализируют необходимость создания специализированной экспериментальной установки (СЭУ), моделирующей как структурно, так и функционально исследуемую сеть предприятия. Принципы построения КСПД значительно отличаются от принципов построения локальных вычислительных сетей (ЛВС) [1]. КСПД – как правило, гетерогенные распределенные структуры, включающие различные среды передачи, множество коммуникационных протоколов, многокомпонентное программное обеспечение, опорное и периферийное оборудование различных производителей (cisco, d-link, ascorp, и т.д.) [2, 3], что делает задачу построения СЭУ нетривиальной.

В работе авторами предлагается реализация структуры СЭУ КСПД на основе программных средств виртуализации (ПСВ): Graphical Network Simulator 3 (GNS3) [4], Oracle VirtualBox.

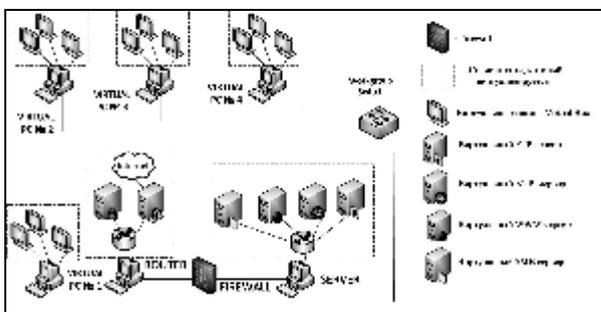


Рис. 1. Схема моделируемой КСПД

В качестве исходной платформы СЭУ выступает ЛВС (состоящая из семи ПК и коммутатора), схема моделируемой КСПД представлена на рис. 1, где пунктиром обозначены элементы, реализуемые ПСВ. Структурно КСПД будем рассматривать как распределенную техническую инфраструктуру, представляющую собой организованную совокупность структурных элементов (СЭ) – окончных узлов (рабочих станций и серверов), коммуникационного оборудования (коммутаторов, маршрутизаторов и т.д.) и каналов электросвязи. Из рис. 1 очевидно, что предлагаемая СЭУ реализует все типовые СЭ КСПД.

Посредством предложенной СЭУ были поставлены следующие эксперименты:

- исследование работоспособности метода обнаружения ботнетов на основе кластерного анализа;
- исследование работоспособности метода обнаружения ботнетов на основе скрытой гибридной модели Маркова;
- исследование системы перехвата сетевого трафика компании и алгоритмов эвристического анализа перехваченных документов;
- исследование SIR-модели динамики распространения вредоносных программ.

Авторы предлагают СЭУ как типовую экспериментальную установку для исследования функциональных характеристик КСПД.

Список литературы:

1. Мишин Д.В., Монахова М.М. Современные подходы к автоматизации администрирования корпоративных сетей передачи данных / Современные информационные технологии в образовательном процессе и научных исследованиях: Материалы III Международной научно-практической конференции (г. Шуя, 26 ноября 2010 года.). – Шуя-Иваново-Владимир: Изд-во ГОУ ВПО "ШГПУ". – 2010. – 136 с.;
2. Кульгин М. Технологии корпоративных сетей / Энциклопедия. - СПб.: Питер, 1999. – 704 с.
3. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.