Романчук Р.И. *— рецензент Киселев Г.Д.*
УНК "ИПСА" НТУУ "КПИ", Киев, Украина

Сетевая инфраструктура кафедры СП

В роботе рассматривается концепция построения сетевой защиты, которая интегрируется во все компоненты защищаемой информационной системы. Даная концепция предоставляет целостный и достаточный набор средств защиты от актуальных угроз информационной безопасности, реализуя проактивную, активную и реактивные модели защиты информации и используя различные направления обеспечения безопасности.

Целью данного исследования является создание модели построения многоуровневой системы защиты, при которой нарушение одного уровня защиты не означает нарушение всей системы безопасности.

При построении модели был использован опыт построения сети, основанный на анализе существующих концепций защиты мультисервисных компьютерных сетей.

Основные шаги моделирования:

1. Анализ информации политики безопасности, выбор устройств защиты.
2. Оценка эффективности защитных сетевых устройств.
3. Определение простой модели реализации, учитывающей взаимодействия базовой сегментации сети и классов многофункциональных сетевых устройств защиты для построения централизованной сети.

Защищенная сетевая инфраструктура отвечает следующим принципам:

1. Централизация сервисов. Такой подход обеспечивает целый ряд преимуществ, таких как сокращение расходов в удаленных офисах на обслуживание сети и содержание персонала, повышение скорости подключения новых офисов и наличие единых корпоративных политик, распространяющихся на новые офисы практически автоматически.
2. Управление сетями. С целью обеспечения гибкости архитектуры корпоративных сетей потребуются интегрированные и упрощенные решения по управлению сетями, позволяющие защитить и оптимизировать сеть.
3. Сегментация сети. Выбор подхода зависит от того, какие приложения будут функционировать в нескольких сегментах, какой уровень контроля над этими приложениями вам нужен, какая информация передается по сети и как часто приходится заниматься конфигурацией сетевых сегментов.
4. Криптографическая защита. Криптографические методы защиты информации работает на любом уровне взаимодействия, что делает их наиболее востребованной на рынке в настоящее время.
5. Межсетевой экран. Позволяет регламентировать потоки сетевого трафика в рамках как внутреннего, так и внешнего информационно.
6. Система обнаружения и предотвращения вторжений. Обнаружения и предотвращения вторжений автоматизируют процесс блокировки вторжений и необходимы в организации любого уровня, чтобы предотвратить ущерб и потери атак.

Результаты. Предложена простая модель сетевой инфраструктуры, учитывающая взаимодействия базовой сегментации сети и многофункциональных сетевых устройств защиты.

Литература

1. Олифер В., Олифер Н. Компьютерные сети: принципы, технологии, протоколы. – 4-е изд. – СПб.: Питер, 2010. С. 828–903.
2. Дж.Л. Месси. Введение в современную криптологию. ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988, с. 24–42.
3. В.А. Галатенко. Основы информационной безопасности.

International conference on System Analysis and Information Technologies SAIT 2011
Institute for Applied System Analysis of National Technical University of Ukraine "KPI", Kyiv, Ukraine, May 23–28, 2011
ISBN 978-966-2153-57-6, revision 0.9.2 (2011.05.12), available at http://sait.kpi.ua/books/sait2011.ebook.pdf