УДК 004.7

ПРОБЛЕМАТИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ПОСРЕДСТВОМ СЕГМЕНТАЦИИ СЕТИ

Бондарева А.Д. (Университет ИТМО, г. Санкт-Петербург)
Научный руководитель – к.т.н., доцент Кузнецов А.Ю.
(Университет ИТМО, г. Санкт-Петербург)

В работе исследованы существующие решения по обеспечению безопасности информационных сетей. Определено влияние конфигурации информационных сетей на уровень безопасности информационных ресурсов.

Введение. С ростом количества информационных ресурсов и сервисов, предоставляемых внутри корпоративной сети, возрастает сложность сопровождения и ведения ИТ-инфраструктуры. Распространенным случаем является подключение новых узлов сети, настройка соединений для каждого нового сотрудника, каждой конкретной задачи производства к существующей системе наиболее быстрым и удобным для администратора сети способом.
Часто организации сталкиваются с рядом проблем, связанных с информационной безопасностью, таких как проникновение злоумышленника во внутреннюю сеть и невозможность предотвращения утечек информации из-за отсутствия полной информации о текущей конфигурации сети. Во избежание подобных инцидентов информационной безопасности применяется процедура сегментации сети, осуществляемая посредством анализа бизнес-процессов, аудита существующей конфигурации сети, проектирования и документирования необходимой безопасной конфигурации.

Основная часть. На основе этого, представляется возможной разработка автоматизированной системы поддержки принятия решений для построения оптимальной конфигурации сети, учитывающей требования по защите информации и возможные ограничения ее реализации. До настоящего времени были предложены отдельные технологии сегментации сетевой инфраструктуры, например, TrustSec от компании Cisco. Однако подобные решения построены для строго определенного аппаратного обеспечения и не учитывают особенности уже реализованной сетевой топологии. В работе предложен метод для решения проблемы сегментации сети. Он основан на разработке набора критериев безопасности сети, основанных на оценке степени критичности информационных активов и анализе угроз информационной безопасности, характерных для сетевых технологий. Данный метод основан на классификации и кластеризации объектов и субъектов сетевого взаимодействия и методах оптимизации предложенных критериев для достижения наибольшей безопасности сети с учетом накладываемых ограничений.

Выводы. Результаты работы предполагается использовать при построении безопасной сетевой инфраструктуры в организациях произвольного размера. Для этого предполагается разработка программного комплекса, включающего в себя как средства сбора и анализа информации о сетевой инфраструктуре, так и механизмы поддержки принятия решений на основе собранных сведений. Использование научно обоснованного подхода к проектированию сети позволяет достичь максимально возможного уровня информационной безопасности при минимальных затратах человеческих и материальных ресурсов.