УДК 004.7

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ДЛЯ СЕГМЕНТАЦИИ СЕТИ

Бондарева А.Д., Шилов И.М. (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 моделированию структуры информационных сетей. Предложены подходы для моделирования сетевой инфраструктуры в задаче сегментации сети.

Введение. Задача обеспечения безопасности сетевой инфраструктуры представляется одной из наиболее важных в контексте защиты информации на предприятии. До настоящего времени было предложено множество подходов к решению данной задачи. Среди прочего возможна сегментация сетевой инфраструктуры для ограничения числа возможных путей для ее компрометации. Существующие методы направлены на построение программной сегментации поверх физической сети и имеют ряд недостатков, ограничивающих их применение. В то же время предложенные механизмы для оценки безопасности сети достаточно сложны, поскольку используют граф действий атакующего. Кроме того, они в значительной степени опираются на экспертный подход.

Основная часть. В работе предложено два метода обеспечения моделирования сетевой инфраструктуры для решения задачи безопасности. В рамках моделирования учитываются такие параметры, как критичность ресурсов, количество доступных атакующим техник и тактик в соответствии с MITRE ATT&CK, наличие средств защиты, повышенных привилегий, доступа в Интернет и т.д. Созданный критерий безопасности представляет собой оптимизируемую функцию, которая вычисляется за меньшее время, чем предложенные другими авторами подходы с моделированием графа действий атакующего.

Математическое моделирование направлено на построение модели сети, для которой возможна задача оптимизации. При этом обеспечивается минимальное значение сформированного критерия безопасности в условиях ограниченности ресурсов. Данная модель используется, в первую очередь, для отсечения избыточных связей в сетевой топологии. С использованием теории графов создается модель сетевой инфраструктуры, для которой возможно решение задачи оптимизации с помощью генетических алгоритмов. Предложенный авторами ранее критерий безопасности также адаптирован для данной модели. Модель, построенная на основе теории графов, позволяет проводить более глубокое перестроение сети по требованиям безопасности.

Результаты. Основными преимуществами сформированных моделей являются простота построения и вычисления критерия безопасности, что позволяет значительно ускорить процесс первичного перестроения сети. В дальнейшем данные модели будут использованы для решения задачи оптимизации при построении сетевой инфраструктуры, а также при перестроении существующей и функционирующей сети.