РАЗРАБОТКА ПОКАЗАТЕЛЕЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Герцог А.Н.
Научный руководитель – к.т.н., доц. Олейников Р.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. БИТ, тел. (057) 702-14-25)

Intrusion detection system evaluation is considered. Qualitative and quantitative indicators of practical functionality IDSs are investigated for developing a scoring system.

Системы обнаружения и предупреждения вторжений являются одной из основных компонент безопасности современной корпоративной сети. Отличительной особенностью таких систем является анализ действий пользователя с последующим принятием решения об их легальности и оповещением офицера безопасности. Такой подход реализует мощное противодействие сетевым атакам и способствует расследованию уже произошедших инцидентов.

Рынок систем обнаружения вторжений достаточно широк и включает в себя как коммерческие, известных мировых производителей в области информационных технологий, так и свободно распространяемые программные продукты. Ввиду такого многообразия становится актуальной проблема выбора решения для конкретной модели корпоративной сети, особенно при наличии нескольких решений обладающих, по словам разработчика, схожими функциональными возможностями. Очевидно, что без применения единой системы количественной и качественной оценки объективная оценка практической применимости той или иной системы обнаружения вторжений является невозможной.

В докладе предложены показатели оценки системы обнаружения вторжений, определяющие ее практические возможности. Практические возможности описываются двумя наборами показателей. Первый набор представляет собой ряд качественных показателей, позволяющих проверить применимость системы для конкретной сетевой модели. Второй набор – ряд количественных показателей, характеризующий эффективность выявления атак, а также реагирования на них.

Применение предложенных показателей оценки эффективности системы обнаружения вторжений позволит объективно определить ее практические возможности, соответствие политике безопасности корпоративной сети, а так же возможность масштабирования в случае расширения сети. Использование предложенных критериев существенно упростит процесс выбора оптимального решения безопасности среди существующих на данный момент.