ОБНАРУЖЕНИЕ АТАК НА ОСНОВЕ КОРРЕЛЯЦИИ ДАННЫХ О СОБЫТИЯХ ОТ НЕСКОЛЬКИХ ИСТОЧНИКОВ

Ю.А. Калинин, А.И. Понамарчук

На сегодняшний день не существует идеальной системы обнаружения и противодействия любых вторжений. Процесс обнаружения можно усовершенствовать путем комбинирования различных средств обнаружения. Корреляция — причинная, дополнительная, схожая (обоюдная) взаимосвязь или структурное, функциональное (качественное) соответствие между двумя сравнимыми событиями, в данном случае — событиями безопасности. Система корреляции событий получает информацию на всех стадиях и объединяет ее по определенным алгоритмам. Произведена классификация корреляций по типу, методу и по условию. Количество сообщений безопасности растет в экспоненциальной зависимости от количества устройств в сети, подверженных атакам. На данный момент, число событий безопасности в крупной телекоммуникационной системе может достигать нескольких миллионов за сутки. Соответственно подавляющее большинство их являются ложными, либо несут минимальный характер. Акцентируется внимание на составление правил корреляции исходя из локальных условий телекоммуникационной системы, к которым можно отнести, к примеру, версию операционной системы, используемые сервисы и их критичность, наличие возможных уязвимостей, человеческий фактор. Рассматриваются алгоритмы выбора нужного механизма корреляции при аудите системы безопасности, а также вопросы приоритезации обнаруживаемых атак или уязвимостей.