А. В. Никишова (Волгоград, ВолГУ)**. Многоагентная модель оценки защищенности информационной системы.**

Существует множество моделей для исследования эффективности действий службы безопасности и злоумышленника. Одной из таких моделей является многоагентная модель. Она включает множество агентов–нарушителей и агентов системы безопасности, которые являются активными агентами, и агентов информационной системы (ИС) — пассивных агентов. Активные агенты способны выбирать наиболее рациональные стратегии защиты и нападения в зависимости от располагаемых знаний об ИС и обучаться в процессе выполнения своих действий.

Агенты злоумышленников и системы безопасности, исходя из инструментария и располагаемых сведений об ИС, строят собственные деревья уязвимостей.

Агент–злоумышленник осуществляет вероятностный переход по построенному дереву уязвимостей, учитывая примененные средства защиты.

Еще одной задачей кроме построения системы защиты, стоящей перед агентами системы безопасности, является задача обнаружения вторжений. Для решения данной задачи в модель может быть добавлен агент обнаружения вторжений. Получая и обрабатывая новые сведения о системе, этот агент способен не только обнаруживать ранее известные ему атаки, но и обучаться, определяя попытки реализации ранее неизвестных ему атак. Для обнаружения неизвестных атак, использующих неизвестные уязвимости, для мониторинга применяется адаптивная способность нейронных сетей.

Для системного мониторинга могут быть использованы следующие сведения о событиях безопасности операционной системы Windows: тип события; код события; имя пользователя; время возникновения.

Для проведения мониторинга на сетевом уровне могут быть использованы следующие сведения о пакетах, пересылаемых по сети: адрес источника; адрес получателя; протокол (следующий заголовок); время приема пакета.

Для анализа собираемых сведений может быть использован наиболее универсальный тип нейронной сети многослойный персептрон. Функционирование нейросетей характеризуется формулами

$$NET_{jl} = \sum_i w_{ijl} x_{ijl}, \quad OUT_{jl} = F(NET_{jl} - \Theta_{jl}), \quad x_{ij(l+1)} = OUT_{ij},$$

где i — номер входа, j — номер нейрона в слое, l — номер слоя; X_{ijl} — i-й входной сигнал j-го нейрона в слое l; w_{ijl} — весовой коэффициент i-го входа нейрона j в слое l; NET_{jl} — взвешенная сумма сигналов на входе j-го нейрона в слое l; OUT_{jl} — выходной сигнал j-го нейрона в слое l; Θ_{jl} — пороговый уровень нейрона j в слое l.

Для обучения может быть использован алгоритм обучения с помощью процедуры обратного распространения.

При обнаружении атаки агент обнаружения вторжений устанавливает на соответствующем ребре дерева политики безопасности флаг детектируемости атаки. Если данный флаг установлен, то злоумышленник не может осуществить переход по соответствующему ребру графа.

Включение в многоагентную модель модели агента обнаружения вторжений позволяет решить задачу активного обнаружения и реагирования на действия злоумышленника.