УДК 681.3

МНОГОАГЕНТНАЯ АДАПТИВНАЯ СИСТЕМА АНАЛИЗА ЗАЩИЩЕННОСТИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Стародумов И.С.
Научный руководитель – к.т.н., доцент Валеев С.С.
Уфимский государственный авиационный технический университет

Предложен прототип многоагентной системы, позволяющей решить проблему выбора контролируемых параметров (уязвимостей) локальной вычислительной сети (ЛВС) при анализе ее защищенности.

Одним из недостатков современных систем анализа защищенности ЛВС (например, Internet Scanner) является отсутствие автоматического выбора параметров, на основе которых проводится анализ. Это влечет за собой излишние затраты времени и средств на проведение анализа защищенности.

Разработанный прототип системы представляет собой сообщество программных агентов, размещенных по узлам ЛВС. Агенты решают задачу оптимального выбора параметров в несколько этапов:

- определение роли каждого пользователя и каждого узла;
- определение ценности каждого узла ЛВС;
- определение риска по каждому из параметров и решение задачи оптимизации;

На этапе определения ролей происходит классификация пользователей и узлов на основании значений их характеристик. Набор характеристик и множество возможных ролей задаются заранее администратором системы. Для каждой роли при помощи метода экспертных оценок задается ее относительная важность. Для классификации агенты могут использовать методы искусственного интеллекта (нейронные сети, нечеткая логика).

Ценность узла сети определяется исходя из роли самого узла, а также его пользователей: $C_i = f_1(R(N_i), R(U_{i1}), R(U_{i2}),..., R(U_{in}),)$, где C_i – ценность i-го узла, $R(N_i)$ – относительная важность роли i-го узла, $R(U_{ij})$ – относительная важность роли j-го пользователя i-го узла.

На заключительном этапе при определении риска агент использует информацию о значимости каждой уязвимости для каждой из ролей. Эта информация также предоставляется администратором заранее и может быть получена при помощи метода экспертных оценок. Риск для i-го узла определяется выражением: $R_{ij} = f_2(C_i, V_{ij})$, где R_{ij} – риск для i-го узла по j-му параметру, C_i – ценность i-го узла, V_{ij} – значимость j-го параметра для i-го узла. Если j-й параметр для i-го узла контролируется, то $R_{ij} = 0$.

Итоговое значение риска для всей сети определяется выражением:

$R = \sum_{i=1}^{N} \sum_{j=1}^{M} R_{ij}$, где N – количество узлов ЛВС, M – количество параметров. Затраты на проведение анализа защищенности определяются по аналогичной формуле. Задача оптимизации заключается в минимизации затрат при заданном уровне риска.