ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 5
2012

А. Ю. Оладько (Волгоград, ВолГУ)**. Иммунная толерантность подсистемы защиты информации в операционных системах.**

В случае, если злоумышленником проводится атака на операционную систему с использованием уязвимости в важном компоненте операционной системы, при функционировании в качестве системы защиты этой ОС адаптивной системы защиты на базе иммунной сети, описанной в работе [1], в результате проведения иммунного ответа против злоумышленных действий процессов может быть проведен лизис — программируемое разрушение процессов под влиянием агентов-реакторов. Однако данная процедура может быть проведена и против того компонента операционной системы, который содержит уязвимость, что приведет к отказу в доступности системного сервиса. Так, например, в случае, если злоумышленник атакует сервер корпоративной сети с использованием уязвимости СУБД, лизис данного процесса СУБД в ходе иммунного ответа может привести к потере данных компании, а также невозможности работы персонала.

Таким образом, целесообразным является дополнение адаптивной системы защиты на базе иммунной сети операционной системы функционалом иммунологической толерантности, которая позволяла бы предотвратить проведение иммунного ответа на важные компоненты операционной системы.

Иммунологическая толерантность — утрата или ослабление способности организма к иммунному ответу на данный антиген [2], т. е. способность иммунной системы специфически не реагировать на конкретный антиген. Например, при беременности развивается толерантность иммунной системы матери по отношению к эмбриону и плаценте.

Активно функционирующие механизмы толерантности необходимы для предупреждения воспалительных реакций в ответ на многие безвредные антигены, попадающие в организм с воздухом и пищей и действующие на слизистую оболочку дыхательных путей. Однако наиболее важна толерантность к собственным антигенам организма; она предотвращает иммунный ответ против собственных тканей.

Разработанную формальную модель системы иммунной толерантности можно описать следующим кортежем:

$$ITol = \{\{S_{\text{proc}}\}, \{S_{\text{func}}\}, \{S_{\text{obj}}\}\},$$

где S_{proc} — множество системных утилит операционной системы, к которым не может быть применен процесс лизиса; S_{func} — множество системных вызовов операционной системы, к которым может быть ограничен доступ уязвимой системной службы; S_{obj} — множество объектов операционной системы, доступ к которым из уязвимой системной службы может быть ограничен.

СПИСОК ЛИТЕРАТУРЫ

1. *Оладько А. Ю.* Модель адаптивной многоагентной системы защиты в ОС Solaris 10. — Изв. ЮФУ. Техн. науки. Информ. безопасность, 2011, № 12 (125), с. 210–217.
2. *Фонталин Л. Н.*, *Певницкий Л. А.* Иммунологическая толерантность. М., 1978.