УДК 004.056

ПРИМЕНЕНИЕ ИММУННЫХ МЕХАНИЗМОВ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Титов Д.С., Университет ИТМО
Научный руководитель – Коржук В.М., Университет ИТМО

В данной работе рассматриваются механизмы иммунной системы, которые применяются в системах обнаружения вторжений. Описан общий алгоритм использования иммунных механизмов для решения задач обнаружения сетевых атак. Выделены основные параметры алгоритма, которые влияют на эффективность его работы.

Введение. В настоящее время системы обнаружения вторжений (СОВ) являются одним из необходимых элементов в системе безопасности практически любой организации, которая обрабатывает различного рода информацию с помощью компьютерных сетей. Существует большое количество методов, с помощью которых СОВ обеспечивают защиту информации. Одним из наиболее перспективных методов является использование иммунных алгоритмов.

Основная часть. Развитие информационных технологий имеет не только положительную сторону для человека. Также с каждым годом растет число различного рода сетевых атак, которые постоянно модифицируются. Именно поэтому очень важно иметь такое средство защиты, которое не будет зависеть от известных сигнатур так злоумышленников. С решением данной задачи могут помочь иммунные механизмы. Иммунные механизмы представляют в совокупности искусственную иммунную систему, которая реализует функции естественной иммунной системы человека. Главная особенность иммунной системы человека – это адаптивность к новым видам чужеродных вредных микроорганизмов. Адаптивность к новым видам сетевых атак может помочь обеспечить механизм клональной селекции. Его главной целью является создание копий той клетки (детектора), которая среагировала на подозрительную активность. После этого копии модифицируются (немного изменяются), что позволяет в итоге находить видоизмененные атаки. Также очень важным является механизм негативного отбора клеток. Он позволяет генерировать детекторы, которые не будут реагировать на «нормальный» сетевой трафик. Целью данной работы является описать алгоритм использования некоторых механизмов иммунной системы (клональная селекция и негативный отбор клеток), а также выделить основные параметры данного алгоритма, которые могут влиять на эффективность его работы, то есть на частоту возникновения ошибок первого и второго рода.

Выводы. В результате проведенного исследования был описан алгоритм работы системы обнаружения вторжения, принцип работы которой основан на механизмах иммунной системы. Также были выделены параметры, настройка которых может увеличить эффективность обнаружения сетевых атак на защищаемые ресурсы.

Титов Д.С.

Коржук В.М.