С. В. Гаврилюк, Б. Н. Оныкий, А. А. Станкевичус

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ СРЕД РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ[1]

Довольно широкую популярность сегодня приобрели технологии, работающие по тем же самым принципам, что и органы человека: искусственный интеллект, основанный на нейронных сетях, средства обработки зрительных образов, искусственная сетчатка, всевозможные генетические алгоритмы. Информационные системы, построенные на принципах работы иммунитета, имеют огромный потенциал во многих областях. На данный момент искусственные иммунные системы используются преимущественно как разновидность систем искусственного интеллекта, однако весьма перспективным видится использование систем защиты, работающих по принципу иммунитета, для борьбы с компьютерными вирусами, обнаружения сетевых вторжений и т. д.

При создании искусственной иммунной системы необходимо представить модель функционирования иммунной системы человека. Это сложный механизм, состоящий из множества различных компонентов. Используя достижения генной инженерии, обозначим некоторые основные элементы, которые переносятся в компьютерные сети.

Главным принципом действия человеческой иммунной системы является сравнение определенных «шаблонов» с находящимися внутри организма телами и выявление таким образом инородных тел.

«Шаблонами» являются лимфоциты, постоянно генерируемые спинным мозгом и тимусом с учетом информации, содержащейся в ДНК. Такая информация накапливается перманентным образом, и этот процесс называется эволюцией генной библиотеки. Лимфоциты разносятся по организму через лимфатические узлы, причем каждый тип лимфоцита отвечает за обнаружение какого-то ограниченного числа инородных тел. При генерировании лимфоцитов используется алгоритм отрицательного отбора. Проводится своеобразный тест на обнаружение лимфоцитом родных клеток организма: если подобное оно имеет место, «зародышевый» лимфоцит уничтожается, ведь в противном случае он будет бороться с собственными клетками. Иными словами, благодаря негативной селекции создаются «шаблоны», соответствующие телам, которые внутри организма отсутствуют, и если какое-то тело подходит под данный шаблон, значит, оно явно чужое. Если лимфоцит начинает бороться с собственными клетками, то у человека происходит аутоиммунная реакция и организм начинает уничтожать сам себя.

В случае обнаружения лимфоцитами инородного тела на основании соответствующего шаблона вырабатываются антитела, которые и уничтожают его. Здесь задействуется еще один процесс — клональная селекция, во время которой происходит своеобразный естественный отбор антител: выживают лишь те, которые максимально подходят под найденное инородное тело. При этом сведения о сгенерированных антителах «заносятся» в упоминавшуюся выше генную библиотеку. Таким образом, генная база данных содержит только ту информацию, которая лучше всего позволяет бороться с угрозой.

Выделим необходимые нам основные особенности иммунной системы человека:

· Распределенность — у иммунной системы нет координирующих узлов.

· Самоорганизация — происходит постоянное расширение генной библиотеки, адаптация процесса репродукции лимфоцитов в зависимости от внешних факторов.

[1] Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы.

· Высокая степень параллелизма — компоненты иммунной системы работают самостоятельно и параллельно друг другу.

Аналогичная система защиты распределенных вычислений, основанная на искусственной иммунной системе, представляется весьма подходящим решением для противодействия вредоносному коду в среде, объединяющей географически распределенные и не имеющие единого владельца ресурсы.

Рассмотрим общий принцип работы системы защиты среды распределенных вычислений на основе искусственных иммунных систем.

Каждый вычислительный узел распределенной сети содержит базу данных, хранящую «шаблоны» вредоносных объектов и «шаблоны» вероятных чужеродных объектов. Эта база является распределенной, на каждом узле хранится только часть «шаблонов» вероятных чужеродных объектов, причем периодически производится обмен этими «шаблонами» между узлами.

При обнаружении вредоносного программного обеспечения сработавший «шаблон» копируется в базы всех узлов. Принципиальная схема работы такой системы представлена на рис. 1.

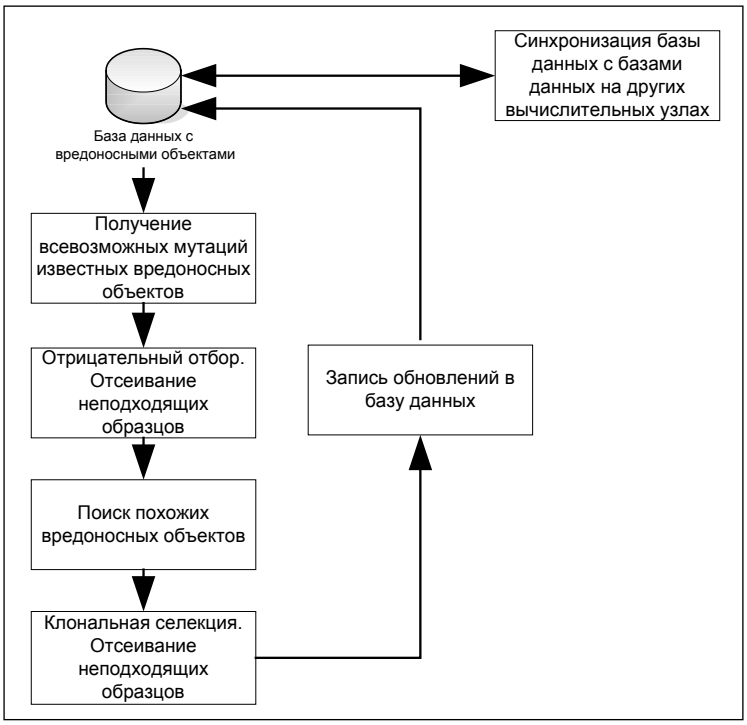

Рис. 1. Принципиальная схема работы системы защиты среды распределенных вычислений

При обнаружении какого-либо инородного тела оно изолируется в среде, где происходит его изучение. На примере вирусов — это модификация одного и того же вируса. Этот процесс позволяет понять принципы защиты не только от найденного объекта, но и от его производных. После этого производится отрицательный отбор, в процессе которого отсеиваются неподходящие образцы антител. Отрицательный отбор необходим для того, чтобы система защиты не реагировала на защищаемую систему как на вредоносный объект (аутоиммунная реакция).

Далее новые антитела осуществляют поиск вредоносных объектов в системе. В случае обнаружения происходит процесс клональной селекции и запись полученных данных в базу.

Рассмотрим преимущества и недостатки систем защиты на основе искусственной иммунной системы.

Преимущества:

· Наличие большого числа детекторов приводит к отказоустойчивости и надежности системы. Отсутствует единая точка отказа.

· При увеличении количества узлов среды распределенных вычислений в предложенной системе повышается уровень защищенности.

· Все столкновения детекторов с вредоносными объектами заносятся в память. Это позволяет проводить обучение детекторов.

Недостатки:

· Возможна аутоиммунная реакция.

· Возможен иммунодефицит, особенно при малом количестве узлов среды распределенных вычислений.

В отличие от многих применяемых на данный момент систем защиты, предложенная выше не имеет центральной подсистемы управления, является децентрализованной высокопараллельной распределенной системой обработки и анализа информации, что делает ее особенно удобной для защиты сред распределенных вычислений. На данный момент ведутся работы над прототипом системы защиты, построенной по предложенной схеме.

Изложенные результаты получены в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Фостер Я.* Что такое Грид. URL: http://www.gridclub.ru/library/publication.2004-11-29.5830756248.
2. *Гвозденко А.* Искусственные иммунные системы как средство сетевой самозащиты. URL: http://itc.ua/node/4270.
3. Искусственные иммунные системы и их применение. URL: http://www.michaelmoorelies.com/page12.htm.