А. В. Моисеев, А. А. Станкевичус, Ю. М. Туманов

ЗАЩИТА СРЕДЫ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ ПРИ ПОМОЩИ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ[1]

Современное общество переходит из постиндустриального в информационное, что сопровождается увеличением как роли информации в жизни общества, так и ростом количества различных средств вычислительной техники (СВТ), соответствующего программного обеспечения (ПО), а также областей их применения. Согласно [1], данный процесс сопровождается увеличением количества ПО, несущего в себе различные ошибки и уязвимости. Кроме того, стоит отметь увеличение инцидентов совершения различного рода атак, основанных на вредоносном программном обеспечении и на неправомерном использовании аппаратного и программного обеспечения.

В статье изложены основные результаты исследований, связанных с построением системы защиты среды распределенных вычислений (СРВ) и, в частности, применением искусственных иммунных систем (ИИС) для защиты сред распределенных вычислений. Предлагаемая в статье архитектура системы предполагает применение ИИС для решения следующих задач:

- обнаружение вредоносного ПО;
- выявление аномалий в сетевом трафике;
- выявление аномалий в работе ПО.

Основным преимуществом СЗИ, предлагаемой в рамках работы, является адаптивность системы защиты и, как следствие, возможность предотвращать новые, ранее неизвестные атаки.

Рассматриваемая среда распределенных вычислений. СРВ является произвольной совокупностью СВТ, осуществляющих взаимодействие между элементами совокупности и направленных на решение одной или нескольких прикладных задач [2].

Одним из распространенных видов СРВ являются так называемые Грид-сети, которые обычно используются для обеспечения распределенных вычислений в фиксированной среде с заданной конфигурацией.

В современном представлении, в соответствии с [3], развитие получают так называемые мобильные Грид-сети, которые обладают следующими особенностями по сравнению с их «классической» реализацией:

- имеют динамическую топологию, возникающую из-за перемещения как пользователей, так и ресурсов Грид-сети;
- узлы мобильных Грид-сетей имеют гетерогенную структуру, т. е. обладают различными вычислительными способностями, в том числе пропускной способностью каналов связи;
- присутствует свойство непостоянности работы отдельных узлов сети.

Данные обстоятельства негативно сказываются как на построении и управлении такими сетями, так и, согласно [2], на обеспечении безопасности данного класса Грид-сетей в целом, что делает задачу построения соответствующей системы защиты крайне актуальной.

Анализ нарушителя. Разработка системы производилась исходя из совокупности предположений о возможностях нарушителя. В работе рассмотрено два вида нарушителей:

- внутренний нарушитель, который является участником СРВ;
- внешний нарушитель, который не принимает непосредственного участия в работе СРВ.

[1] Данная работа выполнена в ходе НИР «Применение искусственной иммунной системы для защиты среды распределенных вычислений», заданной Государственным контрактом № П1314 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

Схематическое расположение данных видов нарушителей представлено на рис. 1.

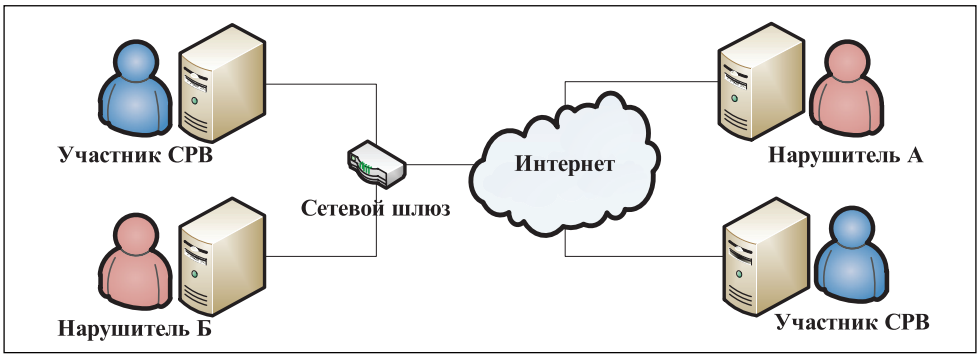

Рис. 1. Схематическое расположение нарушителей СРВ

На рис. 1 внешний нарушитель обозначен как «Нарушитель А», а внутренний нарушитель как «Нарушитель Б».

Внешний нарушитель обладает следующими возможностями:

- подключение к сегменту сети, в котором располагаются участники СРВ;
- проведение удаленных атак на участников СРВ, за исключением атак, направленных на прослушивание и компрометацию сетевого трафика, которым обмениваются участники СРВ.

Внутренний нарушитель обладает всеми возможностями внешнего нарушителя, кроме того, он может участвовать в обмене информацией между участниками СРВ, будучи непосредственным участником СРВ, но не обладает никакими привилегиями по отношению к остальным участникам СРВ.

При этом нарушитель не может оказывать одновременное воздействие на всех участников СРВ с помощью перечисленных выше возможностей, а также осуществлять воздействие на каналообразующее оборудование СРВ.

Целью нарушителя является нарушение работоспособности всей СРВ, которая может быть достигнута посредством нарушения функционирования всех участников СРВ.

Архитектура безопасной среды распределенных вычислений. В данной статье описывается применение искусственных иммунных систем для обеспечения СРВ типа Грид. Подход к защите СРВ, основанный на ИИС, позволяет эффективно защитить данные, обрабатываемые в среде распределенных вычислений, от следующих угроз:

- угроза атаки на СРВ из внешней сети;
- угроза внедрения в СРВ вредоносного программного обеспечения;
- угроза внедрения в клиентские части СРВ недокументированных функций.

На рис. 2 представлена архитектура разработанной безопасной среды распределенной вычислений, обладающей механизмами защиты от вредоносного программного обеспечения, основанными на искусственных иммунных системах.

Представленная архитектура состоит из следующих основных компонентов:

- компонент анализа сетевого трафика;
- компонент защиты от ВПО;
- компонент анализа поведения ПО;
- компонент восстановления;
- журнал.

База данных сигнатур, в свою очередь, также является составным компонентом, включающим в себя следующие логические данные:

- совокупность легитимного ПО, сетевого трафика и нормального поведения ПО, необходимая для работы модифицированного алгоритма отрицательного отбора;

- сигнатуры ИИС, компонента анализа сетевого трафика, компонента защиты от ВПО, компонента анализа поведения ПО.

Все компоненты системы направлены на противодействие различным видам компьютерных атак, кроме журнала, в который происходит запись результатов работы всех элементов системы ЗИ РВС, а также базы данных сигнатур.

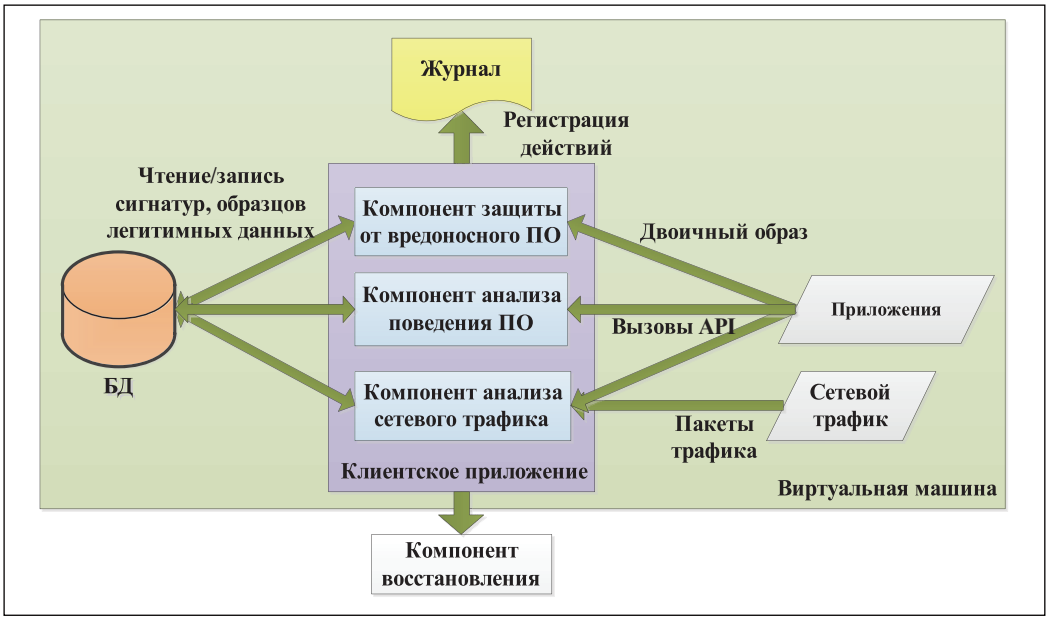

Рис. 2. Архитектура безопасной среды РВ

В результате проведенных исследований по проблеме обеспечения безопасного функционирования СРВ была разработана архитектура СЗИ, представленная в данной статье. Основным отличием предложенной системы защиты является адаптивность этой системы к новым атакам, а также возможность обучения. В случае применения СЗИ, основанной на принципах функционирования ИИС, становится возможным снизить трудозатраты на интеграцию системы защиты в существующую сетевую инфраструктуру. Кроме того, адаптивность предложенной в работе системы защиты позволит в автоматизированном режиме предотвращать возможность новых атак, так называемых 0-day.

СПИСОК ЛИТЕРАТУРЫ:

1. Обзор ошибок и уязвимостей, встречающихся в программном обеспечении. URL: http://cwe.mitre.org.
2. *Семенов Ю. А.* Протоколы Internet. 2-е изд. М.: Горячая линия–Телеком, 2005.
3. *Кулаков Ю. А., Клименко И. А.* Особенности реализации динамической GRID среды. URL: http://nbuv.gov.ua/PORTAL/natural/Pitu/2009_2/content/archive/87-93.pdf