А. А. Краснопевцев, Ю. М. Туманов

ПРИМЕНЕНИЕ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ ДЛЯ ЗАЩИТЫ СРЕДЫ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ[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) и соответствующего программного обеспечения (ПО). Согласно [1], данный процесс сопровождается ростом количества ПО, несущего в себе различные ошибки и уязвимости, а также ростом угроз, связанных с возможностью эксплуатации подобных ошибок и уязвимостей. Среди методов и способов атак, которым могут подвергаться системы распределенных вычислений, являются следующие:

- сканирование объектов сред распределённых вычислений (СРВ);
- зондирование объектов СРВ;
- отказ в обслуживании;
- заражение вредоносным ПО;
- вмешательство в работу приложений системы.

В статье изложены результаты исследований, связанных с построением системы защиты среды распределенных вычислений, основанных на применении искусственной иммунной системы (ИИС).

В связи с тем, что доступ к некоторым важным системным файлам не всегда может быть получен с правами приложения, участвующего в рамках системы распределенных вычислений, оптимальным решением в данном случае является откат вычислительного узла к стабильному и штатному состоянию [2]. В предлагаемой системе подразумевается, что потери, связанные с временными затратами на повторную обработку данных, достаточно невелики по сравнению с возможными проблемами, которые возникнут в случае компрометации результатов вычислений, в следствии вредоносного воздействия.

Важно отметить, что данные, обрабатываемые в Грид-сетях, передаются по открытым каналам. Кроме того, зачастую участие вычислительных узлов в сети не регламентировано, иными словами, вычислительные узлы могут иметь совершенно различную конфигурацию, ресурсы и т. д.

Нередко для выполнения задач, связанных с распределенными вычислениями в рамках Грид-сети, могут быть задействованы не все вычислительные ресурсы ПЭВМ участника, а некоторая их часть.

Архитектура координатора иммунной сети. Система безопасности Грид-сети состоит из двух основных модулей. Первый — это модуль координатора распределенной сети. Координатор распределенной сети является децентрализованным хранилищем и узлом сообщения другого класса модулей, называемых агентами иммунной сети. В задачи координатора входят функции по обеспечению взаимодействия между агентами сети, генерации сигнатур, контроль целостности системы и общая координация функционирования подсистемы безопасности. Кроме того, в задачи координатора могут входить утилитарные функции, связанные с анализом и контролем базы данных сигнатур. Основные компоненты рассматриваемого модуля следующие:

- хранилище идентификаторов клиентов иммунной сети — отвечает за хранение информации о модулях иммунной сети, об антителах, выработанных модулями иммунной сети, как корректных, так и некорректных, а также за логику работы фагоцитов;

[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 г.

- хранилище сигнатур вредоносного кода — обеспечивает хранение информации о выработанных корректных фагоцитах и предоставление информации о них модулям клиентов иммунной сети;
- модуль распределения сигнатур — отвечает за передачу сигнатур, выработанных различными модулями иммунной сети, в случае подозрения на наличие определенных угроз;
- модуль взаимодействия с координатором распределения заданий — отвечает за анализ конфигурации конкретных СВТ, для которых передаются антитела;
- модуль взаимодействия с модулями иммунной сети — отвечает за передачу данных посредством различных коммуникационных каналов.

Общая архитектура модуля приведена на рис. 1.

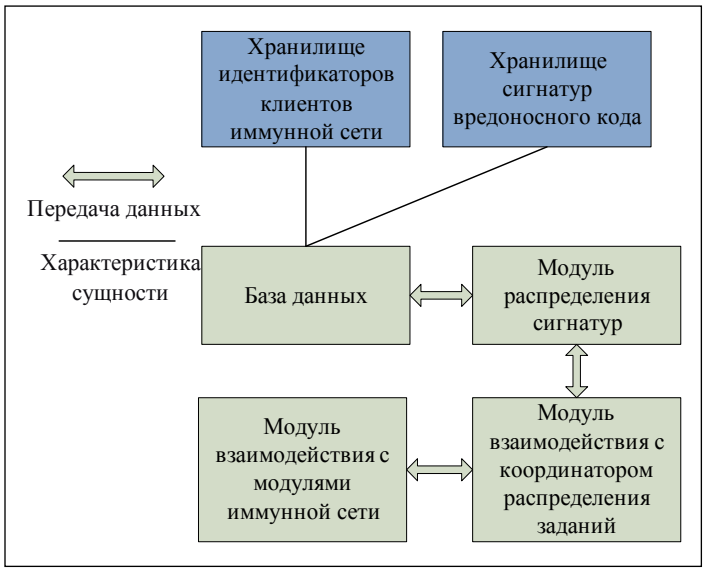

Рис. 1. Архитектура координатора иммунной сети

Модуль иммунной сети. Модуль устанавливается на каждый вычислительный узел сети и обрабатывает информацию, которая поступает от виртуальной среды вычислительного узла и от реальной аппаратной составляющей СВТ. Таким образом, данный элемент системы выступает в роли датчика, который, кроме всего прочего, в зависимости от настроек способен принимать некоторые меры по предотвращению возможных угроз системе распределенных вычислений.

Модуль обработки взаимодействия с подсистемой обработки заданий отвечает за передачу информации и согласование деятельности с координатором иммунной сети.

Модуль взаимодействия с СВТ, на котором осуществляются вычисления, отвечает за взаимодействие с аппаратной платформой, настроенной для взаимодействия с конкретным СВТ.

Модуль обеспечения безопасности СВТ отвечает за защиту СВТ от вредоносного программного обеспечения и деструктивных воздействий. В зависимости от конфигурации и настроек системы безопасности данный модуль может как просто сигнализировать о существующей угрозе, так и пытаться ее устранить.

Модуль обеспечения безопасности виртуальной среды отвечает за блокирование алгоритмов и механизмов, которые могут нарушить целостность, конфиденциальность и доступность среды виртуализации. Кроме того, в задачи данного модуля входит процесс перезапуска виртуальной системы и/или сброса ее состояния. В случае, если система обеспечения безопасности обнаружила новый, ранее неизвестный образец программного обеспечения, имеет смысл перезапустить зараженную виртуальную машину в связи с тем, что без человеческого вмешательства провести полный и детальный анализ вредоносного программного обеспечения не представляется возможным. Как следствие, существует риск того, что результаты вычислений будут скомпрометированы.

Модуль анализа экземпляров ПО осуществляет анализ на основе присутствующих сигнатур ВПО, а также эвристических алгоритмов, с применением которых генерируются фагоциты.

Модуль создания сигнатур отвечает за создание сигнатур вредоносного программного обеспечения после координации с координатором иммунной сети. Полученные сигнатуры после верификации добавляются в базу данных сигнатур вредоносного программного обеспечения.

Модуль верификации корректности сгенерированной сигнатуры отвечает за анализ и верификацию полученных данных относительно конкретного экземпляра ПО. Анализ и верификация осуществляются через координатор иммунной сети, в результате чего в базу данных добавляется либо выработанная сигнатура, либо данные о логике некорректного срабатывания.

Архитектура системы безопасности. В результате проведенных исследований была построена и реализована архитектура системы безопасности Грид-сети, представленная на рис. 2.

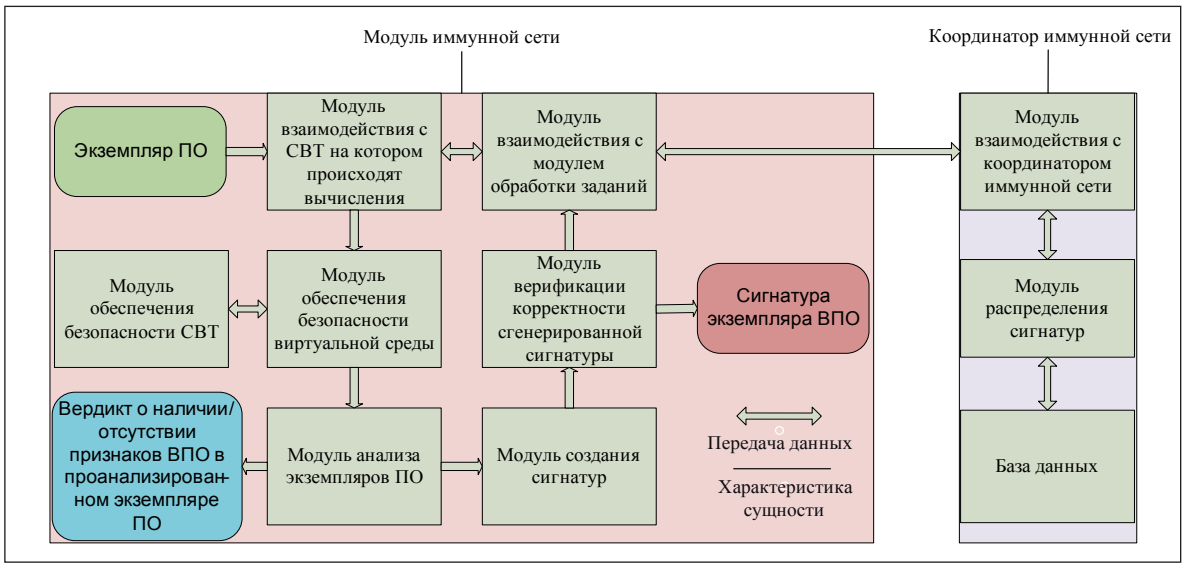

Рис. 2. Архитектура системы безопасности

Стоит отметить, что приведенные на рисунке базовые элементы архитектуры являются масштабируемыми. Такая архитектура продиктована необходимостью обособленного контролирования и обеспечения безопасности каждого отдельного вычислительного узла в сети.

В результате проведенных исследований по проблеме обеспечения безопасного функционирования СРВ была разработана архитектура СЗИ, представленная в данной статье. Основным отличием предложенной системы защиты является ее адаптивность 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. (дата обращения: 12.12.2012)

2. Fuzzy Trust Integration for Security Enforcement in Grid Computing. URL: http://www.springerlink.com/content/63utnfb17dx4yny2/. (дата обращения: 12.12.2012)