На правах рукописи

Степанова Татьяна Владимировна

ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ МНОГОАГЕНТНЫХ СИСТЕМ ЗАЩИТЫ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ РАСПРЕДЕЛЕННЫХ УГРОЗ БЕЗОПАСНОСТИ

Специальность 05.13.19

Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург – 2012

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Санкт-Петербургский государственный политехнический университет»

Научный руководитель:

Зегжда Дмитрий Петрович,
доктор технических наук, профессор

Официальные оппоненты:

Саенко Игорь Борисович,
доктор технических наук, профессор,
ведущий научный сотрудник СПИИРАН

Красов Андрей Владимирович,
кандидат технических наук, доцент, профессор
кафедры ИБТС
Санкт-Петербургского государственного
университета телекоммуникаций им. проф.
М. А. Бонч-Бруевича

Ведущая организация: ФГБОУ ВПО «Петербургский государственный университет путей сообщения»

Защита состоится « » декабря 2012г. в часов на заседании диссертационного совета Д 212.229.27 при ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет» (по адресу 195251, Санкт-Петербург, ул. Политехническая, д.29/1 ауд. 175 главного здания.)

С диссертационной работой можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан « » ноября 2012г.

Ученый секретарь
диссертационного совета

Платонов Владимир Владимирович

Общая характеристика работы

Актуальность темы исследования. Одним из основных средств организации атак в настоящий момент являются бот-сети, объединяющие системы в сети Интернет, находящиеся под управлением вредоносных программ и согласованно осуществляющие деструктивные действия. Современные бот-сети имеют сложную организацию, гибридную или децентрализованную архитектуру, образуют нетривиальные топологии такие как случайные и безмасштабные графы, графы малых миров, а также взаимодействуют друг с другом с целью обмена информацией о применяемых системами защиты методах противодействия. Перечисленные свойства позволяют бот-сетям успешно противостоять системам защиты, использующим традиционный набор средств противодействия таким сетям, что приводит к успешной реализации угроз безопасности компьютерных систем. С усложнением механизмов реализации распределенных угроз, средства защиты также были вынуждены изменить архитектуру на распределенную (антивирусы *Kaspersky Antivirus, ESET NOD32, Panda Antivirus* и др.), но при этом все они используют тривиальную топологию (звезда и звезда из звезд), причем перечисленные средства никак не взаимодействуют между собой и функционируют абсолютно независимо.

Таким образом, и бот-сети, и распределенные системы защиты представляют собой совокупность скоординировано действующих интеллектуальных агентов, т.е. принадлежат к одному классу систем – многоагентным системам (МАС), причем бот-сети превосходят средства защиты по степени согласованности управляющих воздействий, что позволяет им успешно отключать защиту. Следовательно, актуальной проблемой является формирование такой архитектуры и модели управления МАС, которые позволят даже в условиях целенаправленных агрессивных воздействий обеспечить устойчивость функционирования (т. е. сохранить работоспособность) защиты и, как результат, безопасность защищаемых систем.

Степень разработанности темы исследования. Исследованию свойств МАС общего назначения, без учета необходимости выполнения задач защиты, а также исследованию особенностей бот-сетей посвящено множество работ российских и иностранных ученых, таких как И. В. Котенко, В. Б. Тарасов, А.

М. Райгородский, Н. Алон, М. Кришнамурти, И. Ву, Д. Шильяк, П. Эрдёш, А. Реньи, Д. Дейгон. В данных работах предложены модели оценки устойчивости функционирования МАС и степени ее деградации в результате действия естественных, нецеленаправленных факторов. Эти модели не могут непосредственно применяться для оценки устойчивости функционирования МАС защиты (МАСЗ) не только потому, что не учитывают специфику противоборства в сети Интернет, но также не предполагают минимизацию накладных расходов и не учитывают широкий диапазон изменения числа агентов МАС. Также следует отметить, что существующие подходы обеспечивают устойчивость через избыточность, что ведет к значительному увеличению накладных расходов. Таким образом, имеющиеся подходы должны быть адаптированы для оценки устойчивости функционирования МАС как противостоящих распределенным угрозам безопасности в сети Интернет, так и реализующих такие угрозы (МАСУ), с учетом факторов, специфических для противоборства МАС в сети Интернет.

Целью работы является обеспечение устойчивости функционирования МАСЗ в условиях воздействия распределенных угроз безопасности в сети Интернет с помощью поддержания связности сети агентов. Для достижения поставленной цели в работе решались следующие задачи:

1. Исследование современных систем защиты, противостоящих распределенным угрозам безопасности в сети Интернет и систем, реализующих такие угрозы.

2. Разработка критериев оценки устойчивости функционирования МАС, позволяющих оценить связность графа агентов относительно управляющих центров (управляемость), влияние агрессивных воздействий (отказоустойчивость), а также затраты ресурсов на обеспечение связности (константность функционирования) при увеличении и уменьшении числа агентов (масштабируемость).

3. Построение конечно-автоматной модели агента, обеспечивающей устойчивость функционирования МАСЗ за счет изменения ее структуры.

4. Разработка имитационной модели, позволяющей оценивать значения критериев управляемости, отказоустойчивости, масштабируемости и константности функционирования для МАС с различными топологиями и для различных агрессивных воздействий.

5. Проведение имитационного моделирования с целью оценки устойчивости функционирования МАСЗ, построенной на основе разработанной конечно-автоматной модели.

Научная новизна диссертационной работы состоит в следующем:

– формализована задача обеспечения устойчивости функционирования МАС;

– сформулированы критерии оценки устойчивости функционирования МАС в виде показателей управляемости, отказоустойчивости, константности функционирования и масштабируемости;

– предложены аналитические оценки управляемости и отказоустойчивости для d-регулярных графов, основанные на доказанной в работе теореме о свойствах регулярных графов и графов с разреженной асимптотической последовательностью степеней;

– разработана конечно-автоматная модель агента МАСЗ, позволяющая поддерживать регулярность графа агентов в агрессивной среде;

– создана имитационная модель, позволяющая оценивать устойчивость функционирования МАСЗ мощностью до 10000 узлов в условиях воздействия распределенных угроз безопасности;

– проведено имитационное моделирование, позволившее определить пределы устойчивости функционирования системы, построенной на основе разработанной конечно-автоматной модели агента, и сравнить полученные значения с результатами для систем с топологиями звезды и случайного графа Эрдеша-Реньи.

Теоретическая и практическая значимость работы. Полученные теоретические и экспериментальные результаты, а также разработанное ПО, реализующее имитационную модель МАС, могут быть использованы при построении и оценке МАСЗ, устойчивых к целенаправленному воздействию распределенных угроз в сети Интернет. Теоретические и экспериментальные результаты работы используются для подготовки специалистов в области защиты вычислительных систем по дисциплине "Теоретические основы компьютерной безопасности" в ФГБОУ ВПО "СПбГПУ", а также использованы в НИР "Разработка технологии эффективного управления программно-конфигурируемыми сетями" (шифр 2012-1.4-07-514-0021-025) по государственному контракту от 14 июня 2012 г. № 07.514.11.4151, при

проведении работ по оценке эффективности и последующей оптимизации распределенной системы защиты в ФГБОУ ВПО "ГУАП", внедрены в практику деятельности ФГАУ ГНИИ ИТТ "Информика" в виде методики оценки эффективности функционирования используемых средств защиты и практических рекомендаций по защите от распределенных угроз, что подтверждается соответствующими актами об использовании.

Методология и методы исследования. Для решения поставленных задач использовались системный анализ, теория алгоритмов, теория графов, теория перколяций, теория сложных сетей, теория вычислений, методы математического моделирования, математической статистики, математической логики и теории конечных автоматов.

Положения, выносимые на защиту:

1. Формальная постановка задачи обеспечения устойчивости функционирования МАС.
2. Критерии оценки устойчивости функционирования МАС.
3. Конечно-автоматная модель агента, обеспечивающая устойчивость функционирования МАСЗ за счет изменения ее структуры.
4. Имитационная модель, позволяющая оценивать устойчивость функционирования МАСЗ.
5. Полученные в результате имитационных испытаний оценки устойчивости функционирования МАСЗ, построенной на основе разработанной конечно-автоматной модели.

Степень достоверности научных положений диссертации определяется строгим теоретическим обоснованием предлагаемого аналитического аппарата и эффективностью его использования при практическом воплощении.

Апробация результатов работы. Основные теоретические и практические результаты диссертационной работы доложены и обсуждены: на Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России (ИБРР)" (Институт информатики и автоматизации РАН, 2011 г.), на XII Международной научно-практической конференции "Информационная безопасность-2012" (Томский государственный университет систем управления и радиоэлектроники, 2012 г.), 21-ой научно-техническая конференции "Методы и технические средства обеспечения безопасности информации" (СПбГПУ, 2012 г.), всероссийской научно-практической

интернет-конференции с международным участием "Современные экономические информационные системы: актуальные вопросы организации, методы и технологии защиты информации" (МОСИ, 2012 г.), 6-ой международной конференции "Математические методы, модели и архитектуры для защиты компьютерных сетей" (СПИИРАН, 2012 г.). Работа представлена к присуждению премии правительства Санкт-Петербурга победителям конкурса грантов для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга.

Публикации. По теме диссертации опубликовано 9 научных работ.

Объем и структура. Диссертация состоит из введения, четырех глав, заключения и списка литературы из 70 наименований.

Основное содержание работы

Во введении сформулирована и обоснована задача обеспечения устойчивости функционирования МАСЗ.

В первой главе представлены результаты анализа современных систем защиты, противостоящих распределенным угрозам в сети Интернет и систем, реализующих такие угрозы.

Число зараженных компьютеров, подключенных к сети Интернет и формирующих бот-сети, исчисляется миллионами и продолжает расти. В течение нескольких лет отдельные бот-сети нейтрализуются, но появляются новые, или новые версии старых. Например, бот-сеть Win32.Rmnet.12 в начале октября 2012 г. преодолела по числу зараженных ПК 5-миллионную отметку, а к концу месяца достигла размера в 5,5 миллионов инфицированных рабочих станций.

Топология графа агентов МАС определяет ее макрохарактеристики, в том числе наличие путей между УЦ и рядовыми узлами, степень влияния отдельного узла на состояние системы в целом, а также объем ресурсов на поддержание связности. Базовыми параметрами, определяющими эффективность топологии, являются связность графа в условиях удаления узлов и ребер, и избыточность числа связей. В работе приведен анализ топологических и функциональных свойств современных средств защиты и бот-сетей. Основные топологии, характерные для современных МАСЗ – это

звезда и звезда из звезд (например, *Kaspersky Security Network, ESET Live Grid, Panda Cloud Antivirus*); характерные для МАСУ – граф малых миров (например, бот-сеть *Zindos*), случайный граф Эрдеша-Реньи, безмасштабный граф (например, бот-сеть *Nugache*) (рисунок 1). Системы защиты не обеспечивают связность, что является причиной их уязвимости для МАСУ. Бот-сети обеспечивают связность графа агентов через избыточность числа связей. Существующие средства защиты используют распределенность, в основном, при взаимодействии агентов и УЦ (в частности, центров обновления): агенты установлены на каждом рядовом узле и связаны с УЦ: передают ему используемые настройки (контрольные суммы исполняемых файлов, используемые системные вызовы и т.д.), а также получают актуальную информацию об угрозах и уязвимостях. В бот-сетях удаление вершины или ребра в графе агентов не влияет на способность других агентов взаимодействовать друг с другом и выполнять полный набор требуемых функций. В существующих средствах защиты удаление вершины (например, агента обновления) или ребра в графе агентов существенно снижают функционал системы: снижается актуальность имеющейся информации об угрозах и уязвимостях, исчезает возможность ее обновления, что увеличивает вероятность успеха распределенных атак, организованных бот-сетями (рисунок 1).

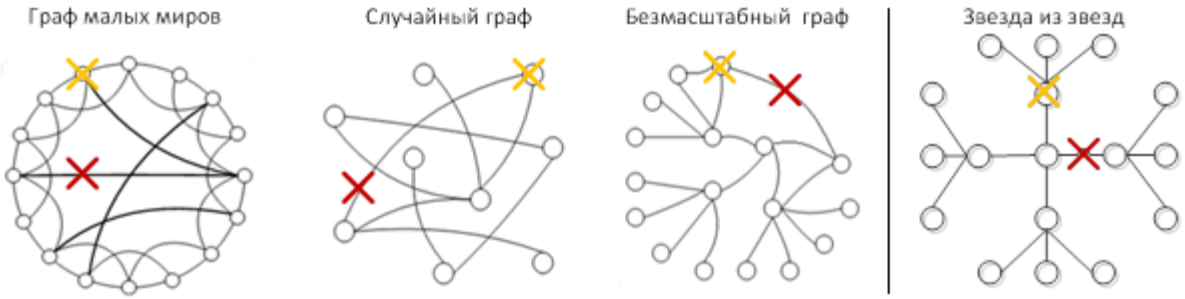

Рисунок 1 – Топологии современных многоагентных систем

Сравнение МАСЗ и МАСУ представлено в таблице 1.

Таблица 1. Сравнение МАСЗ и МАСУ

Признак сравнения	**МАСЗ**	**МАСУ**
Архитектура	Централизованная или гибридная	Гибридная или децентрализованная
Количество УЦ	< 10	≈100
Различия в функциональном назначении узлов	Гетерогенная система	Гомогенная система
Критичность удаления вершины/ребра	Высокая	Низкая
Поддержание связности графа агентов	Нет	Есть
Возможность увеличения числа избыточных связей	Отсутствует	Присутствует

В работе обоснована непригодность для МАСЗ подходов, применяемых в бот-сетях, вследствие неоправданного роста затрат ресурсов и радикального влияния состояния каждого узла на устойчивость системы. Чтобы этого избежать, необходимо сократить число ребер, инцидентных каждой вершине, при этом сохранив высокие показатели связности графа агентов с учетом длины пути до УЦ. Для решения данной задачи с учетом реальных условий противостояния в сети Интернет предлагается ограничиться малым числом связей для каждой вершины, но при этом использовать методы восстановления нарушенных связей. Проведенный в работе анализ позволил формализовать требования к устойчивой МАС и определить характеристики, необходимые для поддержания устойчивости функционирования в условиях агрессивных воздействий.

Таким образом, основной задачей, решаемой перечисленными средствами является задача обеспечения устойчивости функционирования МАС в агрессивной среде, которая может быть формализована следующим образом. Для МАС, заданной кортежем $MAS = (G, ENV, ACT, COM, EV)$, граф агентов $G = (V, E)$ описывается множеством вершин-агентов V, обладающих набором индивидуальных функций ACT, включая коммуникативные функции COM и эволюционный оператор EV, и множеством ребер-соединений E. Агрессивная среда ENV формируется системой-противником и учитывается как вероятность удаления вершин или ребер графа агентов. На устойчивость функционирования оказывают влияние как функциональные, так и топологические характеристики системы.

Во второй главе предложены критерии оценки устойчивости функционирования МАСЗ в условиях воздействия распределенных угроз безопасности в сети Интернет.

В работе предлагается описывать устойчивость функционирования с помощью кортежа $S = (CT_{\text{P}}(t), R_{max},\ Op_{\text{P}},\ Sc_{\text{P}})$. Далее представлен список с описанием всех критериев.

1. Управляемость $CT_P(t)$ – это доля узлов МАС, связанных с УЦ путем длины $\leq t$, задаваемая через вероятность наличия пути длины $\leq t$ от произвольно взятого узла до УЦ, и зависящая от значений параметров P конкретной МАС. За единицу измерения времени принимается время передачи сообщения между соседними узлами, тогда путь длины t соответствует передаче сообщения за время t.

$$CT_P(t) = \begin{cases} \frac{\sum_{i=1}^{N} path\_num\_t_i}{\sum_{i=1}^{N} path\_num_i}, \text{если } \sum_{i=1}^{N} path\_num_i > 0, \\ 0, \text{если } \sum_{i=1}^{N} path\_num_i = 0, \end{cases}$$

где N – общее число узлов, $path\_num_i$ – число путей между узлом и УЦ, $path\_num\_t_i$ – число путей между узлом и УЦ длины $\leq t$. В общем случае управляемость вычисляется эвристически с использованием методов построения альтернативных графов. В работе получены нижняя и верхняя границы управляемости для d-регулярного графа (Теорема 1).

Теорема 1. Для МАС, граф агентов которой имеет топологию случайного d-регулярного графа, управляемость лежит в следующих пределах: $1 - (1 - S_t^{Norm}/n)^{CC} \leq CT_P(t) \leq 1 - (1 - (S_t + 1)/n)^{CC}$, где CC – число УЦ, S_t – сумма первых t членов геометрической прогрессии $b_t = b_1 q^{t-1},\ b_1 = d,\ q = d - 1,\ S_t^{Norm}$ – сумма первых t членов геометрической прогрессии с переменным знаменателем: $b_t^{Norm} = b_0^{Norm} \cdot \prod_{i=1}^{t-1} q_i,\quad b_0^{Norm} = d,\quad q_i^{Norm} = (d-1)\left(1 - p_i^{new_{virt}}\right)$, где $p_i^{new\_virt}$ – это вероятность того, что вершина на i-ом ярусе является "виртуальной", притом, что родительская вершина не является "виртуальной", n – общее число вершин.

Доказательство теоремы основано на оценке числа узлов случайного регулярного графа, длина пути до которых от случайно выбранного узла $\leq t$. При этом в работе предложен подход к представлению регулярного графа в

виде дерева с "виртуальными" вершинами, что позволяет применить к регулярному графу методы вычисления числа вершин на определенном ярусе, используемые для дерева. Данное утверждение выражается леммой 1.

Лемма 1. "Виртуальная" вершина на *i*-ом ярусе может являться копией вершин только с ярусов *i*-2, *i*-1, *i*, если родительская вершина не «виртуальная» (обычная).

Доказательство леммы основано на представлении подграфа регулярного графа в ярусно-параллельной форме в виде регулярного дерева, в котором для каждой вершины регулярного графа, связанной с вершинами того же яруса или порожденной несколькими родительскими вершинами, создается копия – "виртуальная вершина", а недопустимая связь удаляется (рисунок 2).

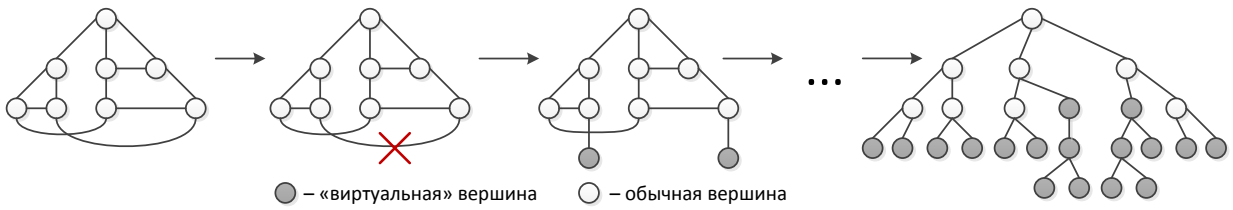

Рисунок 2 – Представление 3-регулярного графа в виде регулярного дерева с "виртуальными" вершинами

2. Отказоустойчивость R_{max} – определяет степень критического деструктивного воздействия на систему, при котором доля узлов МАС, связанных с УЦ путем длины $\leq t$, где t фиксировано, $CR_P(R)$, стремится к нулю. Отказоустойчивость позволяет оценить зависимость доли управляемых узлов МАС от внешних вредоносных воздействий: удаления вершин или ребер графа агентов, и является адаптацией понятия критической вероятности в теории перколяций для рассматриваемых МАС. Т.е., $\lim_{R \to R_{max}} CR_P(R) = 0,\ 0 \leq R \leq R_{max}$. Верхней оценкой отказоустойчивости служат, в соответствии с главой 1, соответствующие критические вероятности удаления вершин и ребер. Данная оценка вычисляется в соответствии с теоремой о критической вероятности для графа, имеющего разреженную асимптотическую последовательность степеней.

3. Константность функционирования Op_P определяется уровнем необходимого изменения объема затрачиваемых в единицу времени ресурсов *V(R)* при изменении величины деструктивного воздействия: $Op_P = \frac{\partial V}{\partial R}$. В

качестве затрачиваемых ресурсов в работе рассматривается объем обрабатываемого агентом служебного трафика, не относящегося непосредственно к решению его задачи. Данный критерий отражает уровень избыточности связей в графе агентов и оценивает эффективность методов восстановления узлов и ребер. Так как агенты установлены в том числе и на компьютерах защищаемой сети и используют ее ресурсы, они не должны оказывать существенного влияния на работоспособность защищаемой системы, включая период восстановления узлов и ребер. Не должно наблюдаться лавинообразного роста трафика в случае удаления небольшой доли узлов МАС.

4. Масштабируемость $Sc_P = Sc_P[k, n]$ – мера разброса управляемости, отказоустойчивости и константности функционирования для МАС мощностью от k до n узлов: $Sc_P[k, n] = (\Delta CT_P(t), \Delta R_{max}, \Delta Op_P)$. Так как функционирование МАС рассматривается в динамике, то она должна быть устойчивой на протяжении всего процесса функционирования, что и отражает данный критерий. Мощность рассматриваемой МАС колеблется в заданных пределах.

Все четыре приведенных критерия описывают функционирование МАС в условиях агрессивных воздействий и позволяют сопоставить устойчивость функционирования противодействующих МАСЗ и МАСУ. При этом считается, что системы имеют высокие показатели имитостойкости и криптостойкости, и агрессивные воздействия, связанные с нарушением этих свойств, не рассматриваются. Современные МАСЗ уступают бот-сетям по устойчивости функционирования, вследствие чего необходима разработка модели агента МАС, применение которой в существующих системах защиты позволит увеличить устойчивость их функционирования.

В третьей главе построена конечно-автоматная модель агента МАСЗ, противостоящей распределенным угрозам безопасности в сети Интернет. Данная модель определяет динамику изменения структуры МАСЗ и позволяет обеспечить устойчивость функционирования системы защиты.

Разработанные для этой модели алгоритмы, описанные в работе, обеспечивают изменение структуры МАС в ответ на агрессивные воздействия системы-противника за счет периодической проверки функционирования соседних узлов, поддержания узлами заданного числа связей и переназначения УЦ в случае снижения их количества. При снижении числа поддерживаемых связей d узел запрашивает адрес нового "соседа" у узла, находящегося на

некотором расстоянии, которое обозначим как *ReqPath.* Алгоритмы поддержания связности сети обеспечивают сохранение разреженной асимптотической последовательности степеней графа в соответствии с теоремой 2, доказанной в работе.

Теорема 2. Для МАС, построенной на основе разработанной конечно-автоматной модели и обеспечивающей временной интервал восстановления $T_r = 2 \cdot ReqPath$, при условии, что вероятность удаления вершин (ребер) графа агентов меньше критической, верны следующие утверждения.

Утверждение 1. Регулярность графа агентов сохраняется, если временной интервал между событиями удаления вершин (ребер) $T_q \geq T_r$.

Утверждение 2. Асимптотическая последовательность степеней вершин графа агентов останется разреженной, если $T_q < 2 \cdot ReqPath$.

Графы с асимптотической разреженной последовательностью степеней имеют схожие с регулярными графами свойства, для них оценка критической вероятности может быть обобщена в виде $p_c = L'(1)/L''(1)$, где $L(s)$ – порождающая функция степенной последовательности, удовлетворяющая условию $L''(1) > L'(1)$. Это позволяет применить оценки управляемости и отказоустойчивости, полученные в главе 2, к графу агентов МАС, которые описываются разработанной конечно-автоматной моделью. Модель агента (описывает подключение к МАС, отключение от МАС, обработку, назначение и выполнение задачи защиты, поддержание связности сети) формализуется в виде композиции конечных автоматов, имеющих единый вход и выход, данное объединение задается кортежем $M = (Q, \sum, \delta, q_0, F)$. Здесь Q – общее множество состояний, подробное описание которых приведено в работе, начальное состояние q_0 = "*отсутствие соединения*", множество заключительных состояний F пусто. Допустимый входной алфавит $\sum$ включает возможные передаваемые сообщения, граничные состояния счетчиков и статусы узла, задачи и резервирования.

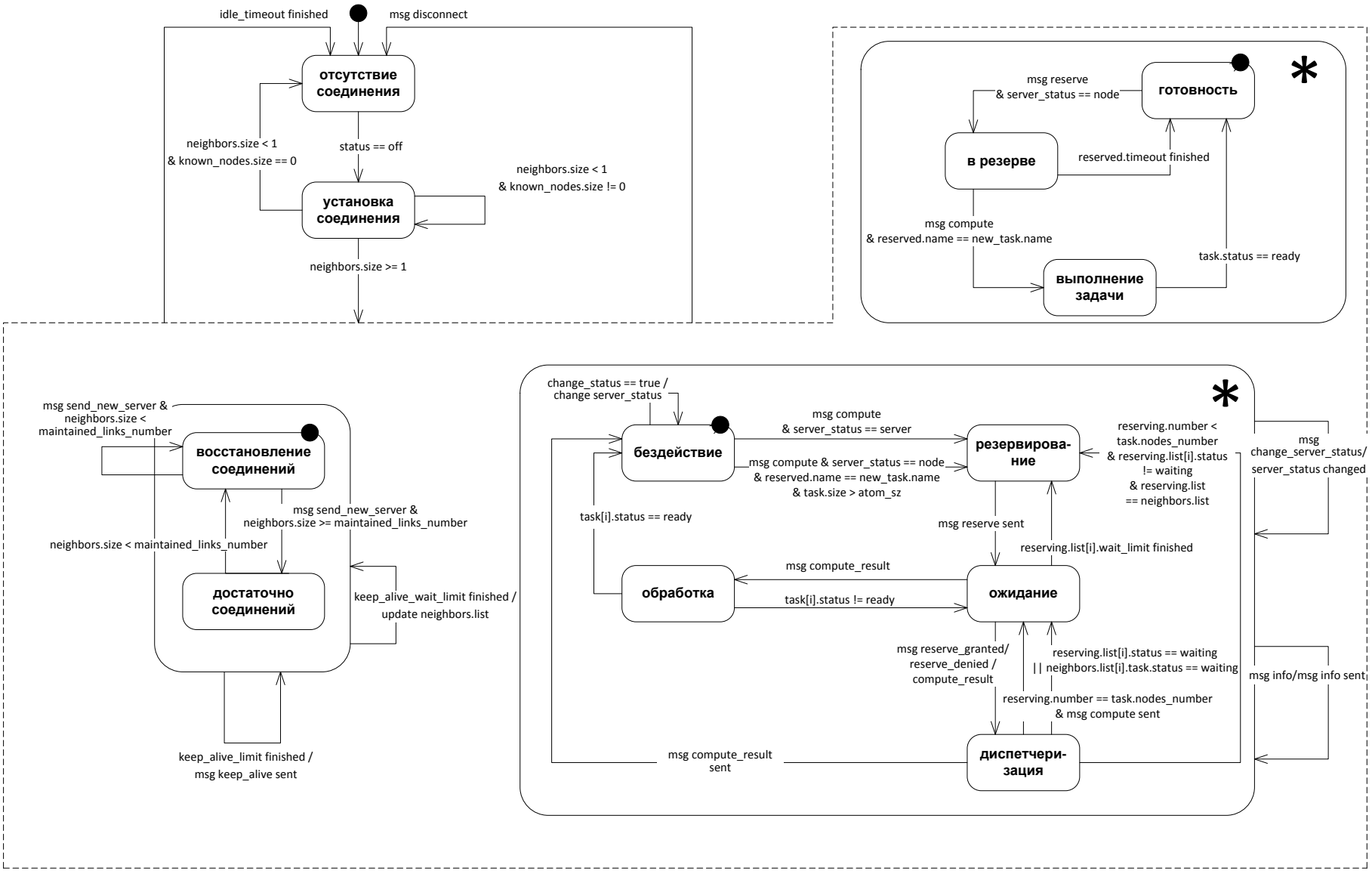

Рисунок 3 – Граф переходов конечно-автоматной модели агента

В конфигурации активных состояний агента в любой момент времени активно одно или несколько состояний. Переход между состояниями инициируется либо полученным сообщением, либо сменой состояния счетчиков и таймеров (например, счетчика проверки статуса соседних узлов). Функция переходов автомата описана графом переходов (рисунок 3). Подсостояния композитных состояний объединены общим контуром (например, *"готовность"*, *"в резерве"*, *"выполнение задачи"*), штрих-контур объединяет параллельные состояния. Входящая стрелка означает возврат в состояние, предшествовавшее смене состояний. Состояния, отмеченные знаком "*", являются множественными композитными, каждое из них описывает процесс обработки одной из задач, назначенных узлу.

В соответствии с теоремой 2, построенная конечно-автоматная модель агента МАСЗ позволяет противодействовать влиянию агрессивной среды и поддерживать управляемость системы в заданных пределах в соответствии с теоремой 1, если агрессивное воздействие не превышает R_{max} и длительность интервала агрессивного воздействия T_q превышает длительность интервала восстановления T_r. Применение предлагаемой модели в существующих системах защиты (рисунок 4) позволит связать в единую систему агенты и УЦ различных средств и, таким образом, повысить актуальность используемой ими информации об угрозах и уязвимостях, и устойчивость функционирования за счет сохранения связности графа агентов и последующего восстановления путей до УЦ.

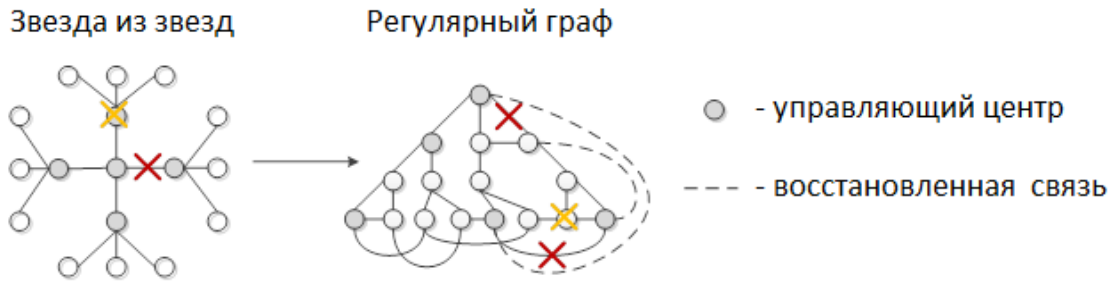

Рисунок 4 – Применение предлагаемого подхода для существующих распределенных систем защиты

В четвертой главе представлены результаты построения имитационной модели МАСЗ, функционирующей в условиях воздействия распределенных угроз безопасности, и результаты имитационного моделирования.

Компоненты имитационной модели задаются кортежем, описанным в главе 1: *MAS = (G, ENV, ACT, COM, EV)*. Входные параметры модели: параметры агрессивной среды *ENV = R* и параметры методов поддержания связности *P* = (*d, ReqPath, CC*). Узлы добавляются и удаляются случайным образом, количество колеблется от 0 (в момент создания сети) до 10 тыс. узлов в процессе ее функционирования. Выходные параметры модели задаются кортежем устойчивости функционирования системы: $S = (CT_{\text{P}}(t), R_{max}, Op_{\text{P}}, Sc_{\text{P}})$. На каждом шаге моделирования работы МАС рассылается широковещательное сообщение и определяется количество узлов, до которых оно доставлено, а также время передачи этого сообщения. По своим временны**ы**м и функциональным параметрам (с точностью до масштабов времени 1:1000) модель является аналогом исследуемого процесса функционирования МАС, которая описывается конечно-автоматной моделью, представленной в главе 3. Функционал конечно-автоматной модели задан алгоритмически и свойства функций (выпуклость, вогнутость, непрерывность и т.п.) неизвестны, поэтому оптимальные значения параметров *d* и *ReqPath* для МАС заданной мощности выбираются на основе решения следующей задачи оптимизации:

$$\begin{cases} CT_P(t) \to max \\ R_{max} \to max \\ Op_P(R) \to min \end{cases}$$

с использованием разработанной имитационной модели для вычисления значений целевых функций. Для МАС мощностью 1000 были получены оптимальные значения *d* = 4 и *ReqPath* = 3, результаты дальнейших испытаний приведены для этих значений. По результатам 10000 проведенных испытаний были получены статистически устойчивые оценки управляемости, отказоустойчивости, константности функционирования и масштабируемости для системы, построенной на основе разработанной конечно-автоматной модели, а также для систем с топологиями звезды (характерна для существующих систем защиты) и классического случайного графа Эрдеша-Реньи (характерна для существующих бот-сетей) (рисунок 5). Изменение

объема накладных расходов аппроксимируется полиномом, взятие первой производной от которого позволяет вычислить константность функционирования.

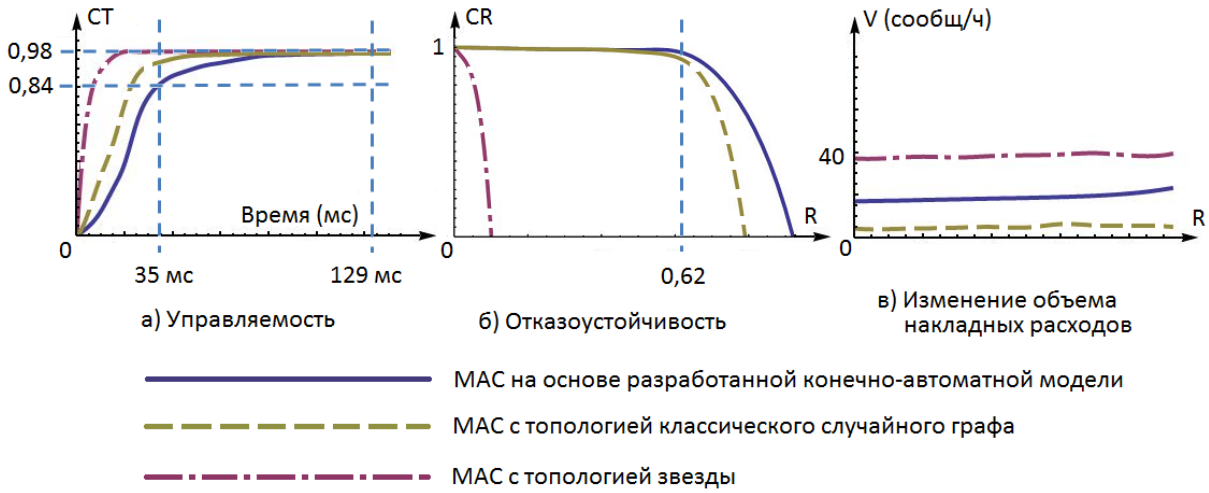

Рисунок 5 – Результаты имитационного моделирования

Таким образом, имитационное моделирование позволило показать, что построение МАС на основе разработанной конечно-автоматной модели агента обеспечит повышение показателей управляемости и отказоустойчивости по сравнению с МАС на основе топологий звезды и классического случайного графа, сохраняя константность функционирования на приемлемом уровне. Причем, этот результат сохраняется при увеличении количества агентов МАС до 10000.

В заключении приведены результаты и выводы, полученные автором в ходе выполнения работы.

Заключение

В работе получены следующие основные результаты:

1. Формализована задача обеспечения устойчивости функционирования МАС.

2. Разработаны критерии оценки устойчивости функционирования МАС, позволяющие оценить связность графа агентов относительно управляющих центров (управляемость), влияние агрессивных воздействий (отказоустойчивость), а также затраты ресурсов на обеспечение связности

(константность функционирования) при увеличении и уменьшении числа агентов (масштабируемость).

3. Построена конечно-автоматная модель агента, обеспечивающая устойчивость функционирования МАСЗ за счет изменения ее структуры.

4. Разработана имитационная модель, позволяющая оценить значения критериев управляемости, отказоустойчивости, масштабируемости и константности функционирования для МАС с различными топологиями и для различных агрессивных воздействий.

5. Получена оценка устойчивости функционирования МАСЗ, построенной на основе разработанной конечно-автоматной модели, а также выбраны оптимальные параметры этой модели.

Перспективы дальнейшей разработки темы диссертации заключаются в применении разработанной конечно-автоматной модели агента МАС для построения единой системы защиты на базе различных существующих средств защиты, а также в разработке критериев оценки методов нейтрализации вредоносных МАС, что, в совокупности с разработанными критериями устойчивости функционирования, позволит предсказать исход противостояния систем защиты и бот-сетей.

Список работ, опубликованных автором по теме диссертации:

1. Степанова, Т. В. Обеспечение устойчивости распределенной системы защиты с помощью адаптивно изменяющейся управляющей структуры на случайном графе [Текст] / Д. П. Зегжда, Т. В. Степанова // Научно-методический журнал "Информатизация образования и науки".— М.: Изд-во ФГУ ГНИИ ИТТ "Информика", 2012.— № 4 (16). — С. 64-73.

2. Степанова, Т. В. Конечно-автоматная модель адаптивного поведения многоагентной системы противодействия распределенным угрозам безопасности в сети Интернет [Текст] / Т. В. Степанова // Журнал "Проблемы информационной безопасности. Компьютерные системы". — СПб.: Изд-во Политехн. ун-та, 2012.— №3. — С. 46-52.

3. Степанова, Т. В. Оценка эффективности использования средств защиты для нейтрализации и устранения бот-сетей [Текст] / Д. П. Зегжда, Т. В. Степанова // Журнал "Проблемы информационной безопасности. Компьютерные системы". — СПб.: Изд-во Политехн. ун-та, 2012.— №2. — С. 21-27.

4. Степанова, Т. В. Stochastic model of interaction between botnets and distributed computer defense systems [Текст] / Д. П. Зегжда, Т. В. Степанова // Сб. материалов Шестой Международной конференции "Математические методы, модели и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2012).— Берлин: Изд-во Springer-Verlag Berlin Heidelberg, 2012.— С. 218-225.

5. Степанова, Т. В. Алгоритмическая модель поведения многоагентной системы обеспечения информационной безопасности в условиях целенаправленного вредоносного воздействия [Текст] / Д. П. Зегжда, Т. В. Степанова // Сб. материалов 21-й научно-технической конференции "Методы и технические средства обеспечения безопасности информации".— СПб.: Изд-во Политехн. ун-та, 2012.— С. 49-52.

6. Степанова, Т. В. Моделирование противостояния бот-сетей и распределенных средств защиты с помощью адаптивных случайных графов [Текст] / Д. П. Зегжда, Т. В. Степанова // Сб. материалов 21-й научно-технической конференции "Методы и технические средства обеспечения безопасности информации".— СПб.: Изд-во Политехн. ун-та, 2012.— С. 52-54.

7. Степанова, Т. В. Оценка устойчивости функционирования многоагентных систем защиты с применением нового метода представления регулярных графов [Текст] / Д. П. Зегжда, Т. В. Степанова // Сб. статей по материалам Всероссийской научно-практической интернет-конференции с международным участием "Современные экономические информационные системы: актуальные вопросы организации, методы и технологии защиты информации".— Йошкар-Ола: Изд-во МОСИ – ООО "СТРИНГ", 2012.— С. 37-41.

8. Степанова, Т. В. Оценка эффективности противостояния средств защиты целевым атакам со стороны бот-сетей [Текст] / Д. П. Зегжда, Т. В. Степанова // Сб. трудов XII Международной научно-практической конференции "Информационная безопасность-2012".— Таганрог: Изд-во ТТИ ЮФУ, 2012.— С. 57-62.

9. Степанова Т. В. Взаимосвязь между действиями пользователя и содержанием исходящего сетевого трафика для обнаружения аномального поведения [Текст] / Т. В. Степанова // Сб. материалов VII Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России".— СПб.: СПОИСУ, 2011.— С.131-132.