МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. Ломоносова
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

На правах рукописи

Гамаюнов Денис Юрьевич

ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ СЕТЕВЫХ ОБЪЕКТОВ

Специальность 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

МОСКВА
2007

Работа выполнена на кафедре Автоматизации систем вычислительных комплексов факультета Вычислительной математики и кибернетики МГУ имени М. В. Ломоносова.

Научный руководитель:	доктор физико-математических наук, профессор, академик РАЕН Смелянский Руслан Леонидович
Официальные оппоненты:	доктор технических наук, заместитель директора НИИ «Квант» Корнеев Виктор Владимирович
	кандидат физико-математических наук, доцент факультета ВМиК МГУ Чернов Александр Владимирович
Ведущая организация:	НИВЦ МГУ имени М. В. Ломоносова

Защита состоится 26 октября 2007 г. в 11:00 на заседании диссертационного совета Д 501.011.44 в Московском государственном университете имени М. В. Ломоносова по адресу: 119991, ГСП-1, Москва, Ленинские горы, МГУ, 2-й учебный корпус, факультет ВМиК, аудитория 685.

С диссертацией можно ознакомиться в библиотеке факультета ВМК МГУ. С текстом автореферата можно ознакомиться на официальном сайте ВМиК МГУ имени М. В. Ломоносова http://www.cmc.msu.ru в разделе «Наука» - «Работа диссертационных советов» - «Д 501.001.44».

Автореферат разослан «_____» _____ 2007 г.

Ученый секретарь
диссертационного совета
профессор Н. П. Трифонов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Компьютерные сети за несколько последних десятилетий из чисто технического решения превратились в глобальное явление, развитие которого оказывает влияние на большинство сфер экономической деятельности. Одним из первых количественную оценку значимости сетей дал Роберт Меткалф, участвовавший в создании Ethernet: по его оценке «значимость» сети во всех смыслах пропорциональна квадрату числа узлов в ней. То есть, зависимость от нормальной работы сетей растёт быстрее, чем сами сети. Обеспечение работоспособности сети и функционирующих в ней информационных систем зависит не только от надёжности аппаратуры, но и, зачастую, от способности сети противостоять целенаправленным воздействиям, которые направлены на нарушение её работы.

Создание информационных систем, гарантированно устойчивых к вредоносным воздействиям и компьютерным атакам, сопряжено с существенными затратами как времени, так и материальных ресурсов. Кроме того, существует известная обратная зависимость между удобством пользования системой и её защищённостью: чем совершеннее системы защиты, тем сложнее пользоваться основным функционалом информационной системы. В 80-е годы XX века, в рамках оборонных проектов США, предпринимались попытки создания распределенных информационных систем специального назначения (MMS – Military Messaging System), для которых формально доказывалась выполнимость основной теоремы безопасности – невыведение системы из безопасного состояния для любой последовательности действий взаимодействующих объектов. В этих системах использовалось специализированное программное обеспечение на всех уровнях, включая системный. Однако, на сегодняшний день подобные системы не получили развития, и для организации информационных систем используются операционные системы общего назначения, такие как ОС семейства Microsoft Windows, GNU/Linux, *BSD и различные клоны SysV UNIX (Solaris, HP-UX, etc).

Из-за высокой сложности и дороговизны разработки защищённых систем by design, тогда же в 80-е годы XX века появилось и начало активно развиваться направление информационной безопасности, связанное с обнаружением (и, возможно, последующим реагированием) нарушений безопасности информационных систем, в качестве эффективного временного решения, позволяющего закрывать «бреши» в безопасности систем до их исправления. Данное направление получило название «обнаружение атак» (intrusion detection); и за прошедшие годы в рамках академических разработок были созданы сотни систем обнаружения атак для различных платформ: от систем класса mainframe до современных операционных систем общего назначения, СУБД и распространённых приложений.

Создание эффективных систем защиты информационных систем сталкивается также с нехваткой вычислительной мощности. С самого начала развития компьютеров и компьютерных сетей наблюдаются две тенденции, называемые законом Мура и законом Гилдера. Закон Мура говорит о ежегодном удвоении производительности вычислителей, доступных за одну и ту же стоимость, а закон Гилдера – об утроении пропускной способности каналов связи за тот же период. Таким образом, рост вычислительной мощности узлов сети отстаёт от роста объёмов передаваемой по сети информации, что с каждым годом ужесточает требования к вычислительной сложности алгоритмов систем защиты информации.

Методы обнаружения атак в современных системах обнаружения атак (далее - СОА) недостаточно проработаны в части формальной модели атаки, и, следовательно, для них достаточно сложно строго оценить такие свойства как вычислительная сложность, корректность, завершимость и т.д. Принято разделять методы обнаружения атак на методы обнаружения аномалий и методы обнаружения злоупотреблений. Ко

второму типу методов относятся большинство современных коммерческих систем (Cisco IPS, ISS RealSecure, NFR) – они используют сигнатурные (экспертные) методы обнаружения. Существует множество академических разработок в области обнаружения аномалий, но в промышленных системах они используются редко и с большой осторожностью, так как такие системы порождают большое количество ложных срабатываний. Для экспертных же систем основной проблемой является низкая, близкая к нулю, эффективность обнаружения неизвестных атак (адаптивность). Низкая адаптивность до сих пор остаётся проблемой, хотя такие достоинства как низкая вычислительная сложность и малая стоимость развёртывания определяют доминирование таких систем в данной области.

Цель работы. Целью данной работы является разработка метода и экспериментальной системы обнаружения атак на РИС на основе наблюдения за поведением объектов РИС, позволяющего объединить достоинства двух подходов – обнаружения аномалий и обнаружения злоупотреблений – при неухудшении показателей эффективности и сложности методов обнаружения злоупотреблений.

Методы исследования. При получении основных результатов диссертации использованы методы теории множеств, теории автоматов и методы анализа поведения программных объектов на основе наблюдения изменения их состояний в процессе взаимодействия.

Основные результаты работы. Основные результаты диссертационной работы заключаются в следующем:

- Построена модель функционирования РИС в условиях воздействия компьютерных атак, в рамках которой задача обнаружения атак сведена к задаче поиска подцепочек в цепочке символов. Данная модель позволила формально оценить вычислительную сложность предложенного в работе метода и показать его корректность.
- Предложен гибридный метод обнаружения атак на основе метода анализа систем переходов состояний, позволяющий обнаруживать неизвестные атаки как отклонения наблюдаемого поведения сетевых объектов от нормального.
- На основе предложенных методов реализована система обнаружения атак для ОС Linux, Windows 2000/XP. Данная экспериментальня система показала высокую эффективность обнаружения на испытательном стенде. Экспериментально показана адаптивность системы к неизвестным атакам.

Предложенный метод обнаружения атак может быть использован для построения систем защиты распределенных вычислительных систем в условиях функционирования в сетях общего доступа, где высока вероятность появления новых реализаций атак. Наибольшая эффективность метода достижима в тех системах, где множество классов объектов (используемых сервисов и программного обеспечения) ограничено и не меняется со временем существенным образом, что позволяет использовать модели нормального поведения для обнаружения атак.

Научная новизна. В настоящей работе предложен метод обнаружения атак на основе наблюдения за поведением взаимодействующих в сети объектов и сопоставления этого поведения с моделями известных атак и нормального поведения объектов в форме конечных автоматов специального вида. Данный метод является адаптивным к модификациям известных атак при сохранении низкой вычислительной сложности обнаружения, устойчивости и верифицируемости, характерных для сигнатурных методов.

Предложена модель функционирования распределенной информационной системы в форме системы состояний составляющих её сетевых объектов и переходов из состояния в состояние при их взаимодействии. Данная модель позволяет определить конкретный вид моделей известных атак и нормального поведения объектов, а также оценить вычислительную сложность метода обнаружения атак.

Теоретическая и практическая ценность. Теоретическая ценность состоит в разработке комплекса алгоритмов, реализующих адаптивный метод обнаружения атак на основе анализа поведения сетевых объектов.

На основе разработанных алгоритмов была спроектирована и реализована экспериментальная система обнаружения атак для сетей общего назначения, построенных на основе стека протоколов TCP/IP и операционных систем семейства Linux и Microsoft Windows 2000/XP. Система опробована на тестовых и реальных примерах компьютерных атак, для которых показана близкая к 100% полнота обнаружения, в том числе модифицированных атак, при низком уровне ложных срабатываний.

Разработанный метод обнаружения атак также применяется в системе обнаружения атак «REDSecure».

Апробация работы. Результаты, представленные в работе, докладывались на объединённом научно-исследовательском семинаре кафедр Автоматизации систем вычислительных комплексов, Системного программирования и Алгоритмических языков факультета ВМК МГУ под руководством профессора М. Р. Шура-Бура, на научных семинарах лаборатории Вычислительных комплексов факультета ВМК МГУ под руководством профессора Р. Л. Смелянского, а также на следующих конференциях:

- Научная конференция «Тихоновские чтения» (Москва, 2005 г.)
- Международные конференции «Интеллектуализация обработки информации» (Украина, Крым, 2004 и 2006 годов).

Публикации. По теме диссертации имеется 5 публикаций, список которых приводится в конце автореферата.

Структура и объём работы. Диссертация состоит из введения, четырёх глав, списка литературы и приложения. Объём работы 88 страниц. Список литературы содержит 113 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение (глава 1) содержит краткий обзор предметной области, актуальность проблемы и неформальную постановку задачи.

Вторая глава работы посвящена обзору и сравнительному анализу близких по тематике методов обнаружения атак и ряда современных систем обнаружения атак. Целью обзора является исследование эффективности доступных в настоящее время систем обнаружения атак и определение основных недостатков используемых в них методов обнаружения атак.

В обзоре рассмотрены следующие методы обнаружения злоупотреблений и аномалий:

- Обнаружение злоупотреблений
  - Анализ систем состояний;
  - Графы атак (верификация на моделях);
  - Нейронные сети;

        - Иммунные сети;
        - SVM;
        - Экспертные системы;
        - Методы, основанные на спецификациях;
        - MARS – Multivariate Adaptive Regression Splines;
        - Сигнатурные методы.
    - Обнаружение аномалий
        - Статистический анализ;
        - Кластерный анализ;
        - Нейронные сети;
        - Иммунные сети;
        - Экспертные системы;
        - Поведенческая биометрия;
        - SVM;
        - Анализ систем состояний.

Из реализаций систем обнаружения атак рассмотрены следующие открытые и свободно распространяемые системы:

- Bro, University of California, Lawrence Berkeley National Laboratory, http://bro-ids.org/
- OSSEC, Daniel B. Sid, http://www.ossec.net/
- STAT, University of California at Santa Barbara, http://www.cs.ucsb.edu/~seclab/projects/stat/index.html
- Snort, Martin Roesch, Sourcefire, http://www.snort.org/

В обзоре показано, что:

1. Большинство современных СОА используют на базовом уровне ту или иную реализацию сигнатурного метода обнаружения (pattern matching, сравнение шаблонов). Реализации отличаются друг от друга уровнем рассмотрения системы, алфавитом сигнатур и используемым «движком» - от простого поиска подстрок до полноценной реализации регулярных выражений над заданным алфавитом.

2. Множество существующих методов обнаружения атак много шире, но их использование в системах имеет принципиальные ограничения, связанные с требованиями верифицируемости, устойчивости и воспроизводимости результата, а также большим числом ошибок второго рода (ложных срабатываний). Использование таких методов ограничено экспериментальными академическими разработками.

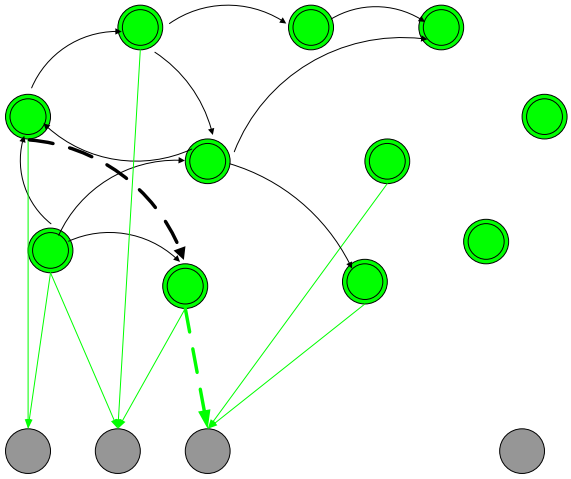
3. Доступные реализации СОА неустойчивы к модификациям атак и не могут автоматически адаптироваться к появлению новых атак. При этом использование методов обнаружения аномалий (например, в препроцессорах СОА Snort) ограничено по причинам, перечисленным в п.2.

Третья глава настоящей работы посвящена формальной модели функционирования РИС, на основе которой обосновывается применимость метода обнаружения атак, основанного на анализе переходов состояний, а также производится оценка вычислительной сложности и доказательство корректности метода.

Особенности формальной модели функционирования РИС:

- функционирование РИС определяется через понятие состояния объекта РИС и переходы между состояниями, объекты типизированы;
- состояния объектов изменяются при выполнении операций доступа от одного объекта к другому, при этом изменяются состояния обоих взаимодействующих объектов;

- множество состояний разделяется на безопасные и опасные состояния. Опасное состояние вводится через нарушение прав доступа при выполнении операций доступа, в том числе транзитивных, и через уровень загруженности объектов;
- в любой момент времени система находится в некотором состоянии, для которого определён граф доступа, в котором вершинами являются объекты РИС, а рёбра соответствуют связям по выполнению операций доступа, в том числе транзитивные:



- вводится понятие траектории и поведения объекта через последовательность операций доступа или последовательность состояний, также показывается эквивалентность представления поведения в виде последовательности операций доступа и последовательности состояний;
- понятие атаки вводится как траектория из безопасного состояния некоторого объекта в опасное.

В терминах данной модели ставится формальная постановка задачи обнаружения атаки:

1. Обнаружение злоупотреблений.

Пусть задано:

- множество примеров атак $X = \{X\}, X^i = x_1^i, x_2^i, ..., x_N^i$ в виде примеров их траекторий;
- последовательность наблюдаемых состояний защищаемой системы $T_{sys} = \theta_1, \theta_2, ..., \theta_N, ...$

Требуется найти множество экземпляров объектов $O^* = \{o\} \subset \Re_C$ и соответствующее им множество траекторий $T^* = \{T_o \mid o \in O^*\}$, которые реализуют атаки из множества примеров атак.

2. Обнаружение аномалий.

Пусть задано:

- множество описаний нормального поведения объектов РИС, определенное в терминах типов объектов $B = \{Bh(Type) \mid Type \in Act \cup Psv, \forall r \in \Re : type(r) = Type, \forall S \in t_r \; S \subset N_r\}$, где Act – множество активных объектов, а Psv – множество пассивных объектов;

- последовательность наблюдаемых состояний защищаемой системы $T_{sys} = \theta_1, \theta_2, ..., \theta_N, ...$

Требуется найти множество экземпляров объектов $O^* = \{o\} \subset \Re_C$ и соответствующее ему множество траекторий $T^* = \{T_o \mid o \in O^*\}$, которые не принадлежат описанию нормального поведения для соответствующих типов объектов РИС.

В качестве решения данной задачи предложен алгоритм построения автоматов первого и второго рода (модель атаки и модель нормального поведения соответственно), и алгоритм обнаружения атак на основе сопоставления наблюдаемого поведения объектов защищаемой системы с ожидаемым в соответствии с моделями.

Формально автомат для каждого класса атак и для нормального поведения некоторого объекта РИС представляет собой структуру следующего вида:

$$K_R^i : (S, P_S, T, P_T, s_0, I, g, q)$$, где

S – множество состояний;
P_S – множество предикатов состояний;
T – множество переходов;
P_T – множество предикатов переходов;
s_0 – начальное состояние;
I – множество экземпляров автомата;
g – глобальное окружение;
q – глобальная очередь таймера.

В диссертации предложен язык описания поведения объектов РИС, позволяющий описывать состояния объектов РИС и переходы между ними. Подробное описание языка приведено в приложении.

В заключительном разделе третьей главы описан алгоритм обнаружения атак на основе обработки трасс наблюдаемых событий от сетевых объектов множеством автоматов первого и второго рода.

Четвёртая глава работы посвящена экспериментальной системе обнаружения атак, в которой реализован предложенный метод, и исследованию её эффективности на испытательном стенде.

Экспериментальная система реализована для сетей общего назначения, построенных на базе стека протоколов TCP/IP и операционных систем семейства Linux и Windows 2000/XP. В состав системы входят следующие модули:

- сетевой сенсор;
- узловой сенсор;
- консоль управления;
- база данных;
- агенты реагирования.

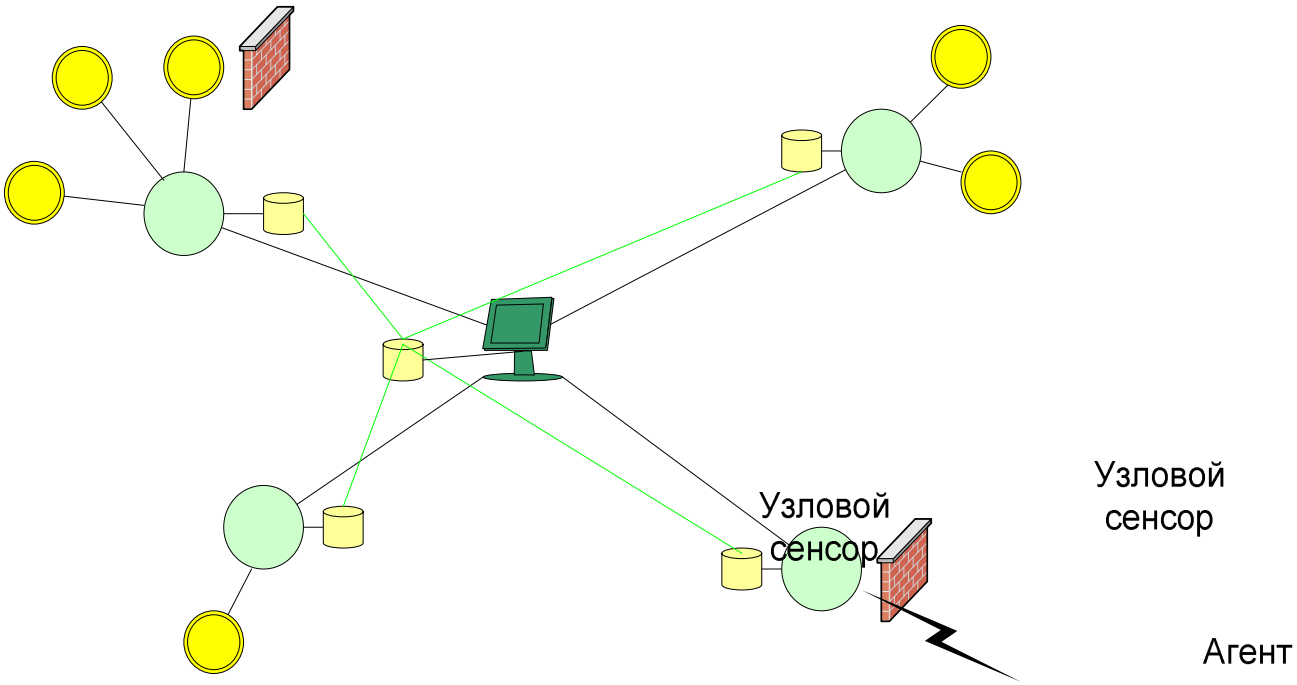


Схема экспериментальной СОА.

Сетевой сенсор. Сетевой сенсор анализирует данные сетевого трафика, выявляет доступ между объектами на разных узлах по некоторому сетевому протоколу, формирует трассу операций доступа между сетевыми объектами для последующего анализа, и выполняет анализ построенной трассы на моделях атак и нормального поведения сетевых объектов. Сетевой сенсор состоит из наблюдателя, который формирует трассу событий на основе декомпозиции сетевого трафика, разбора информации различных протоколов, ядра анализа, которое получает поток событий от наблюдателя, подсистемы реагирования и служебной подсистемы, которая отвечает за управление и взаимодействие между компонентами СОА.

Ядро анализа представляет собой систему поддержки выполнения программ на языке СОА (СПВП) и набор автоматов первого и второго рода, описанных на данном языке. СПВП выполняет функции монитора анализирующих автоматов, формирует очередь выполнения тела переходов и состояний автоматов, планирует порядок выполнения автоматов, порождает и уничтожает экземпляры автоматов. Автоматы по достижении конечного состояния порождают атомарные сообщения об атаках в формате IDMEF.

Подсистема реагирования также состоит из наблюдателя, который получает сообщения об атаках и формирует трассу событий, ядра анализа (СПВП + автоматы), служебной подсистемы. Автоматы реагирования формируют политику реагирования: в конечном состоянии каждого автомата выполняется заданная процедура реагирования. Это может быть разрыв соединения, настройка межсетевого экрана, корреляция сообщений об атаках и формирование более высокоуровневых сообщений.

Служебная подсистема сетевого сенсора отвечает за организацию шифрованного канала между компонентами СОА, сохранение сообщений об атаках и служебных сообщений в базе данных, реализацию функций удаленного управления и настройки сетевого сенсора с консоли управления.

Узловой сенсор. Узловой сенсор предназначен для анализа поведения сетевых объектов РИС на основе данных системных журналов и событий ОС – трассы действий

приложений, пользователей, использования файловой системы и IPC контролируемой рабочей станции или сервера. Узловой сенсор состоит из наблюдателя, который формирует трассу событий, ядра анализа, которое получает поток событий от наблюдателя, и служебной подсистемы, которая отвечает за управление и взаимодействие между компонентами СОА.

На выход узловой сенсор выдаёт сообщения об обнаруженных аномалиях или злоупотреблениях в формате IDMEF. Сообщения пересылаются сетевому сенсору, имеющему соединение с узловым сенсором.

База данных. База данных (БД) СОА представляет собой распределенное хранилище описаний нормального и аномального поведения объектов РИС, сообщений об атаках и журнала компонентов СОА. Данное хранилище используется сетевыми и узловыми сенсорами для централизованной загрузки автоматов в СПВП и хранения сообщений об атаках. База данных построена на основе открытой СУБД PostgreSQL.

Консоль управления. Консоль управления представляет собой графическое приложение управления СОА, в задачи которого входит:

- отображение физической и логической структуры СОА и защищаемой РИС;
- управление и настройка компонентов СОА;
- оповещение оператора о событиях безопасности в режиме рального времени (визуальные и звуковые эффекты);
- корреляция сообщений об атаках;
- централизованное реагирование;
- визуализация сообщений об атаках и журнала компонентов.

Агенты реагирования. Агенты реагирования СОА устанавливаются на узлы РИС, на которых установлены средства реагирования (межсетевые экраны), либо на контролируемые узлы РИС, и выполняют команды от подсистемы реагирования сетевого сенсора и консоли управления. В рамках экспериментальной СОА реализованы следующие агенты:

- агент IPTables для ОС Linux;
- агент для ОС Windows со встроенными возможностями пакетного фильтра и блокирования процессов на узле.

В четвёртой главе показано, что данная реализация экспериментальной системы обнаружения атак удовлетворяет всем критериям сравнения систем данного класса, по которым оценивались системы в главе 2.

В конце главы приведено исследование эффективности экспериментальной системы обнаружения атак. Описан набор тестовых примеров и описание испытательного стенда, на котором проводились эксперименты. В качестве примера автомата второго рода (модели нормального поведения) приведен пример для сервера FTP ProFTPd, на котором демонстрируется свойство адаптивности предложенного в работе метода и его реализации.

Пятая глава содержит описание основных результатов работы, указывает на открытые вопросы построения грамматик для отдельных классов атак, что позволило бы построить оптимальные по сложности алгоримы обнаружения конкретных классов. В пятой главе также сформулированы направления для дальнейших исследований и развития предлагаемого подхода.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Гамаюнов Д. Ю., Смелянский Р. Л., Современные некоммерческие средства обнаружения атак. // Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва, 2002 г.
2. Гамаюнов Д. Ю., Качалин А. И., Обнаружение компьютерных атак как задача распознавания образов. // Материалы пятого Всероссийского симпозиума по прикладной и промышленной математике, Кисловодск, 2004 г.
3. Гамаюнов Д. Ю., Качалин А. И. Обнаружение атак на основе анализа переходов состояний распределенной системы. // Искусственный интеллект, 2004 No 2, с.49-53.
4. Гамаюнов Д. Ю., Качалин А. И., Методика настройки интеллектуальных распознавателей компьютерных атак для работы в корпоративных сетях. // Искусственный интеллект, 2006 No 2, с.30-34.
5. Гамаюнов Д. Ю., Смелянский Р. Л., Модель поведения сетевых объектов в распределенных вычислительных системах. // Журнал «Программирование», 2007, №4.