На правах рукописи

Крупнов Леонид Сергеевич

Математические модели, комплексы программ и алгоритмы принятия решения при возникновении конфликтного взаимодействия компьютерных систем

Специальность:
05.13.18 – «Математическое моделирование, численные методы и комплексы программ»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Рязань – 2015

Работа выполнена в ФГБОУ ВПО
«Рязанский государственный радиотехнический университет»

Научный руководитель - Кириллов Сергей Николаевич
Заслуженный работник Высшей школы РФ,
доктор технических наук, профессор,
заведующий кафедрой Радиоуправления и связи
ФГБОУ ВПО «Рязанский государственный
радиотехнический университет»

Официальные оппоненты - Монахов Михаил Юрьевич
доктор технических наук, профессор, заведующий
кафедрой Информатики и защиты информации,
ФГБОУ ВПО «Владимирский государственный
университет имени А. Г. и Н. Г. Столетовых»,
г. Владимир

- Корнев Павел Александрович
кандидат технических наук, старший
преподаватель учебно-методического отдела
НОЧУ ДПО центр повышения квалификации
«Учебный центр «ИнфоТеКС»,
г. Москва

Ведущая организация - ГКОУ ВПО «Академия Федеральной службы
Охраны Российской Федерации», г. Орел

Защита состоится 17 февраля 2016 года в 12 часов на заседании диссертационного совета Д 212.211.02 в ФГБОУ ВПО «Рязанский государственный радиотехнический университет» по адресу: 390005, г. Рязань, ул. Гагарина, д. 59/1.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Рязанский государственный радиотехнический университет» http://www.rsreu.ru.

Автореферат разослан « » ___ 2015 г.

Ученый секретарь
диссертационного совета
канд. техн. наук, доцент Перепелкин Д.А.

ОБЩАЯ ХАРАКТЕРИСТИКА ДИССЕРТАЦИОННОЙ РАБОТЫ

Актуальность темы. Интенсивное развитие телекоммуникационных технологий приводит к росту числа активов современных предприятий, сосредоточенных в рамках компьютерной системы (КС). В процессе функционирования КС зачастую возникают конфликтные ситуации, связанные непреднамеренными последствиями внутренних сбоев и внешних помех. Значительная роль в решении задач управления КС в конфликтных ситуациях в настоящее время отводится администратору КС. При этом особо сложной задачей является процесс принятия решения о применении адекватного набора механизмов снижения влияния (МСВ) конфликтного взаимодействия (КВ) с внешними КС в случае обнаружения обращений, представляющих угрозу ее нормальному функционированию. На сегодняшний день существует ряд математических моделей оценки работоспособности КС, позволяющих формально решить задачу поиска и уменьшения влияния от определенных классов КВ. Однако каждая из моделей решает, как правило, узкоспециализированные задачи либо ограничена рамками типовых КС, что вынуждает применять их одновременно. Существующие на сегодняшний день подходы к построению обобщенной математической модели системы принятия решений (СПР), способной уменьшить влияние КВ на работоспособность КС, сталкиваются со следующими наиболее актуальными проблемами:

1 Необходимостью получения универсальной численной оценки ущерба в результате КВ, актуального для конкретной КС согласно ее основным задачам. На данный момент указанная проблема частично решается посредством численной оценки целостности активов КС, однако существующие подходы, как правило, ограничены типовой архитектурой рассматриваемых КС или обладают жесткой системой приоритетов важности активов.

2 Необходимостью наличия системы обнаружения и классификации КВ на основании объективных наблюдений за состоянием КС. На данный момент существует множество подходов к обнаружению конфликтных ситуаций, однако ни один из них не позволяет одновременно добиться высоких показателей точности и полноты результатов обнаружения источников КВ.

В КВ КС часто вовлечены комплексы программных средств, что приводит к высокой скорости развития конфликта. Это не позволяет во многих случаях применять автоматизированные системы поддержки принятия решений, не обеспечивающие достаточного быстродействия ввиду влияния человеческого фактора. На данный момент указанная проблема решается применением различных вариантов сигнатурных и эвристических систем обнаружения КВ, способных в автоматическом режиме применять предписанные МСВ для ликвидации последствий КВ. Тем не менее, на сегодняшний день актуальна проблема снижения влияния неизвестных КВ, а также модифицированных КВ, которые обладают отличными от известных КВ характерными признаками, что затрудняет процесс их обнаружения и классификации. Для применения адекватного набора МСВ подобных КВ, необходимо наличие формальной математической модели принятия решений.

Таким образом, актуальны задачи обоснования, разработки и одновременного использования обобщенной математической модели СПР, алгоритмов чис-

ленной оценки ущерба от КВ, реализованных с помощью комплекса программ, в интересах использования полученных данных для обнаружения КВ и принятия решения с целью применении адекватного набора МСВ.

Степень разработанности темы. За весь период формирования различных математических моделей СПР неоднократно предпринимались попытки построения обобщенной математической модели, позволяющей использовать результаты и достижения существующих частных моделей процессов функционирования КС. Среди основных работ в данной области можно выделить труды Хоффмана Л. Д., Аверченкова В. И., Рытова М. Ю., Гайнулина Т. Р., Домарева В. В., Гужвы Д. Ю., Овсянникова Ю. В., Саенко И. Б. Полученные в результате обобщенные математические модели позволяли рассматривать широкий спектр КВ и КС, а также формализовать процесс применения МСВ, однако оставляли открытым вопрос расстановки приоритетов важности активов КС либо основывались на статичной ценности отдельных объектов КС, что затрудняло процесс получения численной оценки работоспособности КС.

Непосредственно вопросам оценки работоспособности КС посвящены работы отечественных ученых Девянина П. Н., Михальского О. О., Правикова Д. И., Щербаков А. Ю., Осовецкого Л., Шевченко В., Суханова А. В., Авраменко В. С., Козленко А. В., а также зарубежных исследователей Филлипса С., Свилера Л. А., Брэгга Р., Родс-Оусли М., Страссберга Е. и др. Результаты указанных работ позволили получить численные оценки работоспособности КС, основанные на обеспечении целостности основных активов, однако для их получения в современных КС необходимо наличие комплекса программ, осуществляющего динамическое наблюдение за требуемыми показателями качества (ПК) КС. Данная задача особенно актуальна для снижения влияния КВ, реализуемых в автоматическом режиме. При этом остается открытым вопрос получения универсальной оценки важности различных активов КС. Это приводит к необходимости наличия высококвалифицированных сотрудников для эффективного применения существующих на данный момент СПР в целях принятия решений о применении адекватного набора МСВ.

Объектом исследования являются РП КС в конфликтных ситуациях.

Предметом исследования является математическая модель СПР, а также численные методы и комплексы программ оценки работоспособности КС при КВ.

Цель и задачи работы. Основной целью работы является повышение надежности и устойчивости функционирования КС посредством разработки и одновременного использование математических моделей, комплексов программ и численных алгоритмов в интересах обоснования обобщенной математической модели СПР, позволяющей в автоматическом режиме формализовать процесс принятия решения о применении адекватного набора МСВ КВ КС на основе численной оценки работоспособности КС.

Для достижения поставленной цели в рамках работы необходимо решить следующие задачи:

1 Обосновать структурную схему математической модели СПР, формализовать ее ключевые составляющие, а также описать основные условия и ограничения применения.

2 Разработать численный метод оценки показателя работоспособности КС на основе метода группового учета аргументов (МГУА), а также обосновать алгоритм построения математической модели работоспособности КС (РКС) для получения универсальных численных оценок значений ущерба КС с помощью комплекса программ.

3 Обосновать структурную схему системы обнаружения и классификации (СОК) КВ и разработать комплекс программ и алгоритмов для их обнаружения и классификации, позволяющий численно оценить значения рисков от ошибок первого и второго рода, в интересах минимизации ущерба КС, полученного при помощи предложенных математических моделей СПР и РКС.

4 Обосновать архитектуру модуля контрастирования неизвестных КВ и модуля выявления полного набора характеристик известных КВ. Разработать комплекс программных модулей, позволяющий структурировать и визуализировать множество ПК, характеризующих неизвестное КВ, полученных в результате натурного эксперимента.

5 Обосновать узкоспециализированные математические модели КВ КС, для которых неприемлемо применение универсальных МСВ, а также разработать комплекс программ по наблюдению и численной оценке связанных с ними ПК КС.

6 Обосновать математическую модель принятия решения о применении адекватного набора МСВ КВ, оптимального по критерию минимума итогового ущерба КС, на основе теоретико-игрового подхода.

Научная новизна. В рамках работы получены следующие новые научные результаты:

1 Разработана и обоснована процедура численной оценки показателя работоспособности КС (ПРКС) с применением математической модели РКС, полученной с помощью численного подхода на основе аддитивно-мультипликативного МГУА. Получены значения весовых коэффициентов относительной важности рабочих процессов (РП) для типовых КС всех классов.

2 Обоснована структура обобщенной математической модели СПР, позволяющая применять существующие узкоспециализированные модели взаимодействия различных классов КВ и МСВ, приведенные к единой численной оценке ущерба КС на основе вычислительного эксперимента.

3 Обоснована структурная схема СОК КВ на основе использования математического аппарата искусственных нейронных сетей (ИНС). Предложены модифицированные критерии качества обучения ИНС, учитывающие относительный вес ошибок обнаружения первого и второго рода, а также ущерб, возникающий в результате ошибок неправильной классификации КВ.

4 Обоснована математическая модель взаимодействия компонентов КС в конфликтных ситуациях, позволяющая получать численную оценку остаточного ущерба КС, а также разработан комплекс программ, позволяющий оптимизировать набор МСВ.

5 Разработана на основе теоретико-игрового подхода математическая модель принятия решения о применении адекватного набора МСВ, оптимального по критерию минимума итогового ущерба КС.

Реализация и внедрение. Оригинальные результаты, полученные одновременно в областях математического моделирования, численных методов и комплексов программ, позволили создать СПР, объективно оценивающую состояние РП КС, учитывающую индивидуальные приоритеты важности активов, а также позволяющую в автоматическом режиме применять адекватный набор МСВ в ответ на обнаруженные КВ. Экспериментальные исследования подтверждают возможность применения полученных в работе оригинальных результатов как для КС малых предприятий, так и для сложных распределенных КС. Результаты работы использовались для построения СПР провайдера Интернет-услуг г. Рязани ООО «РязаньТелеКом», и СПР ООО «Частная охранная организация «Аммон», что подтверждается соответствующими актами о внедрении.

Методология и методы исследования. В работе использовались методы математической статистики, распознавания образов, МГУА, математический аппарат ИНС и теории игр, а также новые достижения в области построения современных систем управления. Перечисленные теоретические методы сочетаются с экспериментальными исследованиями на основе проведения вычислительных и натурных экспериментов, в том числе и с помощью средств виртуализации.

Положения, выносимые на защиту.

1 Математическая модель РКС, полученная на основе использования аддитивно-мультипликативного МГУА, позволяющая в автоматическом режиме в результате проведения вычислительного эксперимента получать численную оценку нанесенного ущерба при КВ КС на основе объективных наблюдений за ПК КС с помощью комплекса программ. При этом математическое ожидание относительной ошибки предсказания ПРКС не превышает 3,11 %, а максимальное значение ошибки снижено с 17,1 % до 6,0 %, по сравнению с использованием классического метода регрессионного анализа.

2 Модифицированный критерий оптимизации ошибки обучения ИНС, выполняющих задачу обнаружения КВ, позволяющий снизить величину нанесенного суммарного ущерба КС от 4 % до 25 % при различных параметрах обучения ИНС. Применение предложенного критерия также позволило расширить в 1,83 раза интервал коэффициента значимости полноты обнаружения КВ, при котором достигаются минимальные значения нанесенного ущерба КС.

3 Модифицированный критерий качества обучения ИНС, выполняющих функцию классификации КВ, в виде модифицированной средней функции риска, позволяющий снизить итоговое значение суммарного ущерба КС на величину от 21 % до 64 % по сравнению с системами классификации, обученными по критерию минимума среднеквадратического отклонения (СКО) ошибки обучения.

Достоверность результатов исследований. Достоверность полученных в диссертационной работе результатов подтверждается с помощью экспериментальных исследований КС, смоделированных с помощью средств виртуализации, подвергаемых воздействию актуальных на сегодняшний день КВ. Корректность полученных данных также подтверждается практическими результатами внедрения обоснованной в рамках работы СПР в действующие КС.

Соответствие паспорту специальности. Содержание работы соответствует п. 4 «Реализация эффективных численных методов и алгоритмов в виде ком-

плексов проблемно-ориентированных программ для проведения вычислительного эксперимента», п. 5 «Комплексные исследования научных и технических проблем с применением современной технологии математического моделирования и вычислительного эксперимента», п. 6 «Разработка новых математических методов и алгоритмов проверки адекватности математических моделей объектов на основе данных натурного эксперимента».

Апробация работы. Результаты работы докладывались на следующих конференциях:

1 Шестнадцатая всероссийская научно-техническая конференция студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях» (НИТ-2012). Рязань, 2012 г.

2 Вторая международная научно-практическая конференция «Обеспечение комплексной безопасности предприятий: проблемы и решения». Рязань, 2013 г.

3 Шестая международная научно-техническая конференция «Космонавтика. Радиоэлектроника. Геоинформатика», посвященная 90-летию со дня рождения академика В.Ф. Уткина. Рязань, 2013 г.

4 Девятнадцатая всероссийская научно-техническая конференция студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях и в образовании» (НИТ-2014). Рязань, 2014 г.

5 Четвертая международная научно-практическая конференция «Обеспечение комплексной безопасности предприятий: проблемы и решения». Рязань, 2015 г.

6 Восемнадцатая международная научно-техническая конференция «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань, 2015 г.

7 Международная научно-практическая конференция «Наука, образование, общество: актуальные вопросы и перспективы развития». Москва, 2015 г.

8 Двадцатая всероссийская научно-техническая конференция студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях НИТ-2015». Рязань, 2015 г.

Публикации. По теме диссертации опубликовано 13 работ: 3 статьи в научно-технических журналах, рекомендованных ВАК, 1 статья в межвузовском сборнике трудов и 9 тезисов докладов на конференциях.

Личный вклад. Все представленные в диссертации результаты исследований и экспериментальные данные получены лично автором или при его непосредственном участии.

Структура и объем работы. Диссертационная работа состоит из введения, трех глав, заключения, списка литературы из 167 наименований и восьми приложений. Диссертация изложена на 291 странице, из которых 147 страниц основного текста, 26 таблиц и 52 рисунка.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Во введении обоснована актуальность выбранной темы, определены цели и задачи, решаемые в рамках работы, сформулированы положения, выносимые на

защиту. Изложены новые научные результаты, полученные в работе, показаны ее теоретическая и практическая значимость.

В первой главе обоснована обобщенная математическая модель СПР, определены ее основные ограничения и структурные составляющие.

Предложена следующая структурная схема математической модели СПР (рисунок 1), которая подразумевает наличие математической модели РКС, с помощью которой производится оценка ПРКС $y=f(x_1, x_2, \ldots, x_n)$, на основе объективных наблюдений за множеством $X=(x_1, x_2, \ldots, x_n)$ ПК КС в автоматическом режиме с помощью комплекса программ.

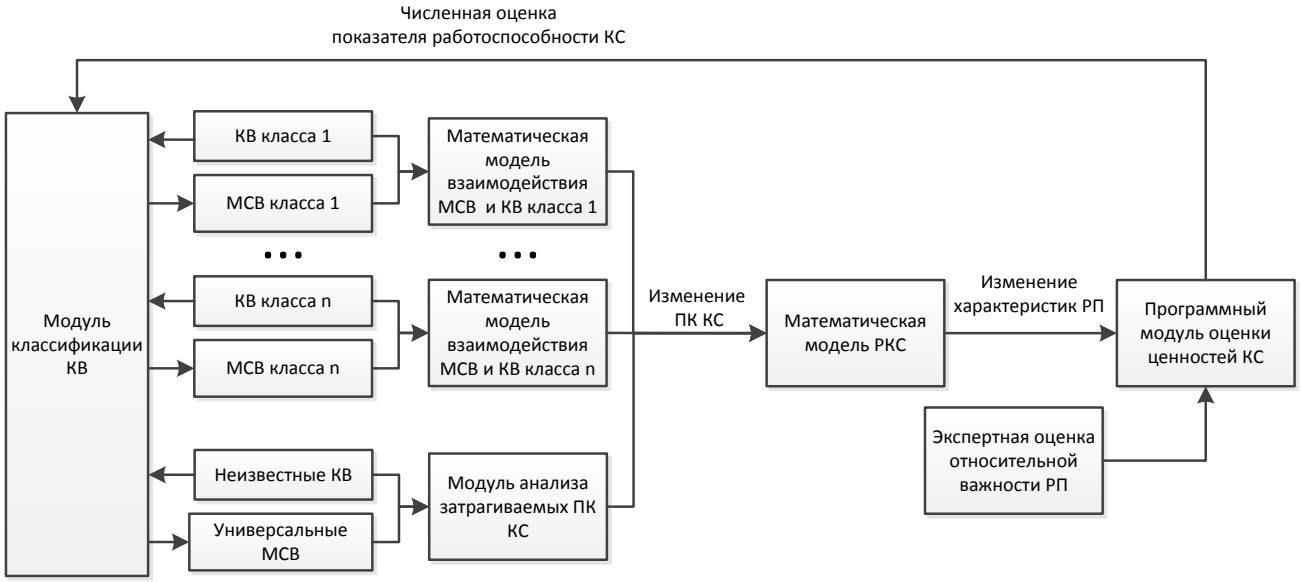

Рисунок 1 – Структурная схема математической модели СПР

Показана возможность применения численной оценки ПРКС $y(x_1 \ldots x_n)$ для получения величины ущерба Q_j^k от взаимного воздействия на КС j-го КВ и k-го МСВ, используемой при численной оценке критерия качества принятых решений.

Произведен анализ и классификация основных типов КВ, с целью получения обобщенных математических моделей их взаимодействия с МСВ внутри каждого отдельного класса. Сформирован эталонный набор КВ, включающий 175 наименований, а также построено семь типовых КС, что позволило смоделировать все эталонные сетевые сценарии КВ КС. Предложена комплексная классификация КВ согласно конечному результату изменения ПК КС. Данный подход позволил выделить для каждого класса КВ множество универсальных МСВ, способных противостоять неизвестным КВ.

Обоснована математическая модель универсального сетевого взаимодействия. При этом выделены следующие ключевые характеристики, присущие любому комплексному КВ: I^A источник, O^A объекты воздействия, X^A множество затрагиваемых ПК КС и Q_j потенциальный ущерб.

Разработана процедура численной оценки $y(x_1 \ldots x_n)$ ПРКС. Показана необходимость экспертной оценки значений a_{ij} весовых коэффициентов относительной важности РП и r_j уровней работоспособности РП, для получения численных оценок важности объектов КС. Из-за высокой сложности получения экспертных оценок ПРКС $y(x_1 \ldots x_n)$ на основе прямого анализа множества $X=(x_1 \ldots x_n)$ ПК КС, в ра-

боте предложено производить экспертную оценку на основе анализа r_j уровней работоспособности РП КС по следующей формуле:

$$y(r_1,r_2...r_m)=\sum_{j=1}^{m}a_j r_j\,. \qquad (1)$$

В результате ПРКС вычисляется в виде $y(r_1...r_m)$ функции от r_j уровней работоспособности РП, и используется в дальнейшем для получения математической модели РКС. Обоснована форма представления РП, позволяющая увеличить значение коэффициента конкордации Кендэла W_e, отражающего степень согласованности мнений экспертов, на величину от 8,0 % (для КС 3-го класса) и 24,0 % (для КС 2-го класса) до 53,7 % (для КС 6-го класса). Получены численные значения a_{ij} весовых коэффициентов относительной важности РП для всех типовых КС.

Обоснована процедура построения математической модели РКС, позволяющей в автоматическом режиме получить численную оценку ПРКС $y(x_1...x_n)$ при КВ на основе объективных наблюдений за ПК КС с помощью комплекса программ. В качестве метода получения математической модели предложено использование аддитивно-мультипликативного МГУА. В общем виде ПРКС представляет собой функцию от r_j уровней работоспособности РП в виде полинома Колмогорова - Габора:

$$y(r_1,r_2,...,r_m)=a_0+\sum_{j=1}^{m}a_j r_j+\sum_{i=1}^{m}\sum_{j=1}^{m}a_{ij}r_i r_j+...+\sum_{i=1}^{m}\sum_{j=1}^{m}...\sum_{q=1}^{m}a_{ij...q}r_i r_j..r_q\,. \qquad (2)$$

В свою очередь, уровни работоспособности РП r_j предложено моделировать в виде функции $r(x_1...x_n)$ от ПК КС с помощью мультипликативного алгоритма МГУА, поскольку отличительной чертой функционирования РП является невозможность компенсации одних ПК другими. В данном случае предложено использовать мультипликативный полином вида:

$$r_j=a_{0,j}x_1^{k_{1j}}x_2^{k_{2j}}...x_n^{k_{nj}}=a_{0,j}\prod_{i=1}^{n}x_i^{k_{ij}}\,, \qquad (3)$$

где $a_{0,j}$, k_i – весовые коэффициенты полинома. Таким образом, обобщенная структура исследуемой зависимости ПРКС $y(x_1...x_n)$, полученная в результате использования аддитивно-мультипликативного МГУА, имеет следующий вид:

$$y(x_1,x_2,..,x_n)=a_0+\sum_{j=1}^{m}a_j\left(a_{0,j}\prod_{i=1}^{n}x_i^{k_{ij}}\right)+\sum_{l=1}^{m}\sum_{j=1}^{m}a_{jl}\left(a_{0,j}\prod_{i=1}^{n}x_i^{k_{ij}}\right)\left(a_{0,l}\prod_{i=1}^{n}x_i^{k_{il}}\right)+.... \qquad (4)$$

Процесс получения весовых коэффициентов полинома (4) основан на последовательном отсеивании моделей-претендентов в рамках применения аддитивно-мультипликативного МГУА, посредством анализа выборок ПК КС, наблюдаемых при КВ КС, а также соответствующих экспертных оценок ПРКС. Выбор моделей-претендентов происходит согласно предложенному в работе комплексному внешнему критерию качества p_k математической модели РКС:

$$p_K=\sqrt{\gamma n_{см}^2+(1-\gamma)\Delta^2(C)}\to\min_{y}, \qquad (5)$$

где $n_{см}^2$ – критерий минимума смещения, обеспечивающий непротиворечивость модели, $\Delta^2(C_m)$– критерий точности краткосрочного прогноза, $\gamma\in[0,1]$ – весовой коэффициент относительной важности критериев. Экспериментальные исследо-

вания показали, что для сложных КС целесообразно выбирать значение γ=0,2…0,4. Это позволило ускорить поиск оптимальной по критерию (5) математической модели в среднем в 1,5 – 2 раза, сохранив при этом точность предсказания моделей в 5 % доверительном интервале с доверительной вероятностью 0,95.

Применение математической модели РКС, полученной на основе использования аддитивно-мультипликативного МГУА, позволило в автоматическом режиме получить численную оценку ПРКС $y(x_1 \ldots x_n)$ при КВ на основе объективных наблюдений за ПК КС с помощью комплекса программ. При этом математическое ожидание y_t^M относительной ошибки предсказания действительного наблюдаемого значения y_t ПРКС не превышало 3,11 % (рисунок 2), а максимальное значение Δy_t ошибки было снижено с 17,1 % до 6,0 %, по сравнению с классическими методами регрессионного анализа.

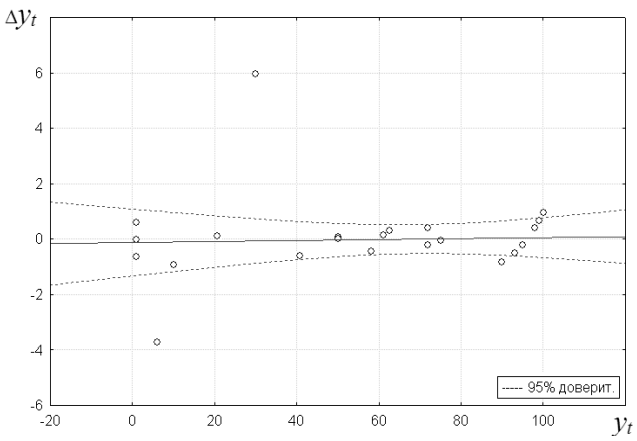

Рисунок 2 – Распределение Δy_t ошибок предсказания от

В работе проведены экспериментальные исследования математических моделей всех типовых КС, согласно Приложению 2, обладающих различными значениями m количества РП и $\max(n_j^{ПК})$ максимального количества ПК, влияющих на функционирование одного РП. В рамках исследований производилась оценка величин среднего значения $\overline{\Delta y_t}$ и дисперсии $D(\Delta y_t)$ абсолютной ошибки предсказания математической модели РКС соответственно, а также значения относительной ошибки предсказания $\overline{\Delta y_t}/y_t^M$ и ее дисперсия $D(\overline{\Delta y_t}/y_t^M)$ (таблица 1).

Таблица 1 – Результаты исследований математических моделей работоспособности основных классов компьютерных систем

Класс КС	γ	$\overline{\Delta y_t}$	$D(\Delta y_t)$	$\overline{\Delta y_t}/y_t^M$	$D(\overline{\Delta y_t}/y_t^M)$	$\max(n_j^{ПК})$, шт.	m, шт.	W_e
1	0,5	1,85	1,727	0,1075	0,0230	25	6	0,95
2	0,5	1,93	1,882	0,1109	0,0223	34	8	0,93
3	0,5	2,15	1,891	0,1147	0,0235	31	13	0,92
4	0,5	2,10	2,011	0,1289	0,0281	29	9	0,94
5	0,39	2,98	2,632	0,1256	0,0315	48	16	0,83
6	0,34	3,11	2,871	0,1374	0,0311	51	17	0,83
7	0,4	2,76	2,121	0,1305	0,0284	35	13	0,91

Обоснована обобщенная математическая модель СПР, позволяющая применять существующие на сегодняшний момент узкоспециализированные модели взаимодействия различных классов КВ и МСВ, приводя их к единой численной оценке Q_j^k ущерба КС. Предложенная обобщенная математическая модель СПР является модификацией известной математической модели Клементса - Хоффма-

на (модели с полным перекрытием). Преимущество предложенной математической модели СПР заключается в применении математической модели РКС для получения численных оценок значений ущерба Q_j^k от КВ, рассчитываемых по формуле:

$$Q_j^k = \sum_{j=1}^{m} a_j a_{0,j} \left(\prod_{i=1}^{n} x_i^{k_i} - \prod_{i=1}^{n} (x + \Delta x)_i^{k_i} \right) + \ldots, \quad (6)$$

где Δx – изменения ПК КС при наличии j-го КВ и k-го МСВ. Предложенная обобщенная математическая модель СПР также учитывает наличие вероятности $P_j^O<1$ обнаружения j-го КВ, что позволяет численно оценить величину целостности КС с помощью формулы:

$$S = 1/\sum_{j=1}^{m} \left(P_j^A \cdot (P_j^O Q_j^{\min} + (1 - P_j^O) Q_j) \right), \quad (7)$$

где P_j^A – априорная вероятность появления j-го КВ, Q_j – потенциальный ущерб от j-го КВ, Q_j^{min} – минимальный остаточный ущерб при применении наилучшего МСВ для j-го КВ. Обоснованная математическая модель СПР используется в дальнейшем для проверки адекватности результатов, полученных от СОК КВ.

Во второй главе обоснована структурная схема СОК КВ. Произведенный анализ основных методов обнаружения КВ показал перспективность сигнатурных и нейросетевых методов обнаружения. В работе предложен подход, основанный на применении математического аппарата ИНС для решения задач обнаружения КВ, использующий существующие на данный момент сигнатурные методы обнаружения, а также обоснованную в первой главе математическую модель СПР.

Предложен модифицированный критерий качества обучения ИНС, выполняющих функцию обнаружения КВ. Предложенный критерий является модификацией F_δ – меры, обобщенного критерия качества бинарной классификации:

$$F_\delta = (1 + \delta^2) \frac{PR \cdot RC}{\delta^2 PR + RC} \quad , \quad (8)$$

где δ – коэффициент значимости полноты, PR – точность обнаружения КВ, RC – полнота обнаружения КВ. Преимущество предложенного критерия качества заключается в применении математической модели РКС, обоснованной в первой главе, для учета веса ошибок обнаружения КВ первого и второго рода. Вес ошибок обнаружения КВ рассчитывается исходя из численных оценок Q_j потенциального ущерба КС, нанесенного j-м КВ, и численных оценок побочного ущерба Q_0^k, возникающего от применения k-го МСВ в отсутствии КВ при ложном срабатывании СОК. Таким образом, предложенный критерий качества обучения ИНС в виде модифицированной F'_δ - меры рассчитывается по формуле (8), где значения PR и RC заменяются на PR' и RC' соответственно и вычисляются по следующим формулам:

$$PR' = \sum_{j=1}^{TP} (Q_j - Q_j^{\min}) / (\sum_{j=1}^{TP} (Q_j - Q_j^{\min}) + \sum_{k=1}^{FP} Q_0^k), \quad (9)$$

$$RC' = \sum_{j=1}^{TP} (Q_j - Q_j^{\min}) / (\sum_{j=1}^{TP} (Q_j - Q_j^{\min}) + \sum_{j=1}^{FN} Q_j). \quad (10)$$

где *TP* – количество верных обнаружений КВ, *FP* – количество ложных срабатываний, *FN* – количество пропущенных КВ, которые не были обнаружены.

Применение модифицированного критерия качества обучения ИНС позволило снизить суммарный ущерб Q_Σ, нанесенный в результате воздействия на КС эталонным набором КВ, на величину от 4 % до 25 % в ширине диапазона коэффициента значимости полноты $\delta \in [0{,}71...2{,}36]$, при котором фактическое значение суммарного ущерба Q_Σ находилось в интервале $\min(Q_\Sigma) + 0{,}05Q_\Sigma$. Применение предложенного критерия также позволило расширить в 1,83 раза интервал коэффициента значимости полноты обнаружения КВ, при котором достигается минимальные значения нанесенного ущерба КС (рисунок 3).

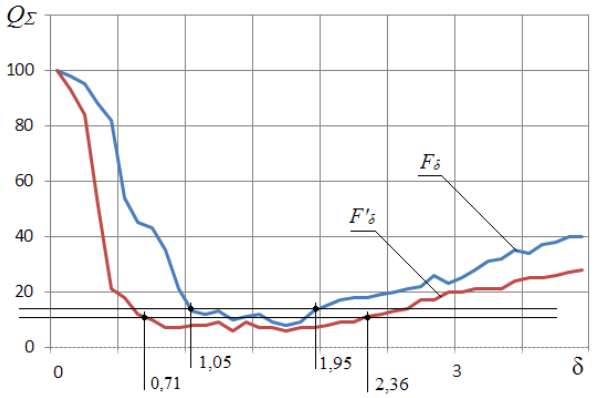

Рисунок 3 – Интервал значения *δ*, обеспечивающий приемлемый уровень целостности КС

На основе полученных результатов разработан комплекс программ обнаружения КВ, представляющий собой программную реализацию обученной ИНС прямого распространения, использующую в качестве входных данных как ПК КС, так и результаты работы комплексов программ, основанных на сигнатурных методах обнаружения КВ.

Обоснована и разработана ИНС классификации КВ. В качестве критерия обучения предложено применение средней функции риска *F*, формула расчета которой в условиях дискретного многомерного характера признаков КВ, имеет следующий вид:

$$F = \sum_{j=1}^{K_p} \sum_{i=1}^{K} \left[\frac{\theta_{ij}}{N_p} S^{k_p}(\vec{X}_i) l_{ij} F_E(\vec{X}_i) \right], \tag{11}$$

где K – количество классов входного сигнала, K_p – количество классов решений, θ_{ik_p} – количество случаев классификации КВ i-го класса как КВ k_p-го класса, N_p – число элементов множества обучающих примеров, $F_E(\vec{X}_i)$ – Евклидова длина векторов ПК, $S^{k_p}(\vec{X})$ – область многомерного пространства признаков КВ.

При этом веса l_{ij} матрицы коэффициентов потерь L рассчитывались с помощью математической модели СПР, обоснованной первой главе, по формуле:

$$l_{ij} = \left| S_{ii} - S_{ij} \right| / \sum_{i=1}^{K} \sum_{j=1}^{K_p} \left| S_{ii} - S_{ij} \right|, \tag{12}$$

где S_{ii} и S_{ij} – величины целостности КС, полученные по формуле (7), и рассчитанные при условии КВ i-го класса на КС, в которой применены МСВ i-го и j-го класса соответственно. Получены матрицы коэффициентов потерь для всех типовых КС, а также построены зависимости коэффициентов потерь от ошибок классификации КВ, приводящих к неоптимальному управлению КС (рисунок 4). Данные зависимости позволили наглядно изобразить максимально опасные ошибки классификации КВ.

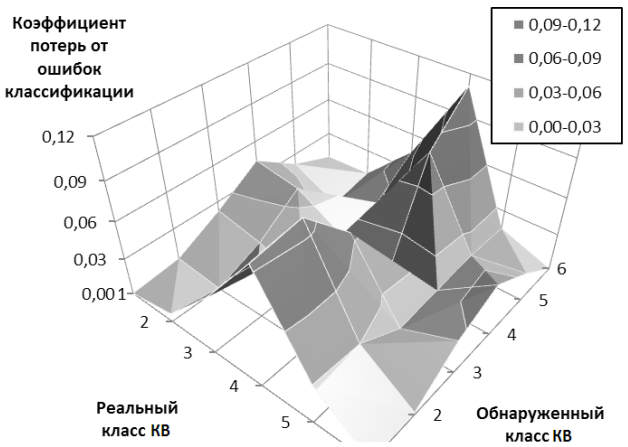

Рисунок 4 – Зависимости коэффициентов потерь от ошибок классификации КВ

Произведен сравнительный анализ качества классификации ИНС, обученных по критерию E минимизации СКО ошибки и по предложенному критерию минимизации функции риска F (таблица 2). В ходе анализа также учитывалось значение θ_Σ – абсолютного количество ошибок классификации КВ.

Учет весов ошибок классификации на этапе обучения ИНС позволил снизить итоговое значение суммарного ущерба более чем на 21 % для всех типовых КС по сравнению с системами классификации, использующими в качестве критерия минимум СКО ошибки предсказания. Максимальные значение снижения ущерба наблюдались для простых КС и достигали 64 %.

Таблица 2 – Результаты сравнительных испытаний ИНС классификации КВ, обученных с использованием различных критериев оптимальности

Класс КС	N_p, шт.	θ_Σ, шт.		θ_Σ / N_p		$Q_\Sigma \in [0,1]$	
		E	F	E	F	E	F
1	15415	1422	1903	0,0923	0,1235	0,1514	0,0541
2	17131	16814	2424	0,9815	0,1415	0,1749	0,0651
3	34721	4381	5288	0,1262	0,1523	0,1893	0,0711
4	42195	5620	7565	0,1332	0,1793	0,1915	0,1512
5	50311	7662	9322	0,1523	0,1853	0,1421	0,0823
6	104223	18874	22668	0,1811	0,2175	0,1723	0,0692
7	70135	12021	13472	0,1714	0,1921	0,1636	0,0731

Обоснована структура модуля выявления характеристик известных КВ, основанная на применении рекуррентных ИНС Хопфилда, позволяющих запоминать от 48 % до 76 % представленных на этапе обучения КВ в зависимости от их класса. Предложенная структура модуля позволила выявить скрытые характеристики КВ, такие как источник I^A, объекты воздействия O^A, а так же специфические для каждого класса КВ характеристики. В результате проведенных исследований было показано, что максимальное количество полностью идентифицированных КВ в интервале от 60 % до 76 % наблюдалось для наиболее опасных классов КВ. Для остальных КВ была достигнута точность выявления таких ключевых характеристик, как I^A источник и O^A объекты воздействия, в пределах от 66 % до 89 % и от 69 % до 92 % соответственно.

Обоснована ИНС встречного распространения, позволяющая структурировать информацию о неизвестных КВ и выделять среди множества неизвестных КВ, обладающих векторами признаков $\vec{r}$, ядра классов $\vec{c}$, максимально близкие к каждому отдельному элементу множества КВ неизвестного класса. В качестве

меры близости принимался коэффициент корреляции между вектором признаков КВ $\vec{r}$ и вектором признаков ядра класса $\vec{c}$:

$$d(\vec{r},\vec{c}) = \sum_j \frac{(r'_j - M_r)(c'_j - M_c)}{\sigma_r \sigma_c}, \quad (13)$$

где r'_j, c'_j – отдельные признаки КВ и ядра класса соответственно, n_r – размерность пространства признаков, M_r и M_c – математическое ожидание отдельного признака КВ и ядра класса соответственно, σ_r и σ_r – СКО отдельного признака КВ и ядра класса соответственно. Для визуализации полученных векторов $\vec{c}$ ядер классов неизвестных КВ разработан комплекс программ, отображающий наиболее значимые ПК, с точки зрения нанесенного ущерба, на сетевой карте КС.

В третьей главе предложена математическая модель взаимодействия компонентов КС в конфликтных ситуациях, позволяющая упростить процесс получения численных оценок Q_j^k остаточного ущерба КС на основе анализа множества $C^{u,\,j}$ условий реализации КВ. На основе предложенной математической модели разработан комплекс программ, позволяющий сократить исходное множество M МСВ до M' более чем на 30 % при наличии в КС менее 25 одновременно обнаруженных КВ для всех 7-ми классов КС. Соответствующие зависимости изображены на рисунке 5, где $\Delta M = M'/M$.

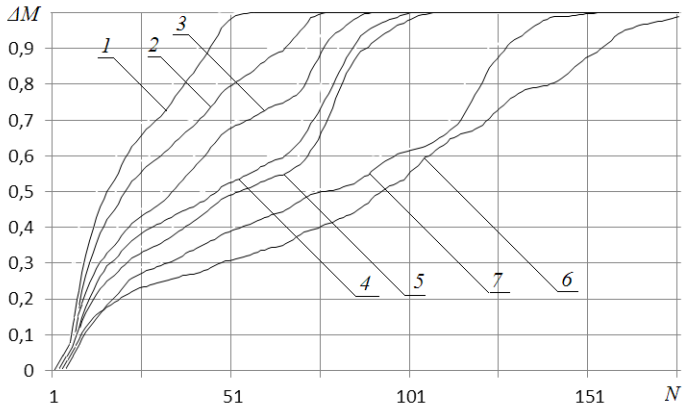

Рисунок 5 – Зависимость ΔM от числа обнаруженных КВ

Разработан комплекс проблемно-ориентированных программ, реализующий модифицированный численный метод оценки стойкости ключевых последовательностей, на основе численной оценки энтропии H, полученной в результате вычислительного эксперимента:

$$H = -\sum_{j=1}^{\Theta} p^W(j) \log_2 p^W(j), \quad (14)$$

где $p^W(j)$ – вероятность появления отдельной последовательности из словаря Θ. Доказана возможности применения энтропии ключевой последовательности в качестве меры стойкости к машинному перебору, при помощи натурных экспериментов подбора для различных пространств событий (ПС) Ω, что обосновано низкими показателями СКО вероятности успешного подбора ключа P^H, которое не превышает 0,0054, для ПС с близкими значениями энтропии H. Предложены формулы для расчета энтропии типовых составляющих последовательностей ключа, а также формулы для расчета взаимной энтропии составных последовательностей.

Предложен набор комплексов программ, предназначенных для автоматического наблюдения за ПК КС. Разработан специализированный комплекс программ наблюдения за ПК топологии КС.

Обоснована математическая модель принятия решения о применении адекватного набора МСВ на основе теоретико-игрового подхода. Показана возможность применения математической модели РКС, обоснованной в первой главе, для получения платежной матрицы $|Q| = ||Q_j^k||$ простой одношаговой игровой

ситуации. Разработана процедура минимизации размерности платежной матрицы на основе удаления доминируемых стратегий решения, что позволило сократить число рассматриваемых стратегий на 1-3 порядка. Предложен подход к решению многошаговых игр путем получения полной матрицы событий с дальнейшим просчетом игровой ситуации на несколько шагов вперед. Получены зависимости численной оценки Q_j^k нанесенного ущерба КС от количества шагов запаздывания n'_q СПР (рисунок 6).

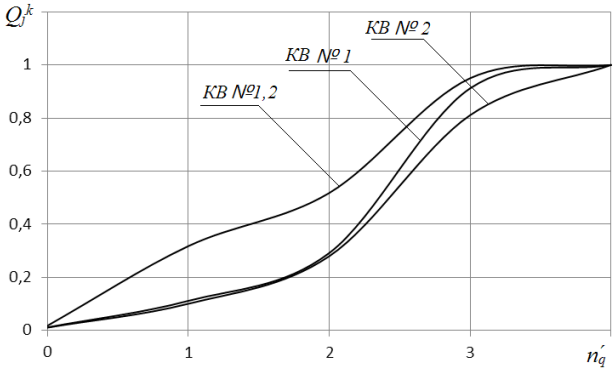

Рисунок 6 – Зависимость ущерба КС от запаздывания СПР

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В заключении приведены основные результаты диссертационной работы.

1 Предложена комплексная классификация КВ, позволяющая применять обобщенные математические модели КВ КС, что позволило снизить количество рассматриваемых МСВ более чем на 30 % и ускорило время реакции СПР на 1-3 порядка.

2 Разработана процедура численной оценки работоспособности КС для обоснования ценностей активов КС. Получены значения a_{ij} весовых коэффициентов относительной важности РП для типовых КС всех классов, согласно Приложению 2. Проведенные исследования показали возможность применения метода экспертной оценки значений a_{ij} весовых коэффициентов относительной важности РП и r_j уровней работоспособности РП. Это обусловлено прозрачностью получаемых значений, относительной простотой расчетов и низким значением $\Delta\lambda$ меры несогласованности экспертов (от 0,38 до 1,84 для различных классов КС).

3 Обоснована процедура построения математической модели РКС для автоматической оценки ПРКС на основе объективных наблюдений за ПК КС с помощью комплекса программ. В качестве метода получения математической модели предложено использование аддитивно-мультипликативного МГУА. Экспериментальные исследования показали, что математическая модель РКС способна предсказывать численную оценку работоспособности КС при КВ с относительной погрешностью, не превышающей 6% (по сравнению с классическим регрессионным анализом, относительная ошибка предсказания которого достигает 17%). При этом математическое ожидание ошибки предсказания среди всех полученных математических моделей РКС не превышало 3,11 %.

4 Обоснована структура обобщенной математической модели СПР, позволяющая применять существующие на сегодняшний день узкоспециализированные модели КВ КС, приводя их к единой численной оценке Q_j^k ущерба КС. Применение математической модели СПР дает возможность получать универсальные численные оценки Q_j^k ущерба от взаимного влияния на КС КВ и МСВ в результате автоматического наблюдения за ПК КС с помощью комплекса программ.

5 Предложен модифицированный критерий качества обучения ИНС, выполняющих функцию обнаружения КВ, что позволило снизить суммарный нанесенный ущерб КС, возникший в результате ошибок обнаружения КВ. Величина относительного снижения суммарного ущерба находилась в 5 % доверительном интервале с доверительной вероятностью 0,95 при оптимальном выборе характеристик классического критерия обучения. Для остальных случаев величина относительного снижения суммарного ущерба составила (10…25) % в широком диапазоне коэффициента значимости полноты $\delta \in [0{,}71...2{,}36]$, при котором фактическое значение суммарного ущерба Q_Σ находилось в доверительном интервале $\min(Q_\Sigma) + 0{,}05Q_\Sigma$ с доверительной вероятностью 0,95. Применение предложенного критерия также позволило расширить в 1,83 раза интервал коэффициента значимости полноты δ обнаружения КВ, при котором достигались минимальные значения нанесенного ущерба КС.

6 Предложен модифицированный критерий качества обучения ИНС, выполняющих функцию классификации КВ. В качестве критерия обучения применялось значение средней функции риска *F*. При этом веса матрицы *L* коэффициентов потерь рассчитывались с помощью обоснованной математической модели СПР. Данный подход позволил ранжировать ошибки от неправильной классификации КВ согласно ущербу, возникающему от применения неадекватных МСВ. Применение предложенного критерия позволило снизить итоговое значение суммарного ущерба КС более, чем на 21 % по сравнению с системами классификации, обученными по критерию минимума СКО ошибки обучения. Максимальная величина снижения ущерба наблюдалась для простых КС и достигала 64%.

7 Обоснована структура модуля выявления характеристик известных КВ, основанная на применении рекуррентных ИНС Хопфилда, позволяющих запоминать от 48 % до 76 % представленных на этапе обучения характеристик. Предложенная структура модуля позволила выявить источник КВ I^A, объекты КВ O^A, а также специфические для каждого класса КВ характеристики. В результате проведенных исследований было показано, что максимальное количество полностью идентифицированных КВ в интервале от 60 % до 76 % наблюдалось для наиболее опасных классов КВ. Для остальных КВ была достигнута точность выявления таких ключевых характеристик, как I^A источник и O^A объекты воздействия, от 66 % до 89 % и от 69 % до 92 % соответственно.

8 Обоснована математическая модель КВ компонентов КС, позволяющая формализовать оценку суммарного влияния на КС КВ и МСВ. Проведенные исследования показали, что для 92 % КВ из эталонного набора значения Q_j^k остаточного ущерба, полученные с помощью математической модели РКС и с помощью математической модели конфликтного взаимодействия КС, отличаются друг от друга не более чем на величину доверительного интервала $\pm 0{,}05 Q_j^k$ с доверительной вероятностью, равной 0,95.

9 Разработан комплекс проблемно-ориентированных программ, реализующий модифицированный численный метод оценки стойкости ключевых последовательностей, в целях снижения эффективности соответствующих КВ на 30 % - 50 % на основе численной оценки энтропии, полученной в результате проведения вычислительного эксперимента. Проведенные исследования доказали возмож-

ность использования энтропии для оценки стойкости ключевых последовательностей к КВ машинного перебора.

10 Разработан комплекс программ, позволяющий оптимизировать набор МСВ, используемый для получения стратегий решения конфликтных ситуаций. Применение разработанного комплекса программ позволило сократить исходное множество *M* МСВ более чем на 30 % при наличии в КС менее 25-ти одновременных КВ.

11 Обоснована на основе теоретико-игрового подхода математическая модель принятия решения о применении набора МСВ, оптимального по критерию минимума итогового ущерба КС. Показана возможность применения математической модели РКС для получения платежной матрицы простой одношаговой игровой ситуации. Предложен подход к решению многошаговых игр путем получения полной матрицы событий с дальнейшим просчетом игровой ситуации на несколько шагов вперед. Произведенные исследования показали возможность применения предложенного теоретико-игрового подхода, что доказывается минимальными значениями полученной численной оценки Q_j^k остаточного ущерба КС.

Полученные оригинальные результаты одновременно в областях математического моделирования, численных методов и комплексов программ позволили создать СПР, объективно оценивающую с помощью комплекса программ состояние целевой КС, учитывающую индивидуальные приоритеты важности активов и РП КС и позволяющую в автоматическом режиме применять адекватный набор МСВ в ответ на возникающие КВ КС.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в журналах, рекомендованных ВАК

1. Крупнов Л.С. Разработка алгоритма формализации параметров компьютерной системы для оценки опасности сетевых атак. // Вестник Рязанского государственного радиотехнического университета. 2014. № 49. – С. 67-72.
2. Кириллов С.Н., Крупнов Л.С. Энтропия паролей как мера оценки стойкости к машинному перебору. // Вестник Рязанского государственного радиотехнического университета. 2015. № 51. – С. 60-66.
3. Кириллов С.Н., Крупнов Л.С. Система обнаружения и классификации сетевых атак на основе искусственных нейронных сетей // Вестник Рязанского государственного радиотехнического университета. 2015. № 53. – С. 41-47.

Публикации в межвузовских сборниках

4. Крупнов Л.С. Обоснование оптимального состава защитных стратегий при теоретико-игровом подходе к обеспечению безопасности компьютерных систем // Межвузовский сборник научных трудов «Методы и средства обработки и хранения информации». – Рязань, 2015. – С. 51-54.

Тезисы докладов на конференциях и семинарах

5. Кириллов С.Н., Крупнов Л.С. Алгоритм классификации сетевых атак на основе искусственных нейронных сетей // XVI Всероссийская научно-техническая конференция студентов, молодых ученых и специалистов «Новые

информационные технологии в научных исследованиях». Тезисы докладов – Рязань: РГРТУ, 2012 – С. 91-92.

6. Кириллов С.Н., Крупнов Л.С. Применение теоретико-игрового подхода для построения автоматизированной системы защиты информации в компьютерной сети предприятия. // II Международная научно-практическая конференция «Обеспечение комплексной безопасности предприятий: проблемы и решения». Тезисы докладов – Рязань: РГРТУ, 2013. – С. 87-88.

7. Кириллов С.Н., Крупнов Л.С. Защита центров управления полетами космических аппаратов от сетевых атак на основе теоретико-игрового подхода. // VI МНТК «Космонавтика. Радиоэлектроника. Геоинформатика», посвященная 90-летию со дня рождения академика В.Ф. Уткина. Тезисы докладов – Рязань: РГРТУ, 2013. – С. 167-168.

8. Кириллов С.Н., Крупнов Л.С. Оценка энтропии паролей как меры стойкости к машинному перебору в телекоммуникационных сетях. // XVIII Всероссийская научно-техническая конференция студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях». Тезисы докладов – Рязань: РГРТУ, 2014. – С. 95.

9. Крупнов Л.С., Кириллов С.Н. Обоснование алгоритма оценки ценностей компьютерной системы в целях адекватной защиты от сетевых атак. // IV международная научно-практическая конференция «Обеспечение комплексной безопасности предприятия: проблемы и решения»: Тез. Докладов – Рязань: РГРТУ, 2015. – С. 34-35.

10. Кириллов С.Н., Крупнов Л.С. Обоснование модифицированных алгоритмов обучения искусственных нейронных сетей в интересах защиты телекоммуникационных систем от сетевых атак // XVIII Международная научно-техническая конференция «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Тезисы докладов – Рязань: РГРТУ, 2015. – С. 254-255.

11. Кириллов С.Н., Крупнов Л.С. Обоснование оптимального состава защитных стратегий при теоретико-игровом подходе к обеспечению безопасности телекоммуникационных систем. // Наука, образование, общество: актуальные вопросы и перспективы развития: Сборник научных трудов по материалам Международной научно-практической конференции 30 сентября 2015 г.: в 3 частях. Часть I. – М.: АР-Консалт, 2015. – С. 71-72.

12. Кириллов С.Н., Крупнов Л.С. Обоснование теоретико-игрового подхода для оптимизации защитных мер противодействия сетевым атакам // XVIII Международная научно-техническая конференция «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Тезисы докладов – Рязань: РГРТУ, 2015. – С. 258-260.

13. Крупнов Л.С. Разработка комплекса программ визуализации результатов контрастирования признаков неизвестных сетевых атак на телекоммуникационные системы. // XX Всероссийская научно-техническая конференция студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях НИТ-2015». Тезисы докладов – Рязань: РГРТУ, 2015. С. 77.

Крупнов Леонид Сергеевич

МАТЕМАТИЧЕСКИЕ МОДЕЛИ, КОМПЛЕКСЫ ПРОГРАММ И АЛГОРИТМЫ ПРИНЯТИЯ РЕШЕНИЯ ПРИ ВОЗНИКНОВЕНИИ КОНФЛИКТНОГО ВЗАИМОДЕЙСТВИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Заказ № 7771. Тираж 100 экз. Подписано в печать 25.11.15 г.
Бумага офсетная. Печать ризографическая.

Отпечатано в ООО «НПЦ «Информационные технологии»
Лицензия серия ПЛД № 66-16 от 20 июля 1999 г.
г. Рязань, ул. Островского, 21/1. Тел.: (4912) 98-69-84