НОМЕР ПРОЕКТА **07-01-00547**		УЧЕТНАЯ КАРТОЧКА
НАЗВАНИЕ ПРОЕКТА **Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации, основывающиеся на моделировании поведения систем защиты, реализации верифицированных политик безопасности, оценке защищенности и проактивном мониторинге**		
ОБЛАСТЬ ЗНАНИЯ **01 - математика, информатика, механика**		КОД(Ы) КЛАССИФИКАТОРА **01-201 01-202 01-217**
ВИД КОНКУРСА **a - Инициативные проекты**		
ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА **Котенко Игорь Витальевич**		ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА **(812)3282642**
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ГДЕ ВЫПОЛНЯЕТСЯ ПРОЕКТ **Учреждение Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН**		
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ЧЕРЕЗ КОТОРУЮ ОСУЩЕСТВЛЯЕТСЯ ФИНАНСИРОВАНИЕ **Учреждение Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН**		
ЧИСЛО УЧАСТНИКОВ ПРОЕКТА (включая руководителя) **10**	ЧИСЛО УЧАСТНИКОВ, ИМЕЮЩИХ УЧЕНУЮ СТЕПЕНЬ **3**	ЧИСЛО МОЛОДЫХ (до 35 лет включительно) УЧАСТНИКОВ **9**
Степашкин Михаил Викторович		
Тишков Артем Валерьевич		
Сидельникова Екатерина Викторовна		
Чечулин Андрей Алексеевич		
Десницкий Василий Алексеевич		
Комашинский Дмитрий Владимирович		
Шоров Андрей Владимирович		
Резник Сергей Александрович		
Полубелова Ольга Витальевна		
ПОДПИСЬ РУКОВОДИТЕЛЯ ПРОЕКТА		ДАТА ПОДАЧИ ОТЧЕТА **14.01.2010**

ОТЧЕТ ЗА 2009 ГОД ПО ПРОЕКТУ РФФИ 07-01-00547-а

Статус отчета: подписан

Дата последнего изменения: 14.01.2010

Отчёт создал: Котенко Игорь Витальевич

Отчет распечатан: 14.01.2010

Форма 501. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1. *Номер проекта*
07-01-00547

1.2. *Руководитель проекта*
Котенко Игорь Витальевич

1.3. *Название проекта*
Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации, основывающиеся на моделировании поведения систем защиты, реализации верифицированных политик безопасности, оценке защищенности и проактивном мониторинге

1.4. *Вид конкурса*
а - Инициативные проекты

1.5. *Год представления отчета*
2010

1.6. *Вид отчета*
итоговый (2007-2009)

1.7. *Аннотация*
В результате работы над проектом разработаны и исследованы модели и методы проектирования, разработки и поддержания функционирования основывающихся на политиках безопасности, интеллектуальных адаптивных систем защиты информации (СЗИ) компьютерных систем функционирующих в открытых информационно-телекоммуникационных сетях.
Получены следующие основные результаты, существенно повышающие эффективность защиты информации в компьютерных системах:
(1) модели и методы защиты информации, реализующие интеллектуальную надстройку над традиционными механизмами защиты, в том числе сбор информации о состоянии информационной системы и ее анализ, проактивное предупреждение атак и препятствование их выполнению, обнаружение аномальной активности и явных атак, активное реагирование на попытки реализации действий нарушителей и дезинформацию злоумышленника;
(2) модели и методы построения единой унифицированной среды для создания и поддержки функционирования систем защиты информации на всем их жизненном цикле, в том числе спецификации и верификации политик безопасности, оценки защищенности, моделирования поведения механизмов защиты, реализации политик безопасности, проактивного мониторинга, а также адаптивного управления политиками безопасности.
Частными результатами работы являются: формальная постановка задачи исследования и основные требования к компонентам, реализующим интеллектуальные механизмы защиты и поддержку жизненного цикла распределенных защищенных компьютерных систем; принципы построения, структура и фрагмент основанной на онтологии распределенной базы знаний для интеллектуальных механизмов защиты; программная среда поддержки жизненного цикла распределенных защищенных компьютерных систем; формальные модели отдельных компонентов интеллектуальных механизмов защиты; проактивный подход к защите от сетевых червей, основанный на комбинировании различных механизмов обнаружения и сдерживания сетевых червей и автоматической настройке основных параметров механизмов защиты; программная реализация исследовательской среды для изучения компьютерных атак и механизмов защиты от них; модели защиты программного обеспечения на основе механизма удаленного доверия; теоретическая и экспериментальная оценка предложенных моделей и методов построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации и разработанной системы моделирования, а также рекомендации по их использованию для защиты информации в компьютерных сетях.

1.8. *Полное название организации, где выполняется проект*
Учреждение Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН

"Исполнители проекта согласны с опубликованием (в печатной и электронной формах) научных отчетов и перечня публикаций по проекту"

Подпись руководителя проекта

Форма 502. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ НА АНГЛИЙСКОМ ЯЗЫКЕ

2.1. *Номер проекта*
07-01-00547

2.2. *Руководитель проекта*
Kotenko Igor Vitalevich

2.3. *Название проекта*
Models and methods of construction and functioning support of intelligent adaptive security systems based on modeling and simulation of security systems behavior, realization of verified security policies, security evaluation and proactive monitoring

2.4. *Год представления отчета*
2010

2.5. *Вид отчета*
итоговый (2007-2009)

2.6. *Аннотация*

As a result of the project, we have developed and investigated the models and methods of design, development and maintenance of policy based intelligent adaptive security systems for protection of computer systems functioning in open information-telecommunication networks.
We have developed the following main results essentially raising the efficiency of information protection in computer systems:
(1) Models and methods of information protection which realize an intelligent superstructure above traditional security mechanisms, including collection and analysis of information on the status of information system, the proactive prevention of attacks and counteraction to their performance, detection of abnormal activity and obvious attacks, active reaction to attempts of malefactors' actions and their disinformation;
(2) Models and methods of construction of uniform unified environment for creation and support of security systems on all their life cycle, including the specification and verification of security policies, security evaluation, modelling and simulation of security mechanisms, realization of security policies, proactive monitoring, and also adaptive management of security policies.
Particular results of the project are as follows: the formal statement of the research problem and the main requirements to the components realizing the intelligent security mechanisms and the life cycle support of distributed protected computer systems; the principles of construction, the structure and a fragment of the distributed knowledge base for intelligent security mechanisms based on subject domain ontology; the life cycle support software environment of distributed protected computer systems; the formal models of particular components of intelligent security mechanisms; the proactive approach to protection against network worms which is based on a combination of various mechanisms of network worm detection and containment and automatic adjustment of key parameters of protection mechanisms; the software realization of the research environment for studying the computer attacks and protection mechanisms against them; the models of software protection based on remote entrusting mechanism; the theoretical and experimental evaluation of suggested models and methods for construction and support of intelligent adaptive information protection systems as well as the developed simulation system; the recommendations on their use for protection of the information in computer networks.

2.7. *Полное название организации, где выполняется проект*
Saint-Petersburg Institute for Informatics and Automation of Russian Academy of Sciences

Подпись руководителя проекта

Форма 503. РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер проекта
07-01-00547

3.2. Название проекта
Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации, основывающиеся на моделировании поведения систем защиты, реализации верифицированных политик безопасности, оценке защищенности и проактивном мониторинге

3.3. Коды классификатора, соответствующие содержанию фактически проделанной работы
01-201 01-202 01-217

3.4. Объявленные ранее (в исходной заявке) цели проекта на 2009 год
Основным содержанием работ по проекту на 2009 год являлось продолжение работ по разработке, прототипированию, теоретической и экспериментальной оценке моделей и методов построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации.
Основными целями проекта на 2009 год являлись
1. Уточнение и доработка формальных моделей и разработка программных прототипов обнаружения аномальной активности и явных атак, а также нелегитимных действий и отклонений работы пользователей от политики безопасности.
2. Уточнение и доработка формальных моделей и разработка программных прототипов механизмов поддержки жизненного цикла распределенных защищенных компьютерных систем, в частности механизмов верификации политики безопасности, основывающихся на методе проверки на модели, а также исчислении событий и абдуктивном выводе.
3. Доработка проактивного подхода к защите от сетевых червей и реализующих его программных прототипов, основанного на комбинировании различных механизмов обнаружения и сдерживания и автоматической настройке основных параметров механизмов защиты, и распространение его на другие классы вредоносного программного обеспечения.
4. Исследование моделей защиты программного обеспечения на основе механизма удаленного доверия, предназначенного для обнаружения несанкционированных изменений клиентской программы, функционирующей в потенциально враждебном окружении, с акцентом на разработку, исследование и верификацию адаптивных протоколов удаленного доверия.
5. Исследование гибридного подхода к моделированию сетевых атак и процессов защиты, основанного на комбинированном использовании записей трафика и генерации трафика на базе моделей и методов эмуляции, виртуализации и имитационного моделирования на уровне сетевых пакетов.
6. Продолжение исследований по теоретической и экспериментальной оценке предложенных моделей и методов построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации и разработанной системы моделирования, а также разработка рекомендаций по их использованию для защиты информации в компьютерных сетях и системах.

3.5. Степень выполнения поставленных в проекте задач
Все задачи, запланированные в проекте на второй год, выполнены полностью.

3.6. Полученные за отчетный период важнейшие результаты
Важнейшие результаты, полученные за отчетный период, таковы:
1. Формальные модели и программные прототипы обнаружения аномальной активности и явных атак, а также нелегитимных действий и отклонений работы пользователей от политики безопасности. Предложен подход к многоуровневому комбинированию алгоритмов обнаружения в виде системы базовых классификаторов, обрабатывающих данные о трафике, и мета-классификатора, осуществляющего выбор весовых коэффициентов для каждого алгоритма, что позволяет объединить достоинства отдельных методов и уменьшить их недостатки. Выбор весовых коэффициентов может осуществляться отдельно для каждого узла сети, что позволит учесть особенности работающих сетевых приложений на каждом хосте. Общий механизм обнаружения и противодействия сетевым атакам можно представить как совокупность следующих компонентов: сенсор – анализатор сетевого трафика; детектор – механизм обнаружения, принимающий на вход данные от анализаторов сетевого трафика и дающий на выходе правила фильтрации; мета-классификатор – модуль, принимающий на вход правила фильтрации от детекторов и дающий на выходе итоговые правила фильтрации, учитывающие вычисленные на основе данных от анализаторов весовые коэффициенты каждого детектора; фильтр – компонент блокирования, модификации или сдерживания трафика на основе правил, полученных от мета-классификатора. Предложенный подход рассматривается в качестве базиса, необходимого для формирования общей объединительной модели детектирования атак и вредоносного программного обеспечения, использующей сильные стороны существующих процедур извлечения, выделения, конструирования групп признаков и обучения классификаторов, обеспечивающих точное выявление отдельных структурных и функциональных аспектов исследуемых потенциально вредоносных файловых объектов.
2. Формальные модели и программные прототипы механизмов поддержки жизненного цикла распределенных защищенных компьютерных систем, в частности механизмов верификации политики безопасности, основывающихся на методе проверки на модели, а также исчислении событий и абдуктивном выводе. Использование преимуществ многомодульной архитектуры механизмов

верификации позволяет комбинировать модули общего назначения со специализированными методами. Модули общего назначения построены на основе методов доказательства теорем с использованием исчисления событий и методов проверки на модели. Они предоставляют возможность обрабатывать противоречия различных типов, в том числе и динамические. Специализированные методы направлены на более эффективную обработку противоречий конкретных типов. В частности, разработаны алгоритмы поиска и разрешения аномалий в правилах фильтрации политики безопасности компьютерной сети. Один из алгоритмов нахождения и разрешения аномалий в правилах фильтрации использует стратегию, которая заключается в разбиении условий правил межсетевого экрана на непересекающиеся части и удалении затененных частей (стратегия разбиения). Данная стратегия может применяться ко всем типам аномалий и ее применение не меняет поведение межсетевого экрана. Также предложен алгоритм нахождения аномалий всех типов, и нахождение аномалий только одного определенного типа. Рассмотрены алгоритмы применения всех типов стратегий разрешения аномалий и проведен их сравнительный анализ с точки зрения количества введения новых правил межсетевого экрана, возможных изменений работы межсетевого экрана, проведен анализ временной эффективности предложенных алгоритмов. Проведены эксперименты, в которых оценивалась эффективность применения предложенного подхода к верификации правил фильтрации политики безопасности компьютерной сети.

3. Проактивный подход к защите от вредоносного программного обеспечения и реализующие его программные прототипы, основанные на комбинировании различных механизмов обнаружения и сдерживания и автоматической настройке основных параметров механизмов защиты. Предложено использовать комбинацию следующих особенностей: "многорезолюционный" подход, сочетающий использование нескольких интервалов времени ("окон") наблюдения сетевого трафика и применение различных порогов для отслеживаемых параметров; гибридный подход, заключающийся в использовании различных алгоритмов и математических методов; многоуровневое комбинирование алгоритмов в виде системы базовых классификаторов, обрабатывающих данные о трафике, и мета-классификатора, осуществляющего выбор решения; адаптивные механизмы обнаружения и сдерживания вредоносного программного обеспечени, способные изменять критерии обнаружения на основе параметров сетевого трафика. Разработан программный комплекс моделирования и оценки механизмов обнаружения и сдерживания вредоносного программного обеспечения, который включает следующие компоненты: источники трафика или генератор трафика (формирующий нормальный трафик и трафик вредоносного программного обеспечения); анализатор трафика; библиотеки механизмов защиты от вредоносного программного обеспечения; сценарии тестирования и базовый тестовый комплекс или компонент оценки. Проведена серия экспериментов по исследованию данного подхода для выбора оптимальных параметров функционирования механизмов защиты.

4. Исследование моделей защиты программного обеспечения на основе механизма удаленного доверия, предназначенного для обнаружения несанкционированных изменений клиентской программы, функционирующей в потенциально враждебном окружении, с акцентом на разработку, исследование и верификацию адаптивных протоколов удаленного доверия. В рамках данного подхода контроль за выполнением клиентской программы делегируется удаленной доверенной сущности – доверенному серверу. Механизм предполагает в качестве своей составной части реализацию отдельных (атомарных) методов защиты, таких как проверка контрольных сумм, метод проверки инвариантов, метод Barrier Slicing, метод Control Flow Checking, Crypto Guards, Orthogonal Replacement, характеризующихся различными подходами к защите целевой программы, и различающихся по уровню предоставляемой защиты. Предложен механизм замещения мобильного модуля в клиентской программе на основе использования концепции аспектно-ориентированного программирования, в соответствии с которой различные функциональности клиентской программы программируются отдельно, а затем встраиваются в целевой код. Разработаны модели и методики, позволяющие достигнуть компромисса между уровнем предоставляемой защиты (безопасностью) и масштабируемостью механизма защиты. Такой компромисс достигается за счет выбора некоторой комбинации атомарных методов защиты, характеризуемых определенными значениями производительности и безопасности, при заданных ограничениях на потребляемые ресурсы сервера.

5. Исследование гибридного подхода к моделированию сетевых атак и процессов защиты, основанного на комбинированном использовании записей трафика и генерации трафика на базе моделей и методов эмуляции, виртуализации и имитационного моделирования на уровне сетевых пакетов. Особенности предлагаемого подхода: учитываются ключевые параметры исследуемых процессов (параметры сети и ее узлов, параметры команды атаки и реализации атаки, параметры команды защиты и механизмов защиты, параметры взаимодействия команд и др.); основные этапы моделирования автоматизированы; на основе выходных параметров производится оценка и сравнение различных механизмов защиты. Разработанные модели и методика моделировании могут быть обобщены для целей решения достаточно большого класса задач, в частности, задачи информационной борьбы в Интернет, конкуренции в сфере электронного бизнеса и др. Для реализации исследовательской среды использована архитектура системы моделирования, включающая базовую систему имитационного моделирования, модуль (пакет) моделирования сети Интернет, подсистему агентно-ориентированного моделирования и модуль (библиотеку) атак

"распределенный отказ в обслуживании" и механизмов защиты от них. Созданная среда моделирования позволяет проводить различные эксперименты с целью исследования стратегий реализации атак "распределенный отказ в обслуживании" и перспективных методов защиты от них. Проведены эксперименты по исследованию кооперативных механизмов защиты, включающих моделирование различных распределенных механизмов защиты. Исследовались также различные адаптивные схемы взаимодействия команд агентов как системы защиты, так и системы реализации атаки.

6. Теоретическая и экспериментальная оценка предложенных моделей и методов построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации и разработанной системы моделирования, а также разработка рекомендаций по их использованию для защиты информации в компьютерных сетях и системах. Проведенная теоретическая и экспериментальная оценка показала, что предложенный подход к построению и поддержке функционирования интеллектуальных адаптивных систем защиты и исследовательскую среду моделирования можно использовать для исследования эффективности разнообразных механизмов защиты, оценки защищенности существующих сетей и выработки рекомендаций для построения перспективных систем защиты.

3.7. Степень новизны полученных результатов

Основные научные результаты являются новыми.

Предлагаемый подход к построению информационно-безопасных распределенных систем, основанных на политиках безопасности, является новаторским и перспективным подходом к построению систем защиты информации в компьютерных сетях. Отличительной особенностью результатов является то, что они направлены на формализацию комплексного антагонистического характера обеспечения информационной безопасности как сложного организационно-технического процесса.

Система обеспечения информационной безопасности представляется в работе как единая холическая система, состояние которой определяется множеством взаимодействий между отдельными процессами кибер-противоборства и развивающегося динамического характера этих процессов, используя достижения в теории и практике построения многоагентных систем, современные тенденции в противоборстве методов нападения и защиты и перспективные подходы к обеспечению информационной безопасности.

3.8. Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения третьего года проекта, соответствуют мировому уровню.

Это подтверждается, в том числе, тем, что в 2009 г. авторы проекта опубликовали полученные результаты в нескольких журналах, сборниках и трудах конференций, в том числе в международных (в издательствах Springer, IEEE и др.), а также апробировали на множестве различных российских и международных конференций.

В 2009 г. руководитель проекта выступал с приглашенными пленарными докладами на нескольких российских и международных конференциях, в частности, на следующих конференциях: Санкт-Петербургский научный форум «Наука и общество» - Информационные технологии. 4-ая Петербургская встреча нобелевских лауреатов (Санкт-Петербург, 21-25 сентября 2009 г.); Четвертая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2009) (Санкт-Петербург, 21-23 октября 2009 г.); VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). (Санкт-Петербург, 28-30 октября 2009 г.).

Апробация результатов была также проведена на IV Международной конференции по проблемам управления МКПУ-IV (Сессия «Многоагентные системы и групповое управление». Москва, 26-30 января 2009 г.), 17-й Европейской (Euromicro) международной конференции по параллельной, распределенной и сетевой обработке информации PDP 2009 (Веймар, Германия. 18-20 февраля 2009 г.), Одиннадцатой конференции "РусКрипто'2009" по криптологии, стеганографии, цифровой подписи и системам защиты информации (Звенигород, Россия. 3-5 апреля 2009 г.), 4-м Международном семинаре "Интеграция информации и геоинформационные системы" (IF&GIS-2009) (Санкт-Петербург, Россия. 17-20 мая 2009 г.), 23-й Европейской конференции по моделированию (ECMS 2009) (Мадрид, Испания. 9-12 июня 2009 г.), XVIII Общероссийской научно-технической конференции "Методы и технические средства обеспечения безопасности информации (МТСОБИ 2009)" (Санкт-Петербург - Валаам, 29 июня - 2 июля 2009 г.), Международной конференции "Интеллектуальные системы (AIS 2009)" (Дивноморское, 3-10 сентября 2009 г.), Пятом IEEE Международном семинаре "Интеллектуальное приобретение знаний и передовые компьютерные системы: технологии и приложения" (IDAACS'2009) (Ренде, Италия, 21-23 сентября 2009 г.), Втором международном семинаре по удаленному доверию RE-TRUST 2008 (Рива дель Гарда, Италия, 30 сентября - 1 октября, 2009 г.), Международной конференции и выставке JETRO BIZMATCH CEATEC JAPAN 2009 (Япония, Чиба, 4-11 октября 2009 г.), Пятой международной научной конференции по проблемам безопасности и противодействия терроризму и Восьмой общероссийской научной конференции "Математика и безопасность информационных технологий" (МаБИТ-2009) (Москва, Россия. 29-30 октября 2009 г.) и др.

3.9. Методы и подходы, использованные в ходе выполнения проекта

В качестве базиса для исследований использовались работы в следующих областях: агентно-ориентированное моделирование; командная работа агентов; системы вывода, основанные на предсказании намерений и планов оппонента; рефлексивные процессы; теоретико-игровое моделирование; моделирование атак на компьютерные сети; моделирование процессов защиты информации; системы защиты, основанные на политиках безопасности; теория адаптивного управления, интеллектуальный анализ данных и др.

Для решения задач, связанных с моделированием компьютерного противоборства использовались методы и модели гибридного многоагентного моделирование сложных распределенных сетевых атак и механизмов защиты от них, в том числе аппаратные стенды, эмуляция, виртуализация, модели на пакетном уровне, гибридные системы, аналитические модели.

При разработке предложенных формальных постановок, моделей, архитектур и прототипов применены методы системного анализа и теории больших систем, методы распределенного искусственного интеллекта, теории защиты информации, теории имитационного моделирования, теории слияния информации, обнаружения знаний и данных, методы объектно-ориентированного проектирования, теории протоколов и языков взаимодействия агентов, формальной логики и проверки на модели (model checking).

3.10.1. Количество научных работ, опубликованных в ходе выполнения проекта

138

3.10.2. Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в 2009 г.

40

3.11. Участие в научных мероприятиях по тематике проекта, которые проводились при финансовой поддержке Фонда

4

3.12. Участие в экспедициях по тематике проекта, проводимых при финансовой поддержке Фонда

3.13. Финансовые средства, полученные от РФФИ

3.14. Вычислительная техника и научное оборудование, приобретенные на средства Фонда

3.15. Адреса (полностью) ресурсов в Internet, подготовленных авторами по данному проекту

http://comsec.spb.ru/index.cgi?l=ru&m=Staff&p=Kotenko
http://comsec.spb.ru/index.cgi?l=en&m=Staff&p=Kotenko
http://comsec.spb.ru/index.cgi?l=ru&m=Projects&p=
http://comsec.spb.ru/index.cgi?l=en&m=Projects&p=

3.16. Библиографический список всех публикаций по проекту

1. Котенко И.В., Уланов А.В. Многоагентное моделирование защиты информационных ресурсов компьютерных сетей в сети Интернет // Известия РАН. Теория и системы управления, № 5, 2007, С.74-88. ISSN 0002-3388.

2. Котенко И.В., Воронцов В.В., Чечулин А.А., Уланов А.В. Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов // Информационные технологии, № 1, 2009. С.37-42. ISSN 1684-6400.

3. Котенко И.В., Уланов А.В. Многоагентное моделирование механизмов защиты от распределенных компьютерных атак // Информационные технологии, № 2, 2009. С.38-44. ISSN 1684-6400.

4. Котенко И.В., Юсупов Р.М. Технологии компьютерной безопасности // Вестник РАН, Т.77, № 4, 2007. С.323-333. ISSN 0869-5873.

5. Котенко И.В., Уланов А.В. Агентно-ориентированная среда для моделирования и оценки механизмов защиты от распределенных атак "Отказ в обслуживании" // Изв. вузов. Приборостроение, Т.50, № 1, 2007. С.18-21. ISSN 0021-3454.

6. Десницкий В.А., Котенко И.В. Защита программного обеспечения на основе механизма "удаленного доверия" // Изв. вузов. Приборостроение, Т.51, № 11 , 2008. С.26-30. ISSN 0021-3454.

7. Воронцов В.В., Котенко И.В. Анализ механизма обнаружения и сдерживания эпидемий сетевых червей на основе «кредитов доверия» // Изв. вузов. Приборостроение, Т.51, № 11, 2008. С.21-26. ISSN 0021-3454.

8. Сидельникова Е.В., Тишков А.В., Котенко И.В. Верификация политик фильтрации с помощью исчисления событий и абдуктивного вывода // Изв. вузов. Приборостроение, Т.51, № 11, 2008. С.31-35. ISSN 0021-3454.

9. Полубелова О.В., Котенко И.В. Верификация правил фильтрации политики безопасности методом "проверки на модели" // Изв. вузов. Приборостроение, Т.51, № 12, 2008. С.44-49. ISSN 0021-3454.

10. Котенко И.В., Тишков А.В., Черватюк О.В., Резник С.А., Сидельникова Е.В. Система верификации политики безопасности компьютерной сети // Вестник компьютерных и информационных технологий, № 11, 2007. С.48-56. ISSN 1810-7206.

11. Kotenko I. Multi-agent modeling and the simulation of computer network security processes: "a game of network cats and mice" // NATO Science for Peace and Security Series, D: Information and Communication Security. Volume 17, 2008. Aspects of Network and Information Security. P.56-73. ISBN

978-1-58603-856-4.
12. Kotenko I. Multi-agent Simulation of Attacks and Defense Mechanisms in Computer Networks // The Journal of Computing, Vol. 7, Issue 2, 2008. P.35-43.
13. Котенко И.В., Десницкий В.А. Аспектно-ориентированная реализация модели защиты программ на основе "удаленного доверия" // Информационные технологии и вычислительные системы, 2010. (Принята к печати).
14. Котенко И.В., Уланов А.В. Моделирование адаптивной кооперативной защиты от компьютерных атак в сети Интернет // Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Том 31. Москва, URSS, 2007. С.103-125. ISBN 978-5-382-00620-8.
15. Котенко И.В., Степашкин М.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Том 31. Москва, URSS, 2007. С.126-207. ISBN 978-5-382-00620-8.
16. Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью // Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Т.41, Москва, URSS, 2009. С.74-103. ISBN 978-5-9710-0255-0.
17. Комашинский Д.В., Котенко И.В. Детектирование вредоносного программного обеспечения на основе обработки статической информации методами интеллектуального анализа данных // Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Т. , Москва, URSS, 2010. (Принята к печати).
18. Десницкий В.А., Котенко И.В. Защищенность и масштабируемость механизма защиты программного обеспечения на основе принципа удаленного доверия // Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Т. , Москва, URSS, 2010. (Принята к печати).
19. Котенко И. В., Воронцов В. В. Аналитические модели распространения сетевых червей // Труды СПИИРАН. Вып.4, т.1. СПб.: Наука, 2007. С.208-224. ISBN 978-5-02-025165-6.
20. Котенко И. В., Воронцов В. В., Уланов А. В. Модели и системы имитационного моделирования распространения сетевых червей // Труды СПИИРАН. Вып.4, т.1. СПб.: Наука, 2007. С.225-238. ISBN 978-5-02-025165-6.
21. Котенко И.В., Резник С.А., Шоров А.В. Верификация протоколов безопасности на основе комбинированного использования существующих методов и средств // Труды СПИИРАН, Выпуск 8, Том 2. СПб.: Наука, 2009. С. 292-310. ISBN 978-5-02-025381-0.
22. Уланов А.В., Котенко И.В. Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. Инсайд, № 1, 2007. С.60-67; № 2, 2007. С.70-77; № 3, 2007. С.62-69.
23. Богданов В.С., Котенко И.В. Проактивный мониторинг выполнения политики безопасности в компьютерных сетях // Защита информации. Инсайд, № 3, 2007. С.42-47; № 4, 2007. С.66-72.
24. Котенко И.В., Уланов А.В. Компьютерные войны в Интернете: моделирование противоборства программных агентов // Защита информации. Инсайд, № 4, 2007. С.38-45.
25. Котенко И.В. Автоматическое обнаружение и сдерживание распространения Интернет-червей: краткий анализ современных исследований // Защита информации. Инсайд, № 4, 2007. С.46-56.
26. Котенко И.В. Международная конференция "Математические модели, методы и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2007) // Защита информации. Инсайд, № 3, 2007, С.12; № 4, 2007, С.56.
27. Котенко И.В., Тишков А.В., Сидельникова Е.В., Черватюк О.В. Проверка правил политики безопасности для корпоративных компьютерных сетей // Защита информации. Инсайд, № 5, 2007. С.46-49; № 6, 2007. С.52-59.
28. Котенко И.В., Чечулин А.А. Исследование механизмов защиты от сетевых червей на основе методик Virus Throttling // Защита информации. Инсайд, № 3, 2008. С.68-73.
29. Десницкий В.А., Котенко И.В., Резник С.А. Разработка и верификация протокола обмена сообщениями для защиты программ на основе механизма "удаленного доверия" // Защита информации. Инсайд, № 4, 2008. С.59-63; № 5, 2008. С.68-74.
30. Котенко И.В., Юсупов Р.М. Информационные технологии для борьбы с терроризмом // Защита информации. Инсайд, № 2, 2009. С.74-79.
31. Резник С.А., Котенко И.В. Методы и средства верификации для комбинированного анализа протоколов безопасности // Защита информации. Инсайд, № 3, 2009. С.56-72.
32. Десницкий В.А., Котенко И.В. Методы защиты программного обеспечения на основе принципа удаленного доверия // Защита информации. Инсайд, № 6, 2009. С.57-61.
33. Комашинский Д.В., Котенко И.В. Концептуальные основы использования методов Data Mining для обнаружения вредоносного программного обеспечения // Защита информации. Инсайд, 2010. № 1-2. (Принята к печати)
34. Mathematical Methods, Models and Architectures for Computer Networks Security. Communications in Computer and Information Science (CCIS). Springer. Vladimir Gorodetsky, Igor Kotenko, Victor Skormin (Eds.). Vol.1, 2007. 416 p. ISSN 1865-0929.
35. Котенко И.В., Уланов А.В. Моделирование адаптации противоборствующих команд

интеллектуальных агентов // КИИ-2008. XI Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Том 1. М.: URSS, 2008. С.32-40. ISBN 978-5-9710-0226-0.
36. Котенко И.В., Юсупов Р.М. Противодействие кибертерроризму: актуальные проблемы и перспективные направления исследований // Санкт-Петербургский научный форум «Наука и общество»: Информационные технологии. 4-ая Петербургская встреча нобелевских лауреатов. Тезисы докладов. Санкт-Петербург. 2009. С.329-332.
37. Степашкин М.В., Котенко И.В. Анализ защищенности компьютерных сетей и систем на основе построения деревьев атак // Санкт-Петербургский научный форум «Наука и общество»: Информационные технологии. 4-ая Петербургская встреча нобелевских лауреатов. Тезисы докладов. Санкт-Петербург. 2009. С.363-366.
38. Kotenko I.V., Ulanov A.V. Multi-agent Framework for Simulation of Adaptive Cooperative Defense against Internet Attacks // Lecture Notes in Artificial Intelligence, Vol.4476. Springer. 2007. P.212-228. ISSN 0302-9743.
39. Kotenko I., Tishkov A., Chervatuk O., Sidelnikova E. Security Policy Verification Tool for Geographical Information Systems // Information Fusion and Geographical Information Systems. Lecture Notes in Geoinformation and Cartography. Springer. 2007. P.128-146. ISSN 1863-2246.
40. Bourgeois J., Ganame A.K., Kotenko I., Ulanov A. Software Environment for Simulation and Evaluation of a Security Operation Center // Information Fusion and Geographical Information Systems. Lecture Notes in Geoinformation and Cartography. Springer. 2007. P.111-127. ISSN 1863-2246.
41. Desnitsky V., Kotenko I. Design of Entrusting Protocols for Software Protection // Information Fusion and Geographic Information Systems. Lecture Notes in Geoinformation and Cartography. Springer. 2009. P.301-316. ISSN 1863-2246. ISBN 978-3-642-00303-5.
42. Komashinskiy D., Kotenko I. Using Data Mining methods for malware detection // Information Fusion and Geographic Information Systems. Lecture Notes in Geoinformation and Cartography. Springer. 2009. P.343-357. ISSN 1863-2246. ISBN 978-3-642-00303-5.
43. Kotenko I., Ulanov A. Agent-based Simulation Environment and Experiments for Investigation of Internet Attacks and Defense Mechanisms // Proceedings of 21th European Conference on Modelling and Simulation (ECMS 2007). Prague, Czech Republic. 4-6 June 2007. P.146-155. ISBN 978-0-9553018-2-7.
44. Kotenko I. Simulation of Agent Teams: the Application of Domain-Independent Framework to Computer Network Security // 23rd European Conference on Modelling and Simulation (ECMS 2009). Madrid, Spain. June 9-12, 2009. P.137-143. ISBN 0-9553018-8-2.
45. Kotenko I., Chervatuk O., Sidelnikova E., Tishkov A. Hybrid Multi-module Security Policy Verification // 2007 IEEE Workshop on Policies for Distributed Systems and Networks (Policy 2007). 13-15 June 2007. Bologna, Italy. 2007. P.277. ISBN 0-7695-2767-1.
46. Kotenko I. Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security // Proceedings of IEEE Fourth International Workshop on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS 2007). Dortmund, Germany, 6-8 September, 2007. P.614-619. ISBN 1-4244-1348-6.
47. Kotenko I., Bogdanov V. Proactive Monitoring of Security Policy Accomplishment in Computer Networks // Proceedings of IEEE Fourth International Workshop on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS 2009). Rende (Cosenza), Italy, September 21-23, 2009. P.364-369. ISBN 978-1-4244-4882-1.
48. Bogdanov V., Kotenko I. Policy-based Proactive Monitoring of Security Policy Performance // Communications in Computer and Information Science (CCIS). Springer. Vol.1, 2007. P.197-212. ISSN 1865-0929.
49. Tishkov A., Sidelnikova E., Kotenko I. Event Calculus based Checking of Filtering Policies // Communications in Computer and Information Science (CCIS). Springer. Vol.1, 2007. P.248-253. ISSN 1865-0929.
50. Kotenko I., Ulanov A. Investigation of Cooperative Defense against DDoS // SECRYPT 2007. International Conference on Security and Cryptography. Proceedings. Barcelona, Spain. 28-31 July 2007. P.180-183. ISBN 978-989-8111-12-8.
51. Kotenko I., Ulanov A. Packet Level Simulation of Cooperative Distributed Defense against Internet Attacks // Proceedings of the 16th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2008). Toulouse, France. February 13-15 2008. IEEE Computer Society. 2008. P.565-572. ISBN 0-7695-3089-3. ISSN 1066-6192.
52. Kotenko I. Framework for Integrated Proactive Network Worm Detection and Response // Proceedings of the 17th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2009). Weimar, Germany. February 18-20, 2009. IEEE Computer Society. 2009. P.379-386. ISSN 1066-6192. ISBN 978-0-7695-3544-9.
53. Desnitsky V., Kotenko I. Analysis and Design of Entrusting Protocol for Distributed Software Protection // Proceedings of the Work in Progress Session held in connection with the 17th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2009). Weimar, Germany. February 2009. SEA-Publications: SEA-SR-21. 2009. P.8-9. ISBN 978-3-902457-21-9.
54. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro International Conference on Parallel, Distributed

and network-based Processing (PDP 2010). Pisa, Italy, 17-19 February, 2010. IEEE Computer Society. 2010. (Принята к печати)
55. Kotenko I., Ulanov A. Simulation of Adaptable Agent Teams in Internet // Proceedings of the 1st International Workshop on Logics for Agents and Mobility (LAM 2008). The European Summer School on Logic, Language and Information (ESSLLI 2008), Hamburg, Germany. 4 - 15 August, 2008. P.67-79.
56. Desnitsky V., Kotenko I. Performance and Scalability of Remote Entrusting Protection // Second International Workshop on Remote Entrusting (RE-TRUST 2009). September 30 - October 1, 2009. Riva del Garda, Italy, 2009. (Принята к печати)
57. Котенко И.В. Актуальные проблемы моделирования процессов защиты информации на основе технологии интеллектуальных агентов // Известия СПбГЭТУ "ЛЭТИ". Специальный выпуск. Проблемы информатики: философия, науковедение, образование. СПб.: СПбГЭТУ "ЛЭТИ", 2007. С.93-109.
58. Котенко И.В., Уланов А.В. Противостояние в Интернет: моделирование противодействия распределенным кибератакам // Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2007. С.485-494.
59. Богданов В.С., Котенко И.В. Проактивный подход к мониторингу выполнения политики безопасности компьютерных сетей // Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2007. С.373-382.
60. Тишков А.В., Котенко И.В., Сидельникова Е.В., Черватюк О.В. Обнаружение и разрешение противоречий в политиках безопасности // Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2007. С.172-185.
61. Котенко И.В., Степашкин М.В. Оценка защищенности компьютерных сетей на основе анализа графов атак // Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2007. С.466-481.
62. Котенко И.В., Воронцов В.В., Тишков А.В., Чечулин А.А., Уланов А.В. Исследование проактивных механизмов защиты от сетевых червей // Проблемы безопасности и противодействия терроризму. Материалы третьей международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2008. С.278-283.
63. Уланов А.В., Котенко И.В. Моделирование кооперативных механизмов защиты компьютерных сетей // Проблемы безопасности и противодействия терроризму. Материалы третьей международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2008. С.266-271.
64. Десницкий В.А., Котенко И.В. Проектирование и анализ протокола удаленного доверия // Проблемы безопасности и противодействия терроризму. Материалы четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. Том 2. М.: МЦНМО, 2009. С.214-219. ISBN 978-5-94057-503-0.
65. Комашинский Д.В., Котенко И.В. Исследование проактивных механизмов обнаружения вредоносного программного обеспечения на базе методов DATA MINING // Проблемы безопасности и противодействия терроризму. Материалы четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. Том 2. М.: МЦНМО, 2009. С.226-231. ISBN 978-5-94057-503-0.
66. Чечулин А.А., Котенко И.В. Защита от сетевых атак методами фильтрации и нормализации протоколов транспортного и сетевого уровня стека TCP/IP // Проблемы безопасности и противодействия терроризму. Материалы четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. Том 2. М.: МЦНМО, 2009. С.242-247. ISBN 978-5-94057-503-0.
67. Десницкий В.А., Котенко И.В. Защита программного обеспечения на основе принципа удаленного доверия // Восьмая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2009). Москва, МГУ, 2010. (Принята к печати)
68. Комашинский Д.В., Котенко И.В. Обнаружение malware на основе обработки статической позиционной информации методами Data Mining // Восьмая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2009). Москва, МГУ, 2010. (Принята к печати)
69. Уланов А.В. Модели противоборства команд агентов, реализующих атаки «распределенный отказ в обслуживании» и механизмы защиты от них // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 07)" и "Интеллектуальные САПР (CAD-2007)". М.: Физматлит, 2007. С.120-127.
70. Котенко И.В., Воронцов В.В. Проактивный подход к обнаружению и сдерживанию сетевых червей // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 07)" и "Интеллектуальные САПР (CAD-2007)". Том.2. М.: Физматлит, 2007. С.61-68.
71. Десницкий В.А., Котенко И.В. Модели удаленной аутентификации для защиты программ // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 07)" и "Интеллектуальные САПР (CAD-2007)". Том.3. М.: Физматлит, 2007. С.43-50.

72. Котенко И.В., Тишков А.В., Воронцов В.В. Комбинирование механизмов защиты от злонамеренного программного обеспечения // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 08")" и "Интеллектуальные САПР (CAD-2008)". Том 2. М.: Физматлит, 2008. С.426-432. ISBN 978-5-9221-0856-0.
73. Десницкий В.А., Котенко И.В., Резник С.А. Разработка и анализ протокола обмена сообщениями для механизма удаленного доверия // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 08)" и "Интеллектуальные САПР (CAD-2008)". Том 2. М.: Физматлит, 2008. С.418-425. ISBN 978-5-9221-0856-0.
74. Котенко И.В. Интеллектуальные механизмы защиты от распространения злонамеренного программного обеспечения // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 09)" и "Интеллектуальные САПР (CAD-2009)". Том 2. М.: Физматлит, 2009. С.431-438. ISBN 978-5-9221-0856-0.
75. Котенко И.В. Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации // Математические методы распознавания образов: 13-я Всероссийская конференция (ММРО-13). Ленинградская обл., г. Зеленогорск, 30 сентября - 6 октября 2007 г.: Сборник докладов. М.: МАКС Пресс, 2007. С.599-602.
76. Уланов А.В., Котенко И.В. Многоагентная среда для проведения экспериментов по защите компьютерных сетей // Математические методы распознавания образов: 13-я Всероссийская конференция (ММРО-13). Ленинградская обл., г. Зеленогорск, 30 сентября - 6 октября 2007 г.: Сборник докладов. М.: МАКС Пресс, 2007. С.631-634.
77. Котенко И.В., Уланов А.В. Исследование моделей противоборства агентов в компьютерных сетях // Мультиконференция «Теория и системы управления». IV Международная конференция по проблемам управления (МКПУ-IV). Сессия «Многоагентные системы и групповое управление». М., 26-30 января 2009 г. CD ROM. ISBN 978-5-91450-026-6.
78. Уланов А.В., Котенко И.В. Моделирование адаптивных кооперативных стратегий защиты от компьютерных атак в сети Интернет // Третья всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2007). Санкт-Петербург, 17-19 октября 2007 г. Сборник докладов. СПб.: ФГУП ЦНИИ технологии судостроения. 2007. Том II. С.211-215. ISBN 978-5-98361-048-4.
79. Котенко И.В., Уланов А.В., Тишков А.В., Богданов В.С., Воронцов В.В., Чечулин А.А. Имитационное моделирование механизмов обнаружения и сдерживания сетевых червей в компьютерных сетях // Третья всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2007). Санкт-Петербург, 17-19 октября 2007 г. Сборник докладов. СПб.: ФГУП ЦНИИ технологии судостроения. 2007. Том II. С.106-109. ISBN 978-5-98361-048-4.
80. Котенко И.В. Многоагентное моделирование для исследования механизмов защиты информации в сети Интернет // Четвертая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2009). Санкт-Петербург, 21-23 октября 2009 г. Сборник докладов. СПб.: ОАО "Центр технологии судостроения и судоремонта". 2009. Том I. С.38-47. ISBN 978-5-902241-21-8.
81. Котенко И.В., Юсупов Р.М. Актуальные исследования в области защиты компьютерных сетей и систем // V Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции. Санкт-Петербург. 2008. С. 21-31.
82. Котенко И.В., Воронцов В.В., Чечулин А.А. Анализ механизмов обнаружения и сдерживания сетевых червей // V Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции. Санкт-Петербург. 2008. С.113-119.
83. Десницкий В.А., Котенко И.В. Модель защиты программ на основе механизма "удаленного доверия" // V Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции. Санкт-Петербург. 2008. С.172-177.
84. Котенко И.В., Воронцов В.В. Использование проактивного подхода для защиты от сетевых червей // Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН, 2007. С.41-44.
85. Десницкий В.А., Котенко И.В. Удаленная аутентификация для защиты программ от несанкционированного изменения // Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН, 2007. С.32-34.
86. Уланов А.В. Методика проведения имитационного моделирования противостояния систем защиты атакам DDOS в сети Интернет // Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН, 2007. С.38-40.
87. Десницкий В.А. Аспектно-ориентированный подход к реализации механизма мобильного модуля в системе защиты программного обеспечения // Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН, 2007. С.35-37.
88. Котенко И.В., Уланов А.В. Исследование механизмов защиты от атак DDOS: имитация противоборства интеллектуальных агентов в сети Интернет // Международная конференция "РусКрипто 2008". 2008. CD ROM. http://www.ruscrypto.ru/
89. Котенко И.В. Проактивные механизмы защиты от быстро распространяющихся сетевых червей //

Международная конференция "РусКрипто 2008". 2008. CD ROM. http://www.ruscrypto.ru/
90. Котенко И.В. "Сетевые кошки-мышки": войны адаптивных программных агентов // Международная конференция "РусКрипто 2009". CD ROM. http://www.ruscrypto.ru/
91. Десницкий В.А., Котенко И.В. Подход к защите программ на основе механизма удаленного доверия // Международная конференция "РусКрипто 2009". CD ROM. http://www.ruscrypto.ru/
92. Комашинский Д.В., Котенко И.В., Шоров А.В. Обнаружение вредоносного программного обеспечения на базе методов интеллектуального анализа данных // Международная конференция "РусКрипто 2009". CD ROM. http://www.ruscrypto.ru/
93. Чечулин А.А., Зозуля Ю.В., Котенко И.В., Тишков А.В., Шоров А.В. Методы защиты от вредоносных Web-сайтов на основе оценок репутации // Международная конференция "РусКрипто 2009". CD ROM. http://www.ruscrypto.ru/
94. Богданов В.С., Котенко И.В. Проактивный мониторинг выполнения политики безопасности компьютерной сети // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.32.
95. Котенко И.В., Воронцов В.В., Уланов А.В. Проактивное обнаружение и сдерживание распространения сетевых червей // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.91.
96. Котенко И.В., Уланов А.В. Моделирование адаптивного противостояния систем защиты распределенным атакам // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.92.
97. Резник С.А., Черватюк О.В. Обнаружение конфликтов фильтрации и защиты каналов в политике безопасности на основе методов верификации на модели // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.37.
98. Десницкий В.А. Удаленная аутентификация как механизм защиты программ на удаленных клиентах // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.5.
99. Уланов А.В. Архитектура и модель среды многоагентного моделирования атак DDoS и защиты от них // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.96.
100. Воронцов В.В. Моделирование распространения сетевых червей // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.88.
101. Десницкий В.А., Котенко И.В., Резник С.А. Разработка и анализ протокола обмена сообщениями для защиты программ посредством "удаленного доверия" // Методы и технические средства обеспечения безопасности информации. Материалы XVII Общероссийской научно-технической конференции. 7-11 июля 2008 года. Санкт-Петербург. Издательство Политехнического университета. 2008. С.16.
102. Котенко И.В., Воронцов В.В., Чечулин А.А. Обнаружение и сдерживание распространения злонамеренного программного обеспечения на основе комбинированных механизмов // Методы и технические средства обеспечения безопасности информации. Материалы XVII Общероссийской научно-технической конференции. 7-11 июля 2008 года. Санкт-Петербург. Издательство Политехнического университета. 2008. С.27.
103. Котенко И.В. Моделирование процессов защиты информации от инфраструктурных атак // Методы и технические средства обеспечения безопасности информации. Материалы XVIII Общероссийской научно-технической конференции. 29 июня - 2 июля 2009 года. Санкт-Петербург. Издательство Политехнического университета. 2009. С.63.
104. Комашинский Д.В., Котенко И.В., Шоров А.В. Технология детектирования вредоносного программного обеспечения на основе методов Data Mining // Методы и технические средства обеспечения безопасности информации. Материалы XVIII Общероссийской научно-технической конференции. 29 июня - 2 июля 2009 года. Санкт-Петербург. Издательство Политехнического университета. 2009. С.122-123.
105. Шоров А.В., Коновалов А.М., Котенко И.В. Исследовательское моделирование бот-сетей и механизмов защиты от них // Методы и технические средства обеспечения безопасности информации. Материалы XVIII Общероссийской научно-технической конференции. 29 июня - 2 июля 2009 года. Санкт-Петербург. Издательство Политехнического университета. 2009. С.132.
106. Чечулин А.А., Котенко И.В. Обнаружение и противодействие сетевым атакам на основе комбинированных механизмов анализа трафика // Методы и технические средства обеспечения безопасности информации. Материалы XVIII Общероссийской научно-технической конференции. 29

июня - 2 июля 2009 года. Санкт-Петербург. Издательство Политехнического университета. 2009. С.69.
107. Котенко И.В., Юсупов Р.М. Актуальные проблемы и решения в области защиты компьютерных сетей и систем // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.55-56. ISBN 978-5-7187-0824-X.
108. Тишков А.В., Котенко И.В. Система защиты компьютерной сети, основанная на политике безопасности // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.122-123. ISBN 978-5-7187-0824-X.
109. Десницкий В.А., Котенко И.В. Модель защиты программ от несанкционированных изменений на основе механизма удаленного доверия // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.81. ISBN 978-5-7187-0824-X.
110. Воронцов В.В., Котенко И.В. Модели обнаружения и сдерживания сетевых червей на основе проактивного подхода // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.47-48. ISBN 978-5-7187-0824-X.
111. Чечулин А.А., Котенко И.В. Механизмы защиты от сетевых червей на основе метода порогового случайного прохождения // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.70. ISBN 978-5-7187-0824-X.
112. Воронцов В.В. Механизм обнаружения и ограничения распространения сетевых червей на основе кредитов доверия // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.46-47. ISBN 978-5-7187-0824-X.
113. Десницкий В.А. Реализация механизма замещения мобильного модуля на основе парадигмы аспектно-ориентированного программирования // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.49-50.
114. Сидельникова Е.В. Верификация правил фильтрации с помощью исчисления событий и абдуктивного вывода // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.95. ISBN 978-5-7187-0824-X.
115. Черватюк О.В. Верификация правил фильтрации политики безопасности методом проверки на модели // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.69-70. ISBN 978-5-7187-0824-X.
116. Чечулин А.А. Исследование механизмов обнаружения и сдерживания сетевых червей, базирующихся на методике "Virus Throttling" // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.99-100. ISBN 978-5-7187-0824-X.
117. Котенко И.В., Юсупов Р.М. Информационные технологии для борьбы с терроризмом // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.39-40. ISBN 978-5-7187-0824-X.
118. Шоров А.В., Котенко И.В. Защита компьютерной сети от инфраструктурных атак на основе реализации "нервной системы сети" // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.118-119.
119. Богданов В.С. Оптимизация тестирования политики безопасности компьютерных сетей // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.93.
120. Десницкий В.А. Разработка и анализ протокола для защиты программ от злонамеренных изменений // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.98-99.
121. Комашинский Д.В. Проактивная технология обнаружения вредоносного программного обеспечения на базе методов интеллектуального анализа данных (Data Mining) // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.101.
122. Коновалов А.М. Моделирование сетевого трафика в задачах защиты от инфраструктурных сетевых угроз // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.101-102.
123. Котенко Д.И. Построение графа атак для оценки защищенности компьютерной сети // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.102-103.
124. Полубелова О.В. Верификация правил фильтрации политики безопасности, содержащих временные параметры, методом проверки на модели // XI Санкт-Петербургская Международная

Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.110-111.
125. Резник С.А. Комплексный подход к верификации протоколов безопасности на примере протокола RE-TRUST // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.111.
126. Сидельникова Е.В. Абдуктивный конфигуратор правил фильтрации межсетевого экрана // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.112.
127. Чечулин А.А. Защита от сетевых атак методами нормализации протоколов транспортного и сетевого уровня стека TCP/IP // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.115-116.
128. Сидельникова Е.В. Верификация политик фильтрации с помощью исчисления событий и абдуктивного вывода // V Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции. Санкт-Петербург. 2008. С.133-136.
129. Котенко И.В. Построение и поддержка функционирования интеллектуальных систем защиты информации // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.112. ISBN 978-5-904031-05-3.
130. Десницкий В.А. Масштабируемость и безопасность механизма защиты на основе принципа удаленного доверия // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.98. ISBN 978-5-904031-05-3.
131. Десницкий В.А. Конфигурирование механизма защиты при помощи политик безопасности // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.97-98. ISBN 978-5-904031-05-3.
132. Зозуля Ю.В. Определение категории Веб-сайта для решения задачи родительского контроля // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.53-54. ISBN 978-5-904031-05-3.
133. Комашинский Д.В. Построение модели статического детектирования вредоносного программного обеспечения на базе методов Data Mining // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.56-57. ISBN 978-5-904031-05-3.
134. Коновалов А.М. Моделирование ботнетов а основе множества взаимодействующих интеллектуальных агентов // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.58. ISBN 978-5-904031-05-3.
135. Резник С.А. Комбинированные подходы к верификации протоколов безопасности // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.122-123. ISBN 978-5-904031-05-3.
136. Сидельникова Е.В. Верификация правил фильтрации политики безопасности компьютерной сети на основе исчисления событий и абдуктивного вывода // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.139-140. ISBN 978-5-904031-05-3.
137. Чечулин А.А. Обнаружение и противодействие сетевым атакам на основе комбинированных механизмов анализа трафика // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.143-144. ISBN 978-5-904031-05-3.
138. Шоров А.В. Анализ биологических подходов для защиты компьютерных сетей от инфраструктурных атак // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.145. ISBN 978-5-904031-05-3.

3.17. Приоритетное направление развития науки, технологий и техники РФ, в котором, по мнению исполнителей, могут быть использованы результаты данного проекта

безопасность и противодействие терроризму

3.18. Критическая технология РФ, в которой, по мнению исполнителей, могут быть использованы результаты данного проекта

технологии обработки, хранения, передачи и защиты информации

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
@Многоагентное моделирование защиты информационных ресурсов компьютерных сетей в сети Интернет

9.5. Язык публикации
русский

9.6.1. Полное название издания
Известия РАН. Теория и системы управления

9.6.2. ISSN издания
0002-3388

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания
5

9.11. Страницы
74-88

9.12.1. Полное название издательства
Наука

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предлагается подход к исследованию механизмов защиты информационных ресурсов в сети Интернет, основанный на многоагентном моделировании. В соответствии с данным подходом системы защиты представляются в виде взаимодействующих команд интеллектуальных агентов. Представлена архитектура и программная реализация среды моделирования, позволившая комплексировать моделирование на основе дискретных событий, многоагентный подход и имитацию обмена сетевыми пакетами по различным протоколам Интернет. Разработанная среда обеспечивает проведение анализа сложных сценариев атак и механизмов защиты от них. Представлены результаты экспериментов по исследованию кооперативных механизмов защиты от атак "распределенный отказ в обслуживании". Продемонстрирована перспективность реализации таких механизмов для защиты от распределенных атак в сети Интернет.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
23

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В.В. Воронцов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАНА.А.Чечулин; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАНА.В.Уланов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы
*(для издания библиографических сборников)*Воронцов В.В.Чечулин А.А.Уланов А.В.

9.4. Название публикации
@Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов

9.5. Язык публикации
русский

9.6.1. Полное название издания
Информационные технологии

9.6.2. ISSN издания
1684-6400

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания
1

9.11. Страницы
37-42

9.12.1. Полное название издательства
Новые технологии

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В статье предлагается проактивный подход к защите от сетевых червей в сети Интернет, базирующийся на комбинировании различных механизмов обнаружения и сдерживания сетевых червей и автоматической динамической адаптации механизмов защиты в соответствии с текущей сетевой конфигурацией и сетевым трафиком. Описываются особенности данного подхода и программной реализации разработанной авторами системы моделирования механизмов защиты от сетевых червей. Приводятся результаты экспериментов, полученные при исследовании применения предлагаемого подхода для обнаружения и сдерживания как известных (CodeRed II, Slammer), так и потенциально возможных сетевых червей.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
11

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В.Уланов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
@Многоагентное моделирование защиты информационных ресурсов компьютерных сетей в сети Интернет

9.5. Язык публикации
русский

9.6.1. Полное название издания
Информационные технологии

9.6.2. ISSN издания
1684-6400

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания
2

9.11. Страницы
38-44

9.12.1. Полное название издательства
Новые технологии

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предлагаются модели, методика и реализующая их система для моделирования механизмов защиты от распределенных компьютерных атак. Подход основывается на представлении сторон атаки и защиты в виде команд интеллектуальных агентов. На основе предложенной архитектуры разработана система моделирования. В качестве примера реализации моделей и методики исследуются механизмы защиты от атак «распределенный отказ в обслуживании».

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
7

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
Р.М. Юсупов; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Юсупов Р.М.

9.4. Название публикации
@Технологии компьютерной безопасности

9.5. Язык публикации
русский

9.6.1. Полное название издания
Вестник Российской Академии Наук

9.6.2. ISSN издания
0869-5873

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
77

9.10.2 Номер издания
4

9.11. Страницы
323-333

9.12.1. Полное название издательства
Наука

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Информационная безопасность в условиях глобальной информатизации общества рассматривается сегодня как одна из основных компонент национальной безопасности. Информация, информационно-телекоммуникационные технологии, информационные ресурсы определяют дальнейшее развитие экономики, оборонного комплекса, социальной сферы, науки и других сфер человеческой деятельности. Одним из важнейших направлений исследований в области информационной безопасности является компьютерная безопасность, связанная с исследованием различных аспектов обеспечения безопасности компьютерных сетей и систем. Авторы рассматривают основные направления научных исследований в этой области, выполняемые учёными Санкт-Петербургского института информатики и автоматизации РАН (СПИИ РАН).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
9

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

*9.1. Номер проекта*07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
@Агентно-ориентированная среда для моделирования и оценки механизмов защиты от распределенных атак "Отказ в обслуживании"

9.5. Язык публикации
русский

9.6.1. Полное название издания
Известия вузов. Приборостроение

9.6.2. ISSN издания
0021-3454

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
50

9.10.2 Номер издания
1

9.11. Страницы
18-21

9.12.1. Полное название издательства
ООО "А-принт"

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В статье предлагается подход к агентно-ориентированному моделированию реализуемых в Интернет процессов защиты от распределенных атак, направленных на нарушение доступности. Подход заключается в представлении нарушителей и систем защиты от них в виде соответствующих команд агентов атаки и защиты, и моделировании исследуемых процессов реализации сетевых атак и защиты в виде взаимодействия отдельных агентов. Для проверки эффективности предложенного подхода авторами разработана программная среда агентно-ориентированного моделирования. В статье приводятся результаты экспериментов, проведенных на основе использования разработанной среды моделирования. Анализируются различные параметры кооперативной работы агентов и их влияние на эффективность защиты.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
8

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Защита программного обеспечения на основе механизма "удаленного доверия"

9.5. Язык публикации
русский

9.6.1. Полное название издания
Известия вузов. Приборостроение

9.6.2. ISSN издания
0021-3454

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания
51

9.10.2 Номер издания
11

9.11. Страницы
26-30

9.12.1. Полное название издательства
ООО "А-принт"

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Предложен подход к построению модели защиты программ от несанкционированных изменений и вмешательств с использованием механизма „удаленного доверия". Рассмотрены основные составляющие элементы механизма и принципы его функционирования. Предложены два варианта реализации механизма замещения мобильного модуля на основе парадигмы аспектно-ориентированного программирования.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
4

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.В. Воронцов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Воронцов В.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Анализ механизма обнаружения и сдерживания эпидемий сетевых червей на основе «кредитов доверия»

9.5. Язык публикации
русский

9.6.1. Полное название издания
Известия вузов. Приборостроение

9.6.2. ISSN издания
0021-3454

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания
51

9.10.2 Номер издания
11

9.11. Страницы
21-26

9.12.1. Полное название издательства
ООО "А-принт"

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Обсуждаются вопросы, связанные с анализом и модификацией механизма обнаружения и сдерживания эпидемий сетевых червей, который базируется на так называемых „кредитах доверия". Представлены особенности реализации данного механизма защиты, а также методика и результаты его оценки для различных типов сетевого трафика.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
4

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Е.В. Сидельникова; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Сидельникова Е.В.

9.3.1. Другие авторы
А.В. Тишков; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАНИ.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Тишков А.В.Котенко И.В.

9.4. Название публикации
@Верификация политик фильтрации с помощью исчисления событий и абдуктивного вывода

9.5. Язык публикации
русский

9.6.1. Полное название издания
Известия вузов. Приборостроение

9.6.2. ISSN издания
0021-3454

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания
51

9.10.2 Номер издания
11

9.11. Страницы
31-35

9.12.1. Полное название издательства
ООО "А-принт"

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Рассматривается подход к верификации политик фильтрации с помощью абдуктивного вывода. Предлагается классификация аномалий в правилах таблицы доступа межсетевого экрана и способы их разрешения. Анализируются различные сценарии моделирования работы межсетевого экрана с помощью исчисления событий. Предлагаются способы применения абдуктивного поиска для нахождения аномалий в политике фильтрации и их разрешения на основе разбиения условий правил политики на непересекающиеся части.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
7

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
О.В. Полубелова; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Полубелова О.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Верификация правил фильтрации политики безопасности методом "проверки на модели"

9.5. Язык публикации
русский

9.6.1. Полное название издания
Известия вузов. Приборостроение

9.6.2. ISSN издания
0021-3454

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания
51

9.10.2 Номер издания
11

9.11. Страницы
44-49

9.12.1. Полное название издательства
ООО "А-принт"

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Предлагается подход к верификации правил фильтрации, предназначенный для обнаружения и разрешения аномалий фильтрации в спецификациях политики безопасности компьютерных сетей. Подход основан на методе "проверки на модели" (model checking). Рассмотрены модели компьютерной системы, межсетевого экрана и аномалий фильтрации, служащие для верификации правил фильтрации данным методом, а также алгоритмы выявления таких аномалий. Предложена методика верификации правил фильтрации политик безопасности на базе этих моделей. Представлен подход к реализации предложенной методики верификации с использованием системы SPIN, а также результаты проведенных экспериментов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
13

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Тишков; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАНО.В. Черватюк; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАНС.А. Резник; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАНЕ.В. Сидельникова; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Тишков А.В.Черватюк О.В.Резник С.А.Сидельникова Е.В.

9.4. Название публикации
@Система верификации политики безопасности компьютерной сети

9.5. Язык публикации
русский

9.6.1. Полное название издания
Вестник компьютерных и информационных технологий

9.6.2. ISSN издания
1810-7206

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания
11

9.11. Страницы
48-56

9.12.1. Полное название издательства
Машиностроение

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Описан подход к верификации спецификаций сложных систем на примере проверки политики безопасности компьютерной сети. Особенностью подхода является применение гибридной архитектуры, использующей разные математические методы для поиска и разрешения различных типов противоречий, открытость для введения дополнительных моделей и методов верификации, а также использование автоматизированных процедур разрешения противоречий. Рассмотрена архитектура предлагаемой системы верификации. Представлены модели реализации двух модулей верификации: модуля, основанного на теории доказательств, с применением исчисления событий и абдуктивного вывода, и модуля, использующего технологию верификации на модели. Описана текущая реализация программного прототипа системы верификации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
10

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
@Multi-agent modeling and the simulation of computer network security processes: "a game of network cats and mice"

9.5. Язык публикации
английский

9.6.1. Полное название издания
NATO Science for Peace and Security Series, D: Information and Communication Security. Aspects of Network and Information Security

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания
17

9.10.2 Номер издания

9.11. Страницы
56-73

9.12.1. Полное название издательства
IOS Press

9.12.2. Город, где расположено издательство
Amsterdam

9.13. Краткий реферат публикации
В работе развивается агентно-ориентированный подход к моделированию противоборства злоумышленников и систем защиты в виде антагонистического взаимодействия команд программных агентов. Основное внимание в работе уделяется представлению разработанной программной среды (полигона) для многоагентного моделирования указанного противоборства, базирующегося на принципах имитационного моделирования на уровне пакетов, и описанию экспериментов по имитации распределенных атак "отказ в обслуживании" (атак DDoS), направленных на нарушение доступности информационных ресурсов, и механизмов защиты, реализующих их обнаружение, предотвращение и проактивное реагирование на атаки.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
29

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
@Multi-agent Simulation of Attacks and Defense Mechanisms in Computer Networks

9.5. Язык публикации
английский

9.6.1. Полное название издания
The Journal of Computing

9.6.2. ISSN издания
1727-6209

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания
7

9.10.2 Номер издания
2

9.11. Страницы
35-43

9.12.1. Полное название издательства
International Scientific Journal of Computing

9.12.2. Город, где расположено издательство
Ternopil

9.13. Краткий реферат публикации
В статье представлен подход к исследованию распределенных кооперативных механизмов киберзащиты против инфраструктурных атак, в том числе распределенного отказа в обслуживании, сетевых червей, бот-сетей, и т.д. Подход основан на агентно-ориентированном моделировании кибератак и механизмов киберзащиты, которое объединяет дискретно-событийное моделирование, многоагентный подход и моделирование протоколов на уровне сетевых пакетов. Различные методы противодействия кибератакам исследуются посредством представления компонентов атаки и защиты в виде команд агентов, использующих разработанную программную среду моделирования. Команды агентов защиты способны сотрудничать как компоненты систем защиты различных организаций и поставщиков Internet-сервисов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
35

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Десницкий В.А.

9.4. Название публикации
@Аспектно-ориентированная реализация модели защиты программ на основе "удаленного доверия"

9.5. Язык публикации
русский

9.6.1. Полное название издания
Информационные технологии и вычислительные системы

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
принято в печать

9.9. Год публикации
2010

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
ИСА РАН

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе рассматривается аспектно-ориентированный подход (АОП) к реализации динамического замещения мобильного модуля в модели защиты программного обеспечения от несанкционированных изменений и вмешательств на основе механизма «удаленного доверия». Главной целью исследования является разработка механизма, позволяющего осуществлять изменения защищаемого программного кода динамически, без перезагрузки и приостановки выполняющегося приложения.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
18

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
@Моделирование адаптивной кооперативной защиты от компьютерных атак в сети Интернет

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН)

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
31

9.10.2 Номер издания

9.11. Страницы
103-125

9.12.1. Полное название издательства
URSS

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В данной работе представлен подход к исследованию перспективных адаптивных и кооперативных механизмов защиты от компьютерных атак в сети Интернет, основанный на многоагентном моделировании. В соответствии с предложенным подходом системы атаки и защиты представляются как взаимодействующие команды интеллектуальных агентов, которые функционируют в соответствии с некоторым критерием адаптации. Они корректируют свои конфигурацию и поведение в соответствии с состоянием сети и мощностью атаки (защиты). В работе представляются архитектура и программная реализация среды моделирования, которая является комбинацией дискретно-событийного моделирования, многоагентного подхода и имитации различных протоколов Интернет на уровне пакетов. Данная среда позволяет исследовать сложные сценарии атак и защиты. Описаны эксперименты по исследованию компьютерных атак "Распределенный отказ в обслуживании" и адаптивных кооперативных механизмов защиты от них.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
43

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
М.В. Степашкин; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Степашкин М.В.

9.4. Название публикации
@Оценка защищенности компьютерных сетей на основе анализа графов атак

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН)

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
31

9.10.2 Номер издания

9.11. Страницы
126-207

9.12.1. Полное название издательства
URSS

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В статье предлагается подход к анализу защищенности компьютерных сетей, базирующийся на моделировании возможных действий злоумышленников, генерации общего графа атак, отражающего возможные распределенные сценарии сетевых атак, и использовании комплекса различных метрик безопасности, характеризующих защищенность компьютерной сети с различной степенью детализации и с учетом различных аспектов. Подход позволяет учитывать конфигурацию сети, реализуемую политику безопасности, а также местоположение, цели, уровень знаний и умений злоумышленника. Рассмотрены общая архитектура предлагаемой системы анализа защищенности, концептуальная модель реализуемых сценариев атак, процедуры формирования общего графа атак, используемые таксономии метрик защищенности, правила их расчета, а также методика экспресс-оценки общего уровня защищенности. Представлено описание реализованной системы анализа защищенности (САЗ) и примеры ее использования для анализа защищенности компьютерной сети.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
55

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
@Интеллектуальные механизмы управления кибербезопасностью

9.5. Язык публикации
русский

9.6.1. Полное название издания
Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН)

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания
41

9.10.2 Номер издания

9.11. Страницы
74-103

9.12.1. Полное название издательства
URSS

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Кибербезопасность в условиях глобальной информатизации общества рассматривается сегодня как одна из основных компонент национальной безопасности. Однако используемым в настоящее время подходам к обеспечению кибербезопасности присущ целый ряд недостатков. Эти недостатки обусловлены, главным образом, узкой специализацией отдельных средств киберзащиты и недостаточным уровнем их взаимодействия (кооперации), неразвитыми механизмами верификации защиты на этапах создания и поддержки, неадекватными механизмами определения уязвимостей, анализа рисков и определения уровня защищенности, мониторинга состояния сетей и адаптации к изменению условий их функционирования. В работе рассматривается подход к разработке и использованию систем киберзащиты (СКЗ), основанный на выделении интеллектуальной надстройки над традиционными механизмами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем защиты. Представляются отдельные механизмы управления кибербезопасностью.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
20

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Д.В. Комашинский; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Комашинский Д.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Детектирование вредоносного программного обеспечения на основе обработки статической информации методами интеллектуального анализа данных

9.5. Язык публикации
русский

9.6.1. Полное название издания
Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН)

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
принято в печать

9.9. Год публикации
2010

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
URSS

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Работа посвящена применению методов интеллектуального анализа данных (Data Mining) для создания эвристических детекторов вредоносного ПО. Описываемый подход отличается от существующих направленностью обработку статической информации, обеспечивающей формирование отдельных функциональных элементов эффективной модели детектирования вредоносных исполняемых объектов. В работе реализована и исследована общая методология формирования системы детектирования на базе применения методов выделения значимых признаков и методов классификации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
13

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Защищенность и масштабируемость механизма защиты программного обеспечения на основе принципа удаленного доверия

9.5. Язык публикации
русский

9.6.1. Полное название издания
Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН)

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
принято в печать

9.9. Год публикации
2010

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
URSS

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Статья посвящена вопросам обеспечения масштабируемости и защищенности механизма защиты программного обеспечения (ПО) и комбинированию различных методов защиты, входящих в состав данного механизма. Указанные аспекты рассматриваются на примере исследования механизма защиты ПО на основе принципа удаленного доверия [9]. Предлагаемый подход к обеспечению масштабируемости и защищенности включает получение количественных оценок производительности и степени защищенности рассматриваемых методов защиты ПО. На основе данной информации для формирования общего механизма защиты выполняется выбор рациональной или оптимальной комбинации методов защиты и их параметров.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
11

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В. В. Воронцов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Воронцов В.В.

9.4. Название публикации
Аналитические модели распространения сетевых червей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Труды СПИИРАН

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
4

9.10.2 Номер издания
1

9.11. Страницы
208-224

9.12.1. Полное название издательства
Наука

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В статье рассматриваются существующие аналитические модели распространения сетевых червей. Приводится описание как детерминированных моделей (SIS, SIR, SEIR, SAIR и PSIDR), так и стохастических.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
11

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В.В. Воронцов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАНА.В. Уланов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Воронцов В.В.Уланов А.В.

9.4. Название публикации
Модели и системы имитационного моделирования распространения сетевых червей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Труды СПИИРАН

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
4

9.10.2 Номер издания
1

9.11. Страницы
225-238

9.12.1. Полное название издательства
Наука

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Рассматриваются существующие модели и системы имитационного моделирования распространения сетевых червей. Приводится описание программных систем имитационного моделирования DDosVax, NWS, SSF.App.Worm, GTNetS, PDNS и DIB:S/TRAFEN. Представлены достоинства и недостатки применения указанных систем для исследования распространения сетевых червей.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
8

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
С.А. Резник; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАНА.В. Шоров; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Резник С.А.Шоров А.В.

9.4. Название публикации
Верификация протоколов безопасности на основе комбинированного использования существующих методов и средств

9.5. Язык публикации
русский

9.6.1. Полное название издания
Труды СПИИРАН

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания
2

9.10.2 Номер издания
8

9.11. Страницы
292-310

9.12.1. Полное название издательства
Наука

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В настоящей статье анализируются существующие подходы к верификации протоколов безопасности и демонстрируется невозможность полноценной верификации протоколов безопасности в рамках только одного из подходов. Для решения данной задачи предлагается комбинированный подход к верификации, основанный на объединении сильных сторон существующих методов и средств.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
32

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Уланов; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Уланов А.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания
1-3

9.11. Страницы
60-67, 70-77, 62-69

9.12.1. Полное название издательства
Любавич

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Одним из наиболее критичных по последствиям классов компьютерных атак являются атаки "распределенный отказ в обслуживании" (Distributed Denial of Service, DDoS), направленные на нарушение доступности информационных ресурсов. Эти атаки осуществляются совместными усилиями множества программных компонентов, размещаемых на скомпрометированных хостах в Интернет. Они могут привести не только к выходу из строя отдельных хостов и служб, но и остановить работу корневых DNS-серверов и вызвать частичное или полное прекращение функционирования сети Интернет. Одной из актуальных задач в области защиты информации является разработка адекватных механизмов защиты от атак DDoS и выработка обоснованных рекомендаций по выбору механизмов, наиболее действенных в конкретных условиях. В статье рассматриваются схемы классификации механизмов защиты, и дается обзор существующих и перспективных механизмов защиты от атак DDoS. Основное внимание уделяется кооперативным механизмам защиты. Данный обзор не претендует на полноту, но охватывает основные подходы к защите от DDoS.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
64

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.С. Богданов; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Богданов В.С.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Проактивный мониторинг выполнения политики безопасности в компьютерных сетях

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания
3-4

9.11. Страницы
42-47, 66-72

9.12.1. Полное название издательства
Любавич

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Основой для организации процесса защиты информации в компьютерных сетях является политика безопасности. Проверка соответствия принятой в организации политики безопасности ее текущей реализации в компьютерной сети является одной из актуальных задач администратора безопасности. В статье рассмотрена проблема создания системы проактивного мониторинга функционирования средств защиты, при выполнении которой осуществляется тестирование соответствия функциональности средств защиты заданной политике безопасности. Предлагаемый подход к мониторингу основан на автоматической имитации возможных действий пользователей в защищаемой компьютерной сети. В отличие от релевантных исследований данный подход применим к различным категориям политики безопасности (аутентификации, разграничения доступа и авторизации, фильтрации, защиты каналов связи и др.). В статье представлены основные особенности задачи проверки выполнения политики безопасности, описаны этапы, обобщенные алгоритмы и особенности предлагаемого подхода к проактивному мониторингу политики безопасности. Представлена обобщенная архитектура разработанной системы мониторинга и примеры ее использования для тестирования политики безопасности компьютерной сети.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
29

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
@Компьютерные войны в Интернете: моделирование противоборства программных агентов

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания
4

9.11. Страницы
38-45

9.12.1. Полное название издательства
Любавич

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Традиционные средства и механизмы компьютерной сетевой безопасности больше ориентированны на защиту от отдельных угроз и типов атак и, обычно, реализованы в виде набора программных и аппаратных компонентов, функционирующих относительно независимо. Более совершенная система защиты должна быть взаимосвязанной и обладать такими свойствами, как автономность, распределенность, адаптивность, интеллектуальность, способность кооперации с другими системами и др. Указанные свойства лежат в основе многоагентных систем. С их помощью можно строить перспективные распределенные системы защиты. Для исследования применения таких систем защиты в работе предлагается моделировать противостояние злоумышленников и систем защиты, представляя их распределенными командами интеллектуальных агентов, которые адаптируются к поведению друг друга и вступают в альянсы (кооперируются) для повышения эффективности своих действий. В соответствии с этим подходом разработана среда моделирования и реализованы различные типы атак "распределенный отказ в обслуживании" и механизмов защиты от них. В среде проводятся эксперименты, например, по защите сети провайдеров Интернет (ISP) от распределенных скоординированных атак. При этом используются различные конфигурации и топологии сетей, методы защиты, способы кооперации и обмена информации с другими системами защиты других ISP.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
18

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРА

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Автоматическое обнаружение и сдерживание распространения Интернет-червей: краткий анализ современных исследований

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания
4

9.11. Страницы
46-56

9.12.1. Полное название издательства
Любавич

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В статье представлен краткий обзор существующих подходов к защите от сетевых червей, изложенных в ряде исследовательских работ. Методы защиты от сетевых червей подразделяются по реализуемым фазам на методы обнаружения и противодействия. Представляются методы обнаружения, основанные на анализе данных сетевых соединений и учете релевантных метрик реализации сетевых соединений, например, разброса адресов соединений и интенсивности неудачных соединений. Анализируются как методы, базирующиеся на непосредственном наблюдении за трафиком червей, так и косвенные методы, основанные на анализе вторичного трафика, коррелированного с трафиком сетевых червей. Представляются исследования по реализации таких методов сдерживания, как карантин, фильтрация контента и ограничение скорости установления сетевых соединений.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
45

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Международная конференция "Математические модели, методы и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2007)

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания
3,4

9.11. Страницы
12, 56

9.12.1. Полное название издательства
Любавич

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Рассматривается информация об одном из ведущих международных форумов в области исследования фундаментальных и прикладных проблем защиты компьютерных сетей четвертой международной конференции “Математические модели, методы и архитектуры для защиты компьютерных сетей” (MMM-ACNS-2007).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Тишков; 1; Россия; СПИИРАНЕ.В. Сидельникова; 1; Россия; СПИИРАНО.В. Черватюк; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Тишков А.В.Сидельникова Е.В.Черватюк О.В.

9.4. Название публикации
Проверка правил политики безопасности для корпоративных компьютерных сетей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания
5. 6

9.11. Страницы
46-49, 52-59

9.12.1. Полное название издательства
Любавич

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Актуальной задачей, решение которой необходимо при поддержке функционирования корпоративных компьютерных сетей, базирующихся на политике безопасности, является проверка правильности (верификация) этой политики. Настоящая работа описывает общий подход к верификации политики безопасности корпоративных компьютерных сетей, основанный на использовании гибридной многомодульной архитектуры системы верификации. Данный подход был предложен и реализован в группе компьютерной безопасности СПИИРАН на основе разработки программного средства "SEcurity Checker" (SEC). SEC может служить для отладки различных правил политики безопасности, включая правила аутентификации, авторизации, фильтрации, защиты каналов связи, а также операционных правил.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
48

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.А. Чечулин; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Чечулин А.А.

9.4. Название публикации
@Исследование механизмов защиты от сетевых червей на основе методик Virus Throttling

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания
3

9.11. Страницы
68-73

9.12.1. Полное название издательства
Любавич

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Актуальной задачей, решение которой необходимо для защиты компьютерных сетей, является обнаружение и сдерживание эпидемий сетевых червей. В статье рассматривается подход к защите от сетевых червей, основанный на методиках Virus Throttling ("регулирования/дросселирования") и модификации данных методик. Описываются особенности данного подхода и программной реализации разработанной авторами системы моделирования механизмов защиты от сетевых червей. Приводятся результаты экспериментов, полученные при исследовании применения методик Virus Throttling для обнаружения и сдерживания различных сетевых червей.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
12

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАНС.А. Резник; 2; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.Резник С.А.

9.4. Название публикации
@Разработка и верификация протокола обмена сообщениями для защиты программ на основе механизма "удаленного доверия"

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания
4, 5

9.11. Страницы
59-63, 68-74

9.12.1. Полное название издательства
Любавич

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Целью механизма "удаленного доверия" является обнаружение несанкционированных модификаций клиентской программы, функционирующей в потенциально враждебном окружении, на основе использования доверенного сервера, располагающегося на защищенном хосте, и непрерывного сетевого соединения между клиентом и сервером. Одним из важнейших элементов механизма защиты программ от злонамеренных изменений на основе "удаленного доверия" является протокол обмена сообщениями ("entrusting-протокол"), который служит для передачи данных между доверенным сервером и защищаемой клиентской программой, в том числе для передачи кода мобильного модуля, предназначенного для проверки клиентского приложения во время выполнения, и результатов проверок. Настоящая статья посвящена разработке entrusting-протокола и его анализу при помощи формальных средств верификации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
16

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
Р.М. Юсупов; 2; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Юсупов Р.М.

9.4. Название публикации
Информационные технологии для борьбы с терроризмом

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания
2

9.11. Страницы
74-79

9.12.1. Полное название издательства
Афина

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В статье делается краткий анализ проблемы использования информационных технологий для борьбы с терроризмом, дается характеристика основных информационных технологий, которые используются или могут быть использованы в данной области, анализируются основные этапы борьбы с террористическими проявлениями и связь этих этапов с базовыми информационными технологиями. Ставятся проблемы создания единого антитеррористического информационного пространства и расширения фундаментальных и прикладных исследований в области создания или совершенствования информационных технологий в интересах борьбы с терроризмом.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
12

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
С.А. Резник; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Резник С.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Методы и средства верификации для комбинированного анализа протоколов безопасности

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания
3

9.11. Страницы
56-72

9.12.1. Полное название издательства
Афина

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В настоящей статье представляется анализ существующих подходов к верификации протоколов безопасности. Дается характеристика как сильных, так и слабых сторон различных методов и средств верификации, и демонстрируется невозможность полноценной верификации протоколов безопасности в рамках только одного из подходов. Для решения данной задачи обосновывается необходимость использования комбинированного подхода, основанного на объединении сильных сторон различных методов и средств верификации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
32

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Методы защиты программного обеспечения на основе принципа удаленного доверия

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания
6

9.11. Страницы
57-61

9.12.1. Полное название издательства
Афина

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Объектом исследования в данной статье является предлагаемый механизм защиты программ на основе принципа удаленного доверия. В статье представлен краткий анализ отдельных (атомарных) методов защиты, применяемых в рамках данного механизма, а также рассмотрены некоторые способы оптимизации методов защиты для повышения их производительности.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
13

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Д.В. Комашинский; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Комашинский Д.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Концептуальные основы использования методов Data Mining для обнаружения вредоносного программного обеспечения

9.5. Язык публикации
русский

9.6.1. Полное название издания
Защита информации. Инсайд

9.6.2. ISSN издания

9.7. Вид публикации
статья в журнале

9.8. Завершенность публикации
принято в печать

9.9. Год публикации
2010

9.10.1 Том издания

9.10.2 Номер издания
1-2

9.11. Страницы

9.12.1. Полное название издательства
Афина

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Данная статья посвящена концептуальным вопросам использования методов Data Mining для реализации отдельных элементов систем обнаружения вредоносного программного обеспечения. Показывается актуальность решаемой задачи, определяются основные общие требования к методам детектирования вредоносного программного обеспечения (ПО). Описывается общая методология применения методов Data Mining, и приводятся примеры ее использования для обнаружения вредоносного программного обеспечения, реализованного в виде исполняемых файлов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
26

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Vladimir Gorodetsky @ В.И. Городецкий; 2; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Gorodetsky V.I.

9.3.1. Другие авторы
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and AutomationVictor Skormin @ V.A. Skormin; 2; США; Binghamton University

9.3.2. Другие авторы (для издания библиографических сборников)
Kotenko I.V.Skormin V.A.

9.4. Название публикации
Mathematical Methods, Models and Architectures for Computer Networks Security

9.5. Язык публикации
английский

9.6.1. Полное название издания
Communications in Computer and Information Science (CCIS)

9.6.2. ISSN издания
1865-0929

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
1

9.10.2 Номер издания

9.11. Страницы
1-416

9.12.1. Полное название издательства
Springer-Verlag

9.12.2. Город, где расположено издательство
Berlin

9.13. Краткий реферат публикации
В настоящем сборнике представлены доклады, сделанные на четвертой международной конференции "Математические модели, методы и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2007). Эта конференция явилась важным событием в области информационной безопасности в 2007 году и одним из ведущих международных форумов в области исследования фундаментальных и прикладных проблем защиты компьютерных сетей. В ходе подготовки к данной конференции были получены доклады из 17 стран. Наибольшее количество статей поступило из России, США, Китая, Польши и Франции. В результате рецензирования международным программным комитетом было отобрано 30 лучших докладов. Кроме того, для участия в конференции были персонально приглашены известные в мире специалисты в области защиты информации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
@Моделирование адаптации противоборствующих команд интеллектуальных агентов

9.5. Язык публикации
русский

9.6.1. Полное название издания
КИИ-2008. XI Национальная конференция по искусственному интеллекту с международным участием. Труды конференции

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания
1

9.10.2 Номер издания

9.11. Страницы
32-40

9.12.1. Полное название издательства
Физматлит

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе, на примере защиты от компьютерных атак в сети Интернет, рассмотрен подход к исследованию адаптивных и кооперативных механизмов функционирования команд интеллектуальных агентов. Представлены особенности предлагаемого подхода, архитектура и программная реализация среды моделирования и эксперименты по исследованию адаптивных кооперативных механизмов защиты от компьютерных атак "Распределенный отказ в обслуживании".

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
15

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
Р.М. Юсупов; 2; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Юсупов Р.М.

9.4. Название публикации
@Противодействие кибертерроризму: актуальные проблемы и перспективные направления исследований

9.5. Язык публикации
русский

9.6.1. Полное название издания
Санкт-Петербургский научный форум «Наука и общество»: Информационные технологии. 4-ая Петербургская встреча нобелевских лауреатов

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания
1

9.10.2 Номер издания

9.11. Страницы
329-332

9.12.1. Полное название издательства
СПГУТТ

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе характеризуется текущее состояние в области противодействия кибертерроризму и обеспечения безопасности компьютерных систем и сетей, рассматриваются актуальные направления исследований в области защиты компьютерных сетей и систем. Наибольшее внимание уделяется ключевым областям исследований, связанным с построением комплексных систем противодействия кибертерроризму: интеллектуализацией механизмов защиты, поддержкой жизненного цикла систем защиты, а также моделированием и исследованием кибер-противоборства в открытых сетях.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
М.В. Степашкин; 1; Россия; СПИИР

9.2.2. Первый автор (для издания библиографических сборников)
Степашкин М.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Анализ защищенности компьютерных сетей и систем на основе построения деревьев атак

9.5. Язык публикации
русский

9.6.1. Полное название издания
Санкт-Петербургский научный форум «Наука и общество»: Информационные технологии. 4-ая Петербургская встреча нобелевских лауреатов

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания
1

9.10.2 Номер издания

9.11. Страницы
363-366

9.12.1. Полное название издательства
СПГУТТ

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Одним из перспективных подходов к анализу защищенности компьютерных сетей и систем является предлагаемый авторами метод построения дерева атак с его последующим анализом. Основное отличие предлагаемого в подхода от других релевантных подходов заключается в способе построения дерева атак (применяется многоуровневое иерархическое представление стратегий действий злоумышленника) и использовании построенного общего дерева атак для определения семейства различных показателей (метрик) защищенности. Важнейшим преимуществом данного подхода перед другими подходами к анализу защищенности (например, по сравнению с тестированием на проникновение) является возможность его использования на различных этапах жизненного цикла анализируемой компьютерной сети или системы (в том числе на основных этапах, среди которых выделяют этапы проектирования и эксплуатации).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы
Alexander Ulanov @ А.В. Уланов; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Ulanov A.V.

9.4. Название публикации
@Multi-agent Framework for Simulation of Adaptive Cooperative Defense against Internet Attacks

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of International Workshop on Autonomous Intelligent Systems: Agents and Data Mining (AIS-ADM-07). Lecture Notes in Artificial Intelligence

9.6.2. ISSN издания
0302-9743

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
4476

9.10.2 Номер издания

9.11. Страницы
212-228

9.12.1. Полное название издательства
Springer-Verlag

9.12.2. Город, где расположено издательство
Berlin

9.13. Краткий реферат публикации
В работе предлагается подход к исследованию перспективных адаптивных и кооперативных механизмов защиты информационных ресурсов в сети Интернет, основанный на многоагентном моделировании. В соответствии с данным подходом системы атаки и защиты представляются в виде взаимодействующих команд интеллектуальных агентов, действующих в соответствии с некоторым критерием адаптации. Представлена архитектура и программная реализация среды моделирования, позволившая комплексировать моделирование на основе дискретных событий, многоагентный подход и имитацию обмена сетевыми пакетами по различным протоколам Интернет. Разработанная среда позволяет исследовать сложные адаптивные сценарии атак и защиты. В работе представлены результаты экспериментов по исследованию адаптивных кооперативных механизмов защиты от атак "распределенный отказ в обслуживании".

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
43

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы
Artem Tishkov @ А.В. Тишков; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)Olga Chervatuk @ О.В. Черватюк; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)Ekaterina Sidelnikova @ Е.В. Сидельникова; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.3.2. Другие авторы (для издания библиографических сборников)
Tishkov A.V.Chervatuk O.V.Sidelnikova E.V.

9.4. Название публикации
Security Policy Verification Tool for Geographical Information Systems

9.5. Язык публикации
английский

9.6.1. Полное название издания
Information Fusion and Geographical Information Systems. Lecture Notes in Geoinformation and Cartography

9.6.2. ISSN издания
1863-2246

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
128-146

9.12.1. Полное название издательства
Springer-Verlag

9.12.2. Город, где расположено издательство
Berlin

9.13. Краткий реферат публикации
В статье рассматривается общий подход к верификации политик безопасности и представляется программное средство “Security Checker”, которое может служить в качестве “отладчика” для различных категорий политики безопасности.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
37

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Julien Bourgeois; 2; Франция; Universite de Franche Comte

9.2.2. Первый автор (для издания библиографических сборников)
Bourgeois J.

9.3.1. Другие авторы
Abdoul Karim Ganame; 2; Франция; Universite de Franche ComteIgor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)Alexander Ulanov @ А.В. Уланов; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.3.2. Другие авторы (для издания библиографических сборников)
Ganame A.K.Kotenko I.V.Ulanov A.V.

9.4. Название публикации
Software Environment for Simulation and Evaluation of a Security Operation Center

9.5. Язык публикации
русский

9.6.1. Полное название издания
Information Fusion and Geographical Information Systems. Lecture Notes in Geoinformation and Cartography

9.6.2. ISSN издания
1863-2246

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
111-127

9.12.1. Полное название издательства
Springer-Verlag

9.12.2. Город, где расположено издательство
Berlin

9.13. Краткий реферат публикации
Несколько проблематично оценить эффективность систем защиты в Интеренет из-за сложности этих систем и Интернет. Поэтому, моделирование становится все более важным для оптимизации поведения систем защиты, включая компоненты защиты, предназначенные защиты различных распределенных географических информационных систем (ГИС). В статье представляется подход и программная среда моделирования для всестороннего исследования системы Security Operation Center (SOCBox), которая является в сущности "метасистемой" обнаружения вторжений. SOCBox собирает данные из широкого диапазона источников (системы обнаружения вторжения (СОВ), межсетевые защиты, маршрутизаторы, рабочие станции, и т.д.), и поэтому имеет глобальное представление сети. Среда моделирования была разработана прежде для моделирования механизмов защиты от атак "распределенный отказ в обслуживании" (DDoS). Эта среда характеризуется агентно-ориентированным подходом, имитацией процессов защиты на уровне сетевых пакетов и открытой библиотекой различных атак и механизмов защиты. В статье рассматривается структура системы SOCBox, архитектура среды моделирования, модели SOCBox в среде моделирования и особенности моделирования SOCBox.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
14

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Vasily Desnitsky @ В.А. Десницкий; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.2.2. Первый автор (для издания библиографических сборников)
Desnitsky V.A.

9.3.1. Другие авторы
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.3.2. Другие авторы (для издания библиографических сборников)
Kotenko I.V.

9.4. Название публикации
Design of Entrusting Protocols for Software Protection

9.5. Язык публикации
английский

9.6.1. Полное название издания
Information Fusion and Geographical Information Systems. Lecture Notes in Geoinformation and Cartography

9.6.2. ISSN издания
1863-2246

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
301-316

9.12.1. Полное название издательства
Springer-Verlag

9.12.2. Город, где расположено издательство
Berlin

9.13. Краткий реферат публикации
В работе рассматривается один из важнейших элементов механизма защиты программ от злонамеренных изменений на основе механизма "удаленного доверия" – специализированный протокол обмена сообщениями ("entrusting-протокол"). Данный протокол предназначен для передачи данных между доверенным сервером и защищаемой клиентской программой, необходимых для работы защитного механизма. Настоящая статья посвящена вопросам разработки entrusting-протокола и его анализа. Рассматриваются модели нарушителя, имеющего цель скомпрометировать работу протокола, и тем самым осуществить вмешательство в работу клиентской программы. Формируются основные требования к entrusting-протоколу, соблюдение которых необходимо для построения надежного, устойчивого к вмешательствам протокола. Предлагаются различные реализации entrusting-протокола, на основе существующих сетевых протоколов, а также интеграция с протоколами, способными его усилить или придать ему какие-либо дополнительные качества. В работе предлагается общий подход к оцениванию временной сложности атак на entrusting-протокол, а также рассматривается возможность применимости методов автоматического синтеза протоколов к задаче построения entrusting-протокола.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
11

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Dmitry Komashinskiy @ Д.В. Комашинский; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.2.2. Первый автор (для издания библиографических сборников)
Komashinskiy D.V.

9.3.1. Другие авторы
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.3.2. Другие авторы (для издания библиографических сборников)
Kotenko I.V.

9.4. Название публикации
Using Data Mining methods for malware detection

9.5. Язык публикации
английский

9.6.1. Полное название издания
Information Fusion and Geographical Information Systems. Lecture Notes in Geoinformation and Cartography

9.6.2. ISSN издания
1863-2246

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
343-357

9.12.1. Полное название издательства
Springer-Verlag

9.12.2. Город, где расположено издательство
Berlin

9.13. Краткий реферат публикации
Проблема противодействия вредоносному программному обеспечению продолжает набирать остроту, несмотря на очевидные успехи в повышении эффективности выявления его распространения, анализа и обновления баз его описаний. Одним из наиболее важных аспектов этой проблемы является повышение качества методов детектирования, называемых эвристическими. Они призваны обеспечить обнаружение ранее неизвестных вредоносных программ на всех этапах их жизненного цикла и, по сути, являются последним рубежом обороны защищаемого объекта. Данная работа посвящена применению методов интеллектуального анализа данных (Data Mining) для создания эвристических детекторов вредоносного программного обеспечения. Предлагаемый подход отличается от существующих направленностью на циклическую интерактивную скрытную обработку поведенческой информации, а также интегрированным использованием различных методов интеллектуального анализа данных для различных классов вредоносного программного обеспечения. В работе реализовано и исследовано семейство различных методов интеллектуального анализа, основанных на Байесовском подходе, деревьях решений, нейронных сетях и др. Предлагается общий интегрированный подход к реализации комплекса методов детектирования вредоносного программного обеспечения.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
9

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы
Alexander Ulanov @ А.В. Уланов; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Ulanov A.V.

9.4. Название публикации
Agent-based Simulation Environment and Experiments for Investigation of Internet Attacks and Defense Mechanisms

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of 21th European Conference on Modelling and Simulation (ECMS 2007). Prague, Czech Republic. 4-6 June 2007

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
146-155

9.12.1. Полное название издательства
ECMS

9.12.2. Город, где расположено издательство
Sbr.-Dudweiler

9.13. Краткий реферат публикации
В статье рассматривается среда моделирования, которая была разработана для всестороннего исследования Интернет-атак и механизмов защиты от них (на примере атак "распределенный отказ в обслуживании" (DDoS) и механизмов защиты от данного класса атак). Эта среда обладает следующими особенностями: агентно-ориентированный подход к моделированию, моделирование атак и систем защиты на уровне сетевых пакетов, возможность добавлять новые атаки и методы защиты и исследовать их. Описывается предложенный подход к моделированию. Специфицируются основные компоненты среды моделирования. Рассматривается методология испытаний для исследования механизмов защиты, и анализируются результаты экспериментов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
12

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Simulation of Agent Teams: the Application of Domain-Independent Framework to Computer Network Security

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of 23rd European Conference on Modelling and Simulation (ECMS 2009). Madrid, Spain. June 9-12, 2009

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
137-143

9.12.1. Полное название издательства
ECMS

9.12.2. Город, где расположено издательство
Sbr.-Dudweiler

9.13. Краткий реферат публикации
В статье рассматривается подход к агентно-ориентированному моделированию сотрудничества и противодействия команд интеллектуальных агентов. Данный подход предназначен для представления сложных процессов, происходящих в различных предметных областях на основе использования различных типов команд агентов и их взаимодействия. Описывается предложенный подход к моделированию на основе моделирования защиты от распределенных атак в Интернет. Специфицируются основные компоненты среды моделирования. Рассматривается методология исследования механизмов защиты, и анализируются результаты экспериментов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
26

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы
Olga Chervatuk @ О.В. Черватюк; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)Ekaterina Sidelnikova @ Е.В. Сидельникова; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)Artem Tishkov @ А.В. Тишков; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.3.2. Другие авторы (для издания библиографических сборников)
Chervatuk O.V.Sidelnikova E.V.Tishkov A.V.

9.4. Название публикации
Hybrid Multi-module Security Policy Verification

9.5. Язык публикации
английский

9.6.1. Полное название издания
2007 IEEE Workshop on Policies for Distributed Systems and Networks (Policy 2007). 13-15 June 2007. Bologna, Italy. 2007

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
277

9.12.1. Полное название издательства
IEEE

9.12.2. Город, где расположено издательство
Los Alamitos, CA

9.13. Краткий реферат публикации
В статье рассматривается предлагаемый подход к верификации политик безопасности и представляется разработанное программное средство верификации для различных категорий политики безопасности.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
1

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of IEEE Fourth International Workshop on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2007). Dortmund, Germany, 6-8 September, 2007

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
614-619

9.12.1. Полное название издательства
IEEE and Fachhochschule Dortmund

9.12.2. Город, где расположено издательство
Dortmund

9.13. Краткий реферат публикации
В работе рассматривается подход к исследованию распределенных кооперативных механизмов киберзащиты против сетевых атак. Подход основан на агентно-ориентированном моделировании атак и механизмов защиты, которое комбинирует моделирование на основе дискретных событий, многоагентный подход и моделирование на уровне сетевых протоколов. На основе представления атак и компонентов защиты в виде команд агентов и использования разработанной программной среды моделирования, исследуются различные методы противодействия атакам. Команды агентов защиты способны сотрудничать, как компоненты систем защиты различных организаций и системных служб Интернет (поставщиков Интернет-сервисов).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
35

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы
Vitaly Bogdanov @ В.С. Богданов; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Bogdanov V.S.

9.4. Название публикации
Proactive Monitoring of Security Policy Accomplishment in Computer Networks

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of IEEE Fourth International Workshop on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2009). Rende (Cosenza), Italy, September 21-23, 2009

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
364-36

9.12.1. Полное название издательства
IEEE

9.12.2. Город, где расположено издательство
Piscataway, NJ

9.13. Краткий реферат публикации
В статье рассмотрен подход к проактивному мониторингу выполнения политики безопасности в компьютерных сетях. Предлагаемый подход к мониторингу основан на реализации различных стратегий автоматической имитации возможных действий пользователей в защищаемой компьютерной сети, включая исчерпывающий поиск (полный перебор возможных вариантов), экспресс-анализ и генерацию оптимизированных тестовых последовательностей. Данный подход применим к различным категориям политики безопасности (аутентификации, разграничения доступа и авторизации, фильтрации, защиты каналов связи и др.). В статье представлены особенности предлагаемого подхода к проактивному мониторингу политики безопасности. Представлена обобщенная архитектура разработанной системы мониторинга и примеры ее использования для тестирования политики безопасности компьютерной сети.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
25

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Vitaly Bogdanov @ В.С. Богданов; 1; Россия; St. Petersburg Institute for Informatics and Automati

9.2.2. Первый автор (для издания библиографических сборников)
Bogdanov V.S.

9.3.1. Другие авторы
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Kotenko I.V.

9.4. Название публикации
Policy-based Proactive Monitoring of Security Policy Performance

9.5. Язык публикации
английский

9.6.1. Полное название издания
Mathematical Methods, Models and Architectures for Computer Networks Security. The Forth International Conference, MMM-ACNS 2007. St. Petersburg, Russia, September 13–15, 2007. Proceedings. Communications in Computer and Information Science (CCIS). Springer. Vladimir Gorodetsky, Igor Kotenko, Victor Skormin (Eds.)

9.6.2. ISSN издания
1865-0929

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
1

9.10.2 Номер издания

9.11. Страницы
197-212

9.12.1. Полное название издательства
Springer-Verlag

9.12.2. Город, где расположено издательство
Berlin

9.13. Краткий реферат публикации
Одной из актуальных задач управления защитой на основе политики безопасности является проверка того, что политика безопасности, используемая в организации, соответствует ее реализации в компьютерной сети. В статье рассматривается предложенный подход к проактивному мониторингу выполнения политики безопасности и функционирования механизмов защиты. Подход основан на различных стратегиях автоматической имитации действий возможных пользователей в компьютерной сети, включая полный перебор, экспресс-анализ и генерацию оптимальных тестовых последовательностей. Такой подход применим к различным категориям политики безопасности (аутентификация, авторизация, фильтрация, защита каналов связи и т.д.). В статье рассматриваются этапы, обобщенные алгоритмы и основные особенности предложенного подхода, а также формальные методы, использованные для оптимизации тестовых последовательностей. Представляется обобщенная архитектура системы проактивного мониторинга, ее реализация и пример тестирования политики безопасности.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
26

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Artem Tishkov @ A.B. Тишков; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Tishkov A.V.

9.3.1. Другие авторы
Ekaterina Sidelnikova @ E.B. Сидельникова; 1; Россия; St. Petersburg Institute for Informatics and AutomationIgor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Sidelnikova E.V.Kotenko I.V.

9.4. Название публикации
Event Calculus based Checking of Filtering Policies

9.5. Язык публикации
английский

9.6.1. Полное название издания
Mathematical Methods, Models and Architectures for Computer Networks Security. The Forth International Conference, MMM-ACNS 2007. St. Petersburg, Russia, September 13–15, 2007. Proceedings. Communications in Computer and Information Science (CCIS). Springer. Vladimir Gorodetsky, Igor Kotenko, Victor Skormin (Eds.)

9.6.2. ISSN издания
1865-0929

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
1

9.10.2 Номер издания

9.11. Страницы
248-253

9.12.1. Полное название издательства
Springer-Verlag

9.12.2. Город, где расположено издательство
Berlin

9.13. Краткий реферат публикации
В статье рассматривается подход к верификации политики фильтрации. Потенциальный сетевой трафик моделируется с использованием исчисления событий. Для обнаружения аномалий фильтрации межсетевого экрана применяются процедуры абдуктивного вывода. Предлагаемый подход позволяет отделять описание поведения сети от определения несогласованностей защиты, и, таким образом, предлагает гибкие и масштабируемые механизмы для верификации политики фильтрации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
7

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы
Alexander Ulanov @ А.В. Уланов; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Ulanov A.V.

9.4. Название публикации
Investigation of Cooperative Defense against DDoS

9.5. Язык публикации
английский

9.6.1. Полное название издания
SECRYPT 2007. International Conference on Security and Cryptography. Proceedings. Barcelona, Spain. 28-31 July 2007

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
180-183

9.12.1. Полное название издательства
INSTICC Press

9.12.2. Город, где расположено издательство
Setubal, Portugal

9.13. Краткий реферат публикации
В статье предлагается новый подход и среда моделирования для всестороннего исследования атак "распределенный отказ в обслуживании" (DDoS) и механизмов защиты от них. Основные особенности подхода и среды: агентно-ориентированный подход к моделированию, моделирование атак и систем защиты на уровне сетевых пакетов, возможность добавлять новые атаки и методы защиты и исследовать их. Описывается предложенный подход к моделированию. Специфицируются основные компоненты среды моделирования. Основным содержанием статьи является использование предлагаемого подхода и среды моделирования для оценивания и сравнения нескольких кооперативных механизмов защиты от атак DDoS (DefCOM, COSSACK и методов, предложенных авторами). Рассматривается методология испытаний для исследования данных механизмов защиты и результаты экспериментов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
8

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы
Alexander Ulanov @ А.В. Уланов; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Ulanov A.V.

9.4. Название публикации
@Packet Level Simulation of Cooperative Distributed Defense against Internet Attacks

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of 16th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2008). Toulouse, France. February 13-15 2008

9.6.2. ISSN издания
1066-6192

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
565-572

9.12.1. Полное название издательства
IEEE Computer Society

9.12.2. Город, где расположено издательство
New-York

9.13. Краткий реферат публикации
В статье рассматривается архитектура и реализация программного средства, предназначенного для моделирования Интернет-атак и механизмов защиты от них. Предлагаемое программное средство базируется на моделировании на уровне пакетов и агентно-ориентированном подходе, оно предназначено для оценивания и сравнения различных кооперативных распределенных механизмов защиты. В статье рассматривается использование предлагаемого программного средства для анализа кооперативных механизмов защиты против атак DDoS (Distributed Denial of Service). Исследуются как механизмы, базирующиеся на частичной кооперации распределенных механизмов защиты, включая DefCOM (Defensive Cooperative Overlay Mesh) и COSSACK (coordinated suppression of simultaneous attacks), так и механизмы, основанные на полной кооперации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
17

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
@Framework for Integrated Proactive Network Worm Detection and Response

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of the 17th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2009). Weimar, Germany. February 18-20, 2009

9.6.2. ISSN издания
1066-6192

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
379-386

9.12.1. Полное название издательства
IEEE Computer Society

9.12.2. Город, где расположено издательство
New-York

9.13. Краткий реферат публикации
В работе предлагается интегрированный проактивный подход к обнаружению и сдерживанию распространения сетевых червей в сети Интернет. Раскрываются особенности предлагаемого подхода, используемые модели и алгоритмы. Подход характеризуется реализацией "многорезолюционного" метода обнаружения, использования комбинации различных механизмов обнаружения, многоуровневой структурой системы защиты для комбинирования результатов различных алгоритмов обнаружения и адаптивностью механизмов обнаружения. Описывается реализованный прототип системы и результаты проведенных экспериментов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
25

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Vasiliy Desnitsky @ В.А. Десницкий; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Desnitsky V.A.

9.3.1. Другие авторы
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Kotenko I.V.

9.4. Название публикации
Analysis and Design of Entrusting Protocol for Distributed Software Protection

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of the Work in Progress Session held in connection with the 17th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2009). Weimar, Germany. February 2009

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
8-9

9.12.1. Полное название издательства
SEA-Publications

9.12.2. Город, где расположено издательство
Weimar

9.13. Краткий реферат публикации
Работа посвящена разработке протокола обмена сообщениями (“entrusting-протокол”), который является одним из важнейших элементов защиты программ от несанкционированных модификаций на основе модели “удаленного доверия”. Рассматривается выполненная реализация entrusting-протокола и проводится его анализ на основе формальных средств верификации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
2

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Dmitry Komashinskiy @ Д.В. Комашинский; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.2.2. Первый автор (для издания библиографических сборников)
Komashinskiy D.V.

9.3.1. Другие авторы
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation (SPIIRAS)

9.3.2. Другие авторы (для издания библиографических сборников)
Kotenko I.V.

9.4. Название публикации
@Malware Detection by Data Mining Techniques Based on Positionally Dependent Features

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). Pisa, Italy, 17-19 February, 2010

9.6.2. ISSN издания
1066-6192

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
принято в печать

9.9. Год публикации
2010

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
IEEE Computer Society

9.12.2. Город, где расположено издательство
New-York

9.13. Краткий реферат публикации
Представляемая работа посвящена применению методов интеллектуального анализа данных (Data Mining) для создания эвристических детекторов вредоносного программного обеспечения. Описываемый подход отличается от существующих направленностью обработку статической информации на основе использования позиционно-зависимых признаков, учитывающих особенности формата файлов, которые могут включать вредоносный код. В работе реализована и исследована общая методология формирования системы детектирования на базе применения методов выделения значимых признаков и методов классификации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
13

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Kotenko I.V.

9.3.1. Другие авторы
Alexander Ulanov @ А.В. Уланов; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Ulanov A.V.

9.4. Название публикации
@Simulation of Adaptable Agent Teams in Internet

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of the 1st International Workshop on Logics for Agents and Mobility (LAM'08). The European Summer School on Logic, Language and Information (ESSLLI 2008), Hamburg, Germany. 4-15 August, 2008

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
67-79

9.12.1. Полное название издательства
Hamburg University

9.12.2. Город, где расположено издательство
Hamburg

9.13. Краткий реферат публикации
В статье предлагается подход к многоагентному моделированию адаптивных распределенных систем в Интернет. Подход позволяет представить такие системы в виде множества команд агентов. Агенты команд могут быть в отношении безразличия, антагонистического противоборства и (или) кооперации, а также могут адаптироваться к изменениям внутренних компонентов и действиям других агентов. В статье рассматривается применение различных критериев адаптации для координации и взаимодействия агентов. Используются следующие процедуры: поддержка согласованности действий, мониторинг и восстановление функциональности агента, поддержка селективности коммуникаций. Подход имеет большую практическую важность. Он демонстрируется на примере многоагентного моделирования распределенных атак и систем защиты в Интернет. На основе заданных критериев адаптации, системы защиты могут приспосабливаться к действиям друг друга, изменяя механизмы формирования команд, режимы атаки, методы защиты, и т.д.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
31

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Vasiliy Desnitsky @ В.А. Десницкий; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.2.2. Первый автор (для издания библиографических сборников)
Desnitsky V.A.

9.3.1. Другие авторы
Igor Kotenko @ И.В. Котенко; 1; Россия; St. Petersburg Institute for Informatics and Automation

9.3.2. Другие авторы (для издания библиографических сборников)
Kotenko I.V.

9.4. Название публикации
Performance and Scalability of Remote Entrusting Protection

9.5. Язык публикации
английский

9.6.1. Полное название издания
Proceedings of the Second International Workshop on Remote Entrusting (RE-TRUST 2009). September 30 - October 1, 2009. Riva del Garda, Italy, 2009

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
принято в печать

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
Springer

9.12.2. Город, где расположено издательство
Berlin

9.13. Краткий реферат публикации
Статья посвящена исследованию аспектов масштабируемости и защищенности механизма защиты программного обеспечения против вмешательств и комбинированию различных методов защиты. Объектом исследования является механизм защиты ПО на основе принципа удаленного доверия. Предлагаемая методика включает получение количественных оценок производительности и степени защищенности рассматриваемых методов защиты. В результате на основе данной информации происходит выбор оптимальной комбинации методов защиты и их параметров.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
12

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Актуальные проблемы моделирования процессов защиты информации на основе технологии интеллектуальных агентов

9.5. Язык публикации
русский

9.6.1. Полное название издания
Известия СПбГЭТУ "ЛЭТИ". Специальный выпуск. Проблемы информатики: философия, науковедение, образование

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
93-109

9.12.1. Полное название издательства
СПбГЭТУ "ЛЭТИ"

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В работе рассматриваются актуальные проблемы моделирования процессов защиты информации на основе технологии интеллектуальных агентов и предложен подход к моделированию противоборства злоумышленников и систем защиты в сети Интернет в виде антагонистического взаимодействия команд программных агентов, представляющих злоумышленников и компоненты систем защиты. Основное внимание уделяется применению агентно-ориентированного моделирования с использованием имитации процессов защиты информации на уровне сетевых протоколов, что обеспечивает, с одной стороны, приемлемую для определенных классов задач точность процессов реализации компьютерных атак и механизмов защиты, а, с другой, - их масштабируемость.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
28

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
Противостояние в Интернет: моделирование противодействия распределенным кибератакам

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
485-494

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предложен подход к моделированию кибернетического противостояния в Интернет. Подход реализован в разработанной среде моделирования, позволяющей моделировать атаки, направленные на нарушение доступности информационных ресурсов, и механизмы защиты от них. Проведено большое количество экспериментов, в которых исследовались параметры эффективности механизмов защиты от топологии и конфигурации сети, структуры и конфигурации команд атаки и защиты, механизмов реализации атак и защиты и параметров кооперации команд защиты. Эксперименты показали, что использование кооперации команд защиты приводит к существенному повышению эффективности защиты. В дальнейшем планируется совершенствование среды моделирования, более глубокое исследование эффективности механизмов кооперации различных команд и внутрикомандного взаимодействия агентов, реализация механизмов адаптации и самообучения агентов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
4

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.С. Богданов; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Богданов В.С.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Проактивный подход к мониторингу выполнения политики безопасности компьютерных сетей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
373-382

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предложен подход к проактивному мониторингу выполнения политики безопасности в компьютерной сети на основе сравнения поведения компьютерной сети с математической моделью. Предложен подход к моделированию основных механизмов реализации политики безопасности в сети: брандмауэров и различных сетевых сервисов. Рассмотрены недостатки проактивного подхода и методы их устранения. Указанный подход был воплощен в программном прототипе системы проактивного мониторинга (СПМ) выполнения политики безопасности. Направлениями дальнейших исследований является разработка методов оптимизации тестовых воздействий, совершенствование предложенных моделей и методик проактивного мониторинга и проведение экспериментальной оценки предложенных решений.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
5

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Тишков; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Тишков А.В.

9.3.1. Другие авторы
И.В. Котенко; 1; РоссияЕ.В. Сидельникова; 1; РоссияО.В. Черватюк; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.Сидельникова Е.В.Черватюк О.В.

9.4. Название публикации
Обнаружение и разрешение противоречий в политиках безопасности

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
172-185

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе приведена и обоснована идея построения многомодульной архитектуры верификатора политик безопасности, и ее отображение на классификацию противоречий, которые могут возникнуть при создании политики и ее применении к конкретной сети. Система верификации разработана на языке Java, с использованием JDK 1.5.0. При реализации абдуктивного вывода для исчисления событий использовался продукт CIFF 3.0, который распространяется в качестве библиотеки, использующей, в свою очередь вызывающей SICStus Prolog. В качестве верификатора моделей был выбран SPIN 4.2.6. Остальные модули реализованы без использования дополнительного программного обеспечения. Были проведены различные эксперименты.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
9

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
М.В. Степашкин; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Степашкин М.В.

9.4. Название публикации
Оценка защищенности компьютерных сетей на основе анализа графов атак

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
466-481

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предложен подход к анализу уязвимостей и оценке уровня защищенности компьютерных сетей, предназначенный для реализации на различных этапах жизненного цикла компьютерных сетей, основанный на генерации графов атак и вычислении показателей защищенности, дан анализ сложности алгоритма формирования графа атак и предложены подходы для ее уменьшения.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
11

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В.В. Воронцов; 1; РоссияА.В. Тишков; 1; РоссияА.А. Чечулин; 1; РоссияА.В. Уланов; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Воронцов В.В.Тишков А.В.Чечулин А.А.Уланов А.В.

9.4. Название публикации
@Исследование проактивных механизмов защиты от сетевых червей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы безопасности и противодействия терроризму. Материалы третьей международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
278-283

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предлагается проактивный подход к защите от сетевых червей, базирующийся на использовании механизмов обнаружения и ограничения интенсивности соединений сетевых червей, а также рассматриваются модели и разрабатываемое программное средство для исследования механизмов защиты от сетевых червей на основе моделирования различных типов и экземпляров сетевых червей и механизмов защиты от них.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
2

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
@Моделирование кооперативных механизмов защиты компьютерных сетей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы безопасности и противодействия терроризму. Материалы третьей международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
266-271

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В отличие от предыдущих работ авторов в данной работе рассматриваются особенности моделирования распределенных кооперативных механизмов защиты и представляются различные эксперименты по исследованию кооперативных механизмов защиты. К распределенным кооперативным механизмам защиты от атак DDoS, рассматриваемым в работе, относятся, например, механизмы, реализующие защиту с помощью переноса ресурсов (Server Roaming), изменения количества ресурсов, разграничения ресурсов (Market-based Service Quality Differentiation (MbSQD), Transport-aware IP router architecture (tIP)), аутентификации (tIP, Secure Overlay Services (SOS)), а также механизмы, выполняющие отслеживание с разметкой пакетов и хранением их сигнатур, в том числе осуществляющие "отталкивание", генерацию служебных пакетов и др (ACC pushback, COSSACK, Perimeter-based DDoS defense, DefCOM, Gateway-based).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
2

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Проектирование и анализ протокола удаленного доверия

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы безопасности и противодействия терроризму. Материалы четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
214-219

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Работа посвящена исследованию модели защиты программ на основе механизма «удаленного доверия» и, в частности, разработке и анализу коммуникационного протокола (entrusting-протокола), предназначенного для обеспечения безопасной передачи сообщений в рамках данной модели защиты. В работе рассматриваются основные виды атак на entrusting-протокол и соответствующие им модели нарушителя. Формируются основные требования к безопасности протокола. Предлагается общая методика построения entrusting-протокола, а также варианты реализации его программного прототипа.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
2

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Д.В. Комашинский; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Комашинский Д.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Исследование проактивных механизмов обнаружения вредоносного программного обеспечения на базе методов DATA MINING

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы безопасности и противодействия терроризму. Материалы четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
226-231

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе рассматривается подход к проактивному обнаружению вредоносного ПО, базирующийся на скрытном сборе информации о поведении запущенных приложений и ее обработке методами интеллектуального анализа данных (Data Mining). Предлагаемый подход отличается от существующих направленностью на циклическую интерактивную скрытную обработку поведенческой информации, а также интегрированным использованием методов интеллектуального анализа данных для различных классов вредоносного ПО.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
5

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.А. Чечулин; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Чечулин А.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Защита от сетевых атак методами фильтрации и нормализации протоколов транспортного и сетевого уровня стека TCP/IP

9.5. Язык публикации
русский

9.6.1. Полное название издания
Проблемы безопасности и противодействия терроризму. Материалы четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания
2

9.10.2 Номер издания

9.11. Страницы
242-247

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Работа посвящена классификации атак, основанных на использовании стека протоколов TCP/IP, разбору и сравнению методов фильтрации и нормализации для каждого класса атак, а также разработке комплексного механизма фильтрации и нормализации трафика, предназначенного для использования на сетевом оборудовании.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
5

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Защита программного обеспечения на основе принципа удаленного доверия

9.5. Язык публикации
русский

9.6.1. Полное название издания
Восьмая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2009). Москва, МГУ, 2010

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
принято в печать

9.9. Год публикации
2010

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Работа посвящена исследованию модели защиты программ на основе механизма «удаленного доверия». Представлен обзор атомарных методов защиты, используемых в рамках данного механизма. Рассматриваются также некоторые возможные способы оптимизации методов защиты, которые способны улучшить производительность механизма, а, следовательно, степень его масштабируемости.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
3

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Д.В. Комашинский; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Комашинский Д.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
@Обнаружение malware на основе обработки статической позиционной информации методами Data Mining

9.5. Язык публикации
русский

9.6.1. Полное название издания
Восьмая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2009). Москва, МГУ, 2010

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
принято в печать

9.9. Год публикации
2010

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
МЦНМО

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе описывается подход к обнаружению вредоносного программного обеспечения, который отличается от существующих фокусом на обработку позиционно-зависимой статической информации. Такая обработка позволяет обеспечить формирование отдельных элементов эффективной комплексной модели обнаружения исполняемых вредоносных объектов. Эти элементы в дальнейшем могут быть использованы совместно за счет комбинирования с уже существующими методами, а также отдельно для выполнения задач, решаемых при уточнении общего контекста задачи анализа. На основе результатов экспериментов формируются задачи, которые подлежат реализации при дальнейших исследованиях комплексного использования существующих методов обнаружения.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
6

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Уланов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Уланов А.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Модели противоборства команд агентов, реализующих атаки «распределенный отказ в обслуживании» и механизмы защиты от них

9.5. Язык публикации
русский

9.6.1. Полное название издания
Труды Международных научно-технических конференций "Интеллектуальные системы (AIS'07)" и "Интеллектуальные САПР (CAD-2007)"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
120-127

9.12.1. Полное название издательства
Физматлит

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предлагается общий подход к моделированию противоборства команд агентов в информационной среде. Модели этих команд рассматриваются на примере распределенных атак «отказ в обслуживании» и механизмов защиты от них. Команды защиты имеют возможность работать в различных кооперативных схемах, в том числе, реализуя определенный распределенный механизм защиты.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
6

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В.В. Воронцов; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Воронцов В.В.

9.4. Название публикации
Проактивный подход к обнаружению и сдерживанию сетевых червей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Труды Международных научно-технических конференций "Интеллектуальные системы (AIS'07)" и "Интеллектуальные САПР (CAD-2007)"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
61-68

9.12.1. Полное название издательства
Физматлит

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предлагается проактивный подход к защите от сетевых червей, базирующийся на использовании механизмов обнаружения и сдерживания распространения сетевых червей (посредством ограничения интенсивности соединений от инфицированных и подозрительных хостов). Подход характеризуется реализацией четырех свойств: (1) "многорезолюционный" метод обнаружения, (2) использование различных механизмов обнаружения, (3) многоуровневость структуры системы защиты для комбинирования результатов различных алгоритмов обнаружения и (4) адаптивность механизмов обнаружения. В работе раскрываются особенности предлагаемого подхода и функциональная архитектура основанной на знаниях системы обнаружения и сдерживания распространения сетевых червей.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
8

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Модели удаленной аутентификации для защиты программ

9.5. Язык публикации
русский

9.6.1. Полное название издания
Труды Международных научно-технических конференций "Интеллектуальные системы (AIS'07)" и "Интеллектуальные САПР (CAD-2007)"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
43-50

9.12.1. Полное название издательства
Физматлит

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В статье предлагаются модели защиты программного обеспечения от несанкционированных изменений на основе механизма удаленной аутентификации. Проводится анализ некоторых дополнительных аспектов, связанных с реализацией механизма удаленной аутентификации: распределение функций верификации между клиентской программой и надежным сервером, а также возможные действия, выполняемые сервером для предотвращения дальнейшего функционирования клиентской программы в случае обнаружения злонамеренных изменений. Предлагается модель атак на рассматриваемый механизм аутентификации, основанная на использовании ориентированных графов. Основные элементы этой модели – это состояния программы и действия, выполняемые над ней потенциальным нарушителем.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
5

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Тишков; 1; РоссияВ.В. Воронцов; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Тишков А.В.Воронцов В.В.

9.4. Название публикации
Комбинирование механизмов защиты от злонамеренного программного обеспечения

9.5. Язык публикации
русский

9.6.1. Полное название издания
Труды Международных научно-технических конференций "Интеллектуальные системы (AIS'08)" и "Интеллектуальные САПР (CAD-2008)"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания
2

9.10.2 Номер издания

9.11. Страницы
426-432

9.12.1. Полное название издательства
Физматлит

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предлагаются модели и методы комбинирования механизмов обнаружения и сдерживания распространения сетевых червей, разрабатываемые в рамках исследуемого авторами проактивного подхода к защите от сетевых червей. Раскрываются особенности комбинирования, и приводится методика определения коэффициентов применимости отдельных механизмов защиты. В качестве основы для определения коэффициентов применимости отдельных механизмов защиты предлагается использовать значения статистических параметров сетевого трафика и результаты анализа эффективности отдельных механизмов обнаружения и сдерживания.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
8

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАНС.А. Резник; 2; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.Резник С.А.

9.4. Название публикации
Разработка и анализ протокола обмена сообщениями для механизма удаленного доверия

9.5. Язык публикации
русский

9.6.1. Полное название издания
Труды Международных научно-технических конференций "Интеллектуальные системы (AIS'08)" и "Интеллектуальные САПР (CAD-2008)"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания
2

9.10.2 Номер издания

9.11. Страницы
418-425

9.12.1. Полное название издательства
Физматлит

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Важнейшим элементом механизма защиты программ от несанкционированных модификаций на основе модели "удаленного доверия" является протокол обмена сообщениями ("entrusting-протокол"), предназначенный для передачи сообщений между клиентской программой и доверенным сервером. Настоящая статья посвящена разработке entrusting-протокола и его анализу на основе формальных средств верификации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
13

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Интеллектуальные механизмы защиты от распространения злонамеренного программного обеспечения

9.5. Язык публикации
русский

9.6.1. Полное название издания
Труды Международных научно-технических конференций "Интеллектуальные системы (AIS'09)" и "Интеллектуальные САПР (CAD-2009)"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания
2

9.10.2 Номер издания

9.11. Страницы
431-438

9.12.1. Полное название издательства
Физматлит

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Рассматривается подход к защите от распространения злонамеренного программного обеспечения (сетевых червей, вирусов и др.) в сети Интернет, базирующийся на применении различных интеллектуальных эвристических механизмов, их комбинировании и автоматической динамической адаптации в соответствии с текущей сетевой обстановкой. Представлены программная реализация системы моделирования механизмов защиты и результаты экспериментов по обнаружению и сдерживанию различных сетевых червей.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
9

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации

9.5. Язык публикации
русский

9.6.1. Полное название издания
Математические методы распознавания образов: 13-я Всероссийская конференция (ММРО-13). Ленинградская обл., г. Зеленогорск, 30 сентября - 6 октября 2007 г.: Сборник докладов

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
599-602

9.12.1. Полное название издательства
МАКС Пресс

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Используемым в настоящее время подходам к защите информации в распределенных компьютерных системах присущ целый ряд недостатков, и системы защиты информации (СЗИ) оказываются не в состоянии эффективно решать задачу управления защищенностью в режиме реального времени. Эти недостатки обусловлены, главным образом, узкой специализацией отдельных средств обеспечения безопасности, неразвитыми механизмами верификации защиты на этапах создания и поддержки, неадекватными механизмами определения уязвимостей, анализа рисков и определения уровня защищенности, мониторинга состояния сетей и адаптации к изменению условий функционирования. В докладе предлагается подход к разработке и использованию СЗИ, основанный на использовании интеллектуальной надстройки над традиционными механизмами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем защиты.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
1

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Уланов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Уланов А.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Многоагентная среда для проведения экспериментов по защите компьютерных сетей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Математические методы распознавания образов: 13-я Всероссийская конференция (ММРО-13). Ленинградская обл., г. Зеленогорск, 30 сентября - 6 октября 2007 г.: Сборник докладов

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
631-634

9.12.1. Полное название издательства
МАКС Пресс

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предлагается подход и реализованная среда многоагентного моделирования для анализа существующих и перспективных методов защиты от атак "распределенный отказ в обслуживании". Подход базируется на представлении систем, реализующих компьютерные атаки и защиту от них, в виде команд интеллектуальных агентов. В работе реализован ряд методов кооперативной защиты и проведено исследование их эффективности.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
2

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
Исследование моделей противоборства агентов в компьютерных сетях

9.5. Язык публикации
русский

9.6.1. Полное название издания
Мультиконференция «Теория и системы управления». IV Международная конференция по проблемам управления (МКПУ-IV). Сессия «Многоагентные системы и групповое управление». 26-30 января 2009 г.

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
Учреждение Российской академии наук Институт проблем управления им. В.А.Трапезникова РАН

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе рассматривается подход к исследованию киберпротивоборства в компьютерных сетях на основе моделирования антагонистического взаимодействия команд агентов, представляющих атакующих (злоумышленников, кибертеррористов) и компоненты систем защиты информации. Основное внимание уделяется применению агентно-ориентированного моделирования с использованием имитации процессов защиты информации на различных уровнях сетевого взаимодействия. Подход рассмотрен на примере моделирования механизмов защиты от распределенных атак "отказ в обслуживании".

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
36

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Уланов; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Уланов А.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Моделирование адаптивных кооперативных стратегий защиты от компьютерных атак в сети Интернет

9.5. Язык публикации
русский

9.6.1. Полное название издания
Третья всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2007). Санкт-Петербург, 17-19 октября 2007 г. Сборник докладов.

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
2

9.10.2 Номер издания

9.11. Страницы
211-215

9.12.1. Полное название издательства
ФГУП ЦНИИ технологии судостроения

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В статье рассматривается подход и разработанная программная среда для многоагентного моделирования распределенных атак и механизмов защиты от них. Подход заключается в представлении сторон атак и защиты в виде команд интеллектуальных агентов. Основное внимание уделяется особенностям имитационного моделирования механизмов адаптации команд агентов к действиям друг друга в соответствии с заданными критериями. Агенты атаки пытаются реализовать и поддерживать атаку в заданном режиме, а агенты защиты – наилучшим образом отражать атаку, отслеживать состояние и обезвреживать атакующих. Приводятся примеры проведенных экспериментов по применению адаптивных кооперативных стратегий защиты.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
10

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; РоссияА.В. Тишков; 1; РоссияВ.С. Богданов; 1; РоссияВ.В. Воронцов; 1; РоссияА.А. Чечулин; 2; Россия

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.Тишков А.В.Богданов В.С.Воронцов В.В.Чечулин А.А.

9.4. Название публикации
Имитационное моделирование механизмов обнаружения и сдерживания сетевых червей в компьютерных сетях

9.5. Язык публикации
русский

9.6.1. Полное название издания
Третья всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2007). Санкт-Петербург, 17-19 октября 2007 г. Сборник докладов.

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания
2

9.10.2 Номер издания

9.11. Страницы
106-109

9.12.1. Полное название издательства
ФГУП ЦНИИ технологии судостроения

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В работе предлагается подход и средство имитационного моделирования, предназначенное для исследования механизмов обнаружения и сдерживания распространения сетевых червей. Подход характеризуется реализацией четырех основных свойств: "многорезолюционный" метод обнаружения; использование различных механизмов обнаружения; многоуровневость структуры системы защиты для комбинирования результатов различных алгоритмов защиты; адаптивность механизмов обнаружения. В работе раскрываются особенности предлагаемого подхода, представляется архитектура системы моделирования обнаружения и сдерживания распространения сетевых червей, и описываются проведенные эксперименты.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
7

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Многоагентное моделирование для исследования механизмов защиты информации в сети Интернет

9.5. Язык публикации
русский

9.6.1. Полное название издания
Четвертая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2009). Санкт-Петербург, 21-23 октября 2009 г. Сборник докладов.

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания
1

9.10.2 Номер издания

9.11. Страницы
38-47

9.12.1. Полное название издательства
ФГУП ЦНИИ технологии судостроения

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В связи с большой сложностью Интернет и невозможностью воспроизведения реальных событий, связанных с сетевыми атаками, в том числе в силу возможных негативных последствий, имитационное моделирование играет важную роль для исследования механизмов защиты от сетевых атак (таких как "распределенный отказ в обслуживании", распространение сетевых червей и др.). В работе предлагается подход к многоагентному моделированию, применимый для исследования данных классов атак и механизмов защиты от них. Подход заключается в имитации антагонистического взаимодействия команд программных агентов, представляющих злоумышленников и компоненты систем защиты. Рассматривается разработанная среда моделирования и результаты проведенных экспериментов по исследованию распределенных кооперативных механизмов защиты.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
11

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
Р.М. Юсупов; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Юсупов Р.М.

9.4. Название публикации
Актуальные исследования в области защиты компьютерных сетей и систем

9.5. Язык публикации
русский

9.6.1. Полное название издания
Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
21-31

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В работе характеризуется текущее состояние в области безопасности компьютерных систем и сетей, рассматриваются актуальные направления исследований в области защиты компьютерных сетей и систем. Проводится анализ работ, выполняемых в настоящее время в Санкт-Петербургском институте информатики и автоматизации РАН (СПИИРАН), в таких направлениях как интеллектуализация механизмов защиты, поддержка жизненного цикла систем защиты и моделирование кибер-противоборства. Рассматриваются основные результаты исследований, проводимых в группе компьютерной безопасности СПИИРАН.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
18

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В.В. Воронцов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАНА.А. Чечулин; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Воронцов В.В.Чечулин А.А.

9.4. Название публикации
Анализ механизмов обнаружения и сдерживания сетевых червей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
113-119

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В статье рассматриваются два реализованных и исследованных механизма обнаружения и сдерживания: механизм, использующий "пороговое случайное прохождение", и механизм, основанный на кредитах доверия. Поводится сравнительный анализ эффективности применения рассмотренных механизмов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
7

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Модель защиты программ на основе механизма "удаленного доверия"

9.5. Язык публикации
русский

9.6.1. Полное название издания
Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
172-177

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Основным составным элементом рассматриваемого в данной статье подхода к защите программного обеспечения от несанкционированных модификаций является механизм «удаленного доверия» (remote entrusting). Данный механизм предполагает реализацию защиты программ посредством их программной верификации удаленным защищенным сервером в реальном времени. Важным преимуществом данного подхода является возможность учета возможных временных ограничений на выполнение потенциальным злоумышленником несанкционированных изменений и вмешательств (взлома).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
4

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В.В. Воронцов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Воронцов В.В.

9.4. Название публикации
Использование проактивного подхода для защиты от сетевых червей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
41-44

9.12.1. Полное название издательства
РАН

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Сегодня атаки сетевых червей и вирусов уверенно лидируют во всех хит-парадах угроз сетевой безопасности. Этот вид вредоносного программного обеспечения не только наносит прямой финансовый ущерб, но и служит базисом для реализации многих других опасных угроз (несанкционированный доступ к данным, кража конфиденциальной информации, нарушение приватной личной информации, отказ в обслуживании и т.п.). С другой стороны, существующие системы обнаружения не всегда способны оперативно остановить развитие эпидемии на начальных этапах, поэтому остро стоит вопрос о разработке качественно новых систем обнаружения и сдерживания сетевых эпидемий. Для решения этой проблемы предлагается применение проактивного подхода, базирующегося на использовании механизмов обнаружения и сдерживания распространения сетевых червей.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
8

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Удаленная аутентификация для защиты программ от несанкционированного изменения

9.5. Язык публикации
русский

9.6.1. Полное название издания
Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
32-34

9.12.1. Полное название издательства
РАН

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Данная работа посвящена представлению предлагаемой модели защиты программного обеспечения от несанкционированных изменений на основе механизма удаленной аутентификации, а также модели атак на рассматриваемый механизм удаленной аутентификации, основанной на использовании ориентированных графов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
5

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Уланов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Уланов А.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Методика проведения имитационного моделирования противостояния систем защиты атакам DDOS в сети Интернет

9.5. Язык публикации
русский

9.6.1. Полное название издания
Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
38-40

9.12.1. Полное название издательства
РАН

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Рассматриваются особенности предлагаемой методики проведения имитационного моделирования противостояния систем защиты атакам DDOS в сети Интернет. Представляются параметры моделируемых механизмов защиты и атаки, особенности реализации стенда моделирования и результаты проведенных экспериментов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
5

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Аспектно-ориентированный подход к реализации механизма мобильного модуля в системе защиты программного обеспечения

9.5. Язык публикации
русский

9.6.1. Полное название издания
Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
35-37

9.12.1. Полное название издательства
РАН

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Одной из задач системы защиты программного обеспечения от несанкционированных изменений является выработка механизма, обеспечивающего возможность периодического обновления мобильного модуля, встраиваемого в защищаемое программное обеспечение. Обновляемый модуль состоит из монитора, выполняющего набор верификаций, и генератора подписей, порождающего необходимую для надежного сервера информацию о состоянии клиентской программы. Регулярное обновление модуля выполняется для того, чтобы ограничить время, затрачиваемое потенциальным нарушителем с целью осуществления атаки на модуль. В работе проанализированы основанные на аспектно-ориентированном программировании подходы, которые могут быть использованы для реализации механизма мобильного модуля в системе защиты программного обеспечения.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
4

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
Исследование механизмов защиты от атак DDOS: имитация противоборства интеллектуальных агентов в сети Интернет

9.5. Язык публикации
русский

9.6.1. Полное название издания
Международная конференция "РусКрипто'2008"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
Ассоциация "РусКрипто"

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В работе предлагается подход к исследованию атак DDOS и механизмов защиты от них. В его основу положено представление сторон атаки и защиты в виде команд интеллектуальных агентов, которые могут противоборствовать, кооперироваться и адаптироваться к действиям друг друга. Описаны разработанные модели взаимодействия команд: антагонистическое противоборство, кооперативная защита, адаптивная схема.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
4

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Проактивные механизмы защиты от быстро распространяющихся сетевых червей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Международная конференция "РусКрипто'2008"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
Ассоциация "РусКрипто"

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В докладе рассматривается проактивный подход к защите от быстро распространяющихся сетевых червей в сети Интернет. Подход базируется на комбинировании различных механизмов обнаружения и сдерживания сетевых червей и автоматической динамической адаптации механизмов защиты в соответствии с изменением сетевой конфигурации и сетевого трафика. Предлагаемый подход предназначен для обнаружения сетевых червей (посредством выявления их действий по сканированию уязвимых хостов) и сдерживания их дальнейшего распространения за счет ограничения и блокирования посылаемых инфицированными узлами сетевых пакетов. В докладе описываются особенности данного подхода и программной реализации разработанной авторами системы моделирования механизмов защиты от сетевых червей.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
10

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
"Сетевые кошки-мышки": войны адаптивных программных агентов

9.5. Язык публикации
русский

9.6.1. Полное название издания
Международная конференция "РусКрипто'2009"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
Ассоциация "РусКрипто"

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
В данной работе, на примере защиты от компьютерных атак "Распределенный отказ в обслуживании" в сети Интернет, предлагается подход к исследованию адаптивных и кооперативных механизмов функционирования команд интеллектуальных агентов. Предлагаемый подход основан на представлении сетевых систем в виде комплекса команд взаимодействующих агентов, которые могут быть в состоянии антагонистического противостояния, безразличия или кооперации. Агрегированное поведение системы выражается в локальных взаимодействиях агентов. Задача многоагентного моделирования процессов кибернетического противоборства представляется как моделирование антагонистического взаимодействия команды агентов-злоумышленников и агентов защиты. В докладе рассматриваются методы организации командной работы агентов, структуры команд агентов нападения и защиты, механизмы их взаимодействия и планы действий, реализованный стенд (среда) моделирования противоборства агентов и различные примеры реализованных сценариев моделирования.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
3

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Подход к защите программ на основе механизма удаленного доверия

9.5. Язык публикации
русский

9.6.1. Полное название издания
Международная конференция "РусКрипто'2009"

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
Ассоциация "РусКрипто"

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Работа посвящена разработке и анализу модели защиты программ на основе механизма удаленного доверия. Цель данного подхода – обнаружение несанкционированных модификаций клиентской программы, выполняющейся в потенциально враждебном окружении. Механизм ориентирован, в первую очередь, на защиту приложений, для корректного функционирования которых требуются сетевые коммуникации с удаленными клиентами или серверами. В работе представлены основные виды атак, компрометирующие защищаемую программу, в том числе, атака клонирования, которая является наиболее сложно обнаружимой. Рассматриваются дополнительные идеи, которые могут использоваться для повышения устойчивости программы к атакам, а именно, осуществление части верификаций в пределах доверенного сервера; реализация модели с несколькими мониторами, каждый из которых верифицирует остальные; само-верификация монитора.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
5

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Д.В. Комашинский; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Комашинский Д.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАНА.В. Шоров; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.Шоров А.В.

9.4. Название публикации
Обнаружение вредоносного программного обеспечения на базе методов интеллектуального анализа данных

9.5. Язык публикации
русский

9.6.1. Полное название издания
Обнаружение вредоносного программного обеспечения на базе методов интеллектуального анализа данных

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
Ассоциация "РусКрипто"

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Работа посвящена применению методов интеллектуального анализа данных для построения средств эвристического детектирования. Помимо раскрытия общей постановки задачи и анализа результатов предыдущих релевантных исследований в работе представляется собственная точка зрения на возможные пути решения проблемы детектирования вредоносного ПО средствами эвристического анализа. Предлагаемый подход основан на скрытном процессе циклического интерактивного сбора поведенческой информации, который в совокупности с результатами обобщения доступной статической информации, извлекаемого из файлового контейнера исследуемого объекта, облегчает принятие решения о степени его опасности. Также при подготовке данного подхода внимание было уделено вопросам интегрированного использования различных методов интеллектуального анализа данных для различных классов вредоносного ПО. В работе реализовано и исследовано семейство различных методов интеллектуального анализа, основанных на Байесовском подходе, деревьях решений, нейронных сетях и др. Предлагается общий интегрированный подход к реализации комплекса методов детектирования вредоносного программного обеспечения.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
3

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.А. Чечулин; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Чечулин А.А.

9.3.1. Другие авторы
Ю.В. Зозуля; 2; Россия; СПИИРАНИ.В. Котенко; 1; Россия; СПИИРАНА.В. Тишков; 1; Россия; СПИИРАНА.В. Шоров; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Зозуля Ю.В.Котенко И.В.Тишков А.В.Шоров А.В.

9.4. Название публикации
Методы защиты от вредоносных Web-сайтов на основе оценок репутации

9.5. Язык публикации
русский

9.6.1. Полное название издания

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
Ассоциация "РусКрипто"

9.12.2. Город, где расположено издательство
Москва

9.13. Краткий реферат публикации
Одним из классов методов, которые могут использоваться для защиты от вредоносных Web-сайтов, является так называемые репутационные методы. Эти методы базируются на понятии репутации, отражающей некоторую меру вредоносности сайта, определяемую на основе множества источников. В докладе проводится анализ существующих методов оценки репутации и предлагается подход к оценке репутации Web-сайтов, формируемый на основе многофакторного анализа его характеристик, получаемых из различных источников.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
9

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.С. Богданов; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Богданов В.С.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Проактивный мониторинг выполнения политики безопасности компьютерной сети

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
32

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе рассмотрена задача анализа соответствия спроектированной политики безопасности компьютерной сети ее реализации. Данная задача становится актуальной с началом периода функционирования компьютерной сети и не утрачивает своей актуальности на протяжении всего периода ее эксплуатации. Ввиду сложности современных компьютерных сетей необходимы методики, позволяющие автоматизировать процесс решения данной задачи. Данный доклад посвящен рассмотрению разработанной методики проактивного мониторинга политики безопасности и ее реализации в виде программного комплекса.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В.В. Воронцов; 1; Россия; СПИИРАНА.В. Уланов; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Воронцов В.В.Уланов А.В.

9.4. Название публикации
Проактивное обнаружение и сдерживание распространения сетевых червей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
91

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В настоящее время в связи с увеличением скорости появления новых сетевых червей большую роль играет своевременное обнаружение и дальнейшее блокирование развития сетевой эпидемии. Существующие системы раннего оповещения и сдерживания имеют ряд существенных недостатков, в том числе неудовлетворительное качество обнаружения и блокирования легитимного трафика, характерного для P2P-сетей или узлов, демонстрирующих высокую сетевую активность. Для решения этих трудностей, в работе предлагается проактивный подход. Предполагается, что разрабатываемая система ориентирована на реализацию на сетевом оборудовании, в частности на коммутаторе. В качестве основных признаков инфицированности узла используется факт посылки узлом большого количества сетевых пакетов к заданному количеству новых адресов с частотой, превышающей установленную, и большого количества неудачных соединений. Разрабатываемая система обнаружения и сдерживания сетевых червей имеет двухуровневую архитектуру. Первый уровень представляет собой базовые классификаторы, которые реализуют отдельные методы обнаружения и их модификации (например, методы «virus throttling», TRW-методы и др.). Второй уровень представляет собой мета-классификатор, осуществляющий комбинирование различных алгоритмов обнаружения и сдерживания, а также общие процедуры, необходимые для реализации при сетевой защите (поддержка списков ACL для механизмов обнаружения и др.).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
А.В. Уланов; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Уланов А.В.

9.4. Название публикации
Моделирование адаптивного противостояния систем защиты распределенным атакам

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
92

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В работе предлагаются модели для исследования перспективных адаптивных и кооперативных систем защиты в Интернет. Подход основан на многоагентном моделировании атак "распределенный отказ в обслуживании". В соответствии с этим подходом системы атаки и защиты представляются как команды интеллектуальных агентов, взаимодействующих в соответствии с заданным критерием адаптации. На основе этого критерия системы защиты и атаки изменяют свою конфигурацию и поведение в зависимости от состояния сети и серьезности атаки. Предложенные схемы адаптации были реализованы в разработанной среде моделирования распределенных атак «отказ в обслуживании» и механизмов защиты от них.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
С.А. Резник; 2; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Резник С.А.

9.3.1. Другие авторы
О.В. Черватюк; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Черватюк О.В.

9.4. Название публикации
Обнаружение конфликтов фильтрации и защиты каналов в политике безопасности на основе методов верификации на модели

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
37

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
При создании и развертывании распределенных систем с достаточно сложным набором политики безопасности необходимо убедиться в том, что созданная политика не содержит внутренних конфликтов. Такого рода конфликты могут быть как статическими, так и динамическими. При этом обнаружение статических конфликтов можно осуществлять с помощью формул логики предикатов первого порядка. Для динамических же конфликтов этого не достаточно, поскольку динамический конфликт может возникнуть лишь по мере наступления определенных событий. Таким образом, встает проблема обнаружения динамических конфликтов. В работе предлагается подход к обнаружению динамических конфликтов на основе использования средства верификации моделей SPIN, позволяющего описывать модель параллельных взаимодействующих между собой и взаимно синхронизирующихся процессов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 2; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Удаленная аутентификация как механизм защиты программ на удаленных клиентах

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В работе предлагается подход к защите программ от несанкционированных изменений и вмешательств на основе механизма удаленной аутентификации. Данный механизм предполагает использование надежного сервера, который контролирует процесс выполнения клиентской программы: во время работы сервер непрерывно получает информацию о текущем состоянии выполняющейся удаленно клиентской программы, анализирует ее, после чего принимает решение о том, было ли осуществлено вмешательство в работу программы или нет. В работе также поднимается вопрос о распределении местоположения конкретных функций верификации между монитором клиентской программой и надежным сервером. Перенос части кода верификаций на сервер способствует повышению устойчивости всей программы к взлому. В работе предложена модель атак на рассматриваемый механизм удаленной аутентификации.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Уланов; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Уланов А.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Архитектура и модель среды многоагентного моделирования атак DDoS и защиты от них

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
96

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В работе предлагается архитектура среды для исследования атак «распределенный отказ в обслуживании» (DDoS) и механизмов защиты от них. Стороны атаки и защиты представляются в виде комплекса различных взаимодействующих команд интеллектуальных агентов, которые могут находиться между собой как в состоянии антагонистического противоборства, так и кооперации. Используемый подход к моделированию предполагает наличие следующих компонентов системы моделирования: базовую систему имитационного моделирования (Simulation Framework), модуль (пакет) моделирования сети Интернет (Internet Simulation Framework), подсистему агентно-ориентированного моделирования (Agent-based Framework) и модуль (библиотеку) имитации процессов предметной области (Subject Domain Library).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.В. Воронцов; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Воронцов В.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Моделирование распространения сетевых червей

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
88

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Важным направлением исследований в области компьютерной безопасности в настоящее время являются исследования и разработка новых методов обнаружения и сдерживания сетевых эпидемий. В связи с невозможностью проведения испытаний предлагаемых методов обнаружения и сдерживания сетевых червей в реальных условиях по вполне очевидным причинам, проверка разработанных систем обычно проводится на моделях эпидемий сетевых червей. В настоящее время в СПИИРАН ведутся работы по созданию перспективных механизмов защиты от сетевых червей. Для решения задачи тестирования разработанного механизма обнаружения и сдерживания исследуются различные подходы к моделированию распространения сетевых червей. В докладе рассматриваются различные подходы к моделированию сетевых червей и механизмов защиты от них.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАНС.А. Резник; 2; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.Резник С.А.

9.4. Название публикации
Разработка и анализ протокола обмена сообщениями для защиты программ посредством "удаленного доверия"

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVII Общероссийской научно-технической конференции. 7-11 июля 2008 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
16

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Актуальной проблемой в области компьютерной безопасности является защита программ от несанкционированных модификаций. Работа посвящена разработке и анализу протокола обмена сообщениями ("entrusting-протокола"), действующего в рамках механизма защиты программ от несанкционированных модификаций на основе модели "удаленного доверия". Рассматриваются модели злоумышленника, осуществляющего компрометацию процесса выполнения entrusting-протокола, определяются и анализируются основные требования к entrusting-протоколу, реализация которых позволяет повысить его безопасность. Анализируюся методики верификации, используемые для доказательства корректности и надежности протокола, в частности, основанные на методе проверки на модели, а также формальном доказательстве целевых свойств. Представлены примеры программного кода, демонстрирующие верификацию упрощенного варианта entrusting-протокола при помощи инструментов верификации AVISPA и Isabelle.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
В.В. Воронцов; 1; Россия; СПИИРАНА.А. Чечулин; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Воронцов В.В.Чечулин А.А.

9.4. Название публикации
Обнаружение и сдерживание распространения злонамеренного программного обеспечения на основе комбинированных механизмов

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVII Общероссийской научно-технической конференции. 7-11 июля 2008 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
27

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Представляется, что при большом количестве узлов в контролируемой сети и многообразии работающих в ней приложений перспективным подходом к обнаружению и сдерживанию развития сетевой эпидемии является согласованное использование комплекса различных механизмов защиты. Это объясняется, в первую очередь тем, что отдельные методы ориентированы преимущественно на определенный тип трафика и вид злонамеренного программного обеспечения, а комбинированные механизмы позволяют объединить преимущества отдельных методов и нивелировать их недостатки. В работе рассматривается разработка проактивной системы защиты от распространения сетевых червей, основанной на использовании комбинированных механизмов обнаружения и сдерживания сетевых эпидемий на основе кооперативной работы различных механизмов защиты (методов "virus throttling", TRW-методов, методов, основанных на "кредитах доверия" и др.).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Моделирование процессов защиты информации от инфраструктурных атак

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVIII Общероссийской научно-технической конференции. 29 июня - 2 июля 2009 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
63

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Доклад посвящен разработке методологического подхода к исследованию инфраструктурных атак и механизмов защиты от них на основе комплексного подхода к моделированию, базирующегося на интеграции агентно-ориентированного и имитационного моделирования на уровне сетевых пакетов, аналитического моделирования, методов эмуляции и виртуализации сетевых процессов, моделей и методов использования зафиксированных записей трафика, генерации трафика на основе моделей и др.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Д.В. Комашинский; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Комашинский Д.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАНА.В. Шоров; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.Шоров А.В.

9.4. Название публикации
Технология детектирования вредоносного программного обеспечения на основе методов Data Mining

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVIII Общероссийской научно-технической конференции. 29 июня - 2 июля 2009 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
122-123

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа, предлагаемая к рассмотрению, представляет один из способов построения технологии, ориентированной на обнаружение вредоносного программного обеспечения, находящегося в активных фазах своего жизненного цикла (распространение / выполнение атакованным хостом). Рассмотрены вопросы формирования пространства аттрибутов, присущих вредоносным и безопасным приложениям, на которых производится обучение и валидация классификаторов семейств Bayes, Decision Tree, Rule Induction.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Шоров; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Шоров А.В.

9.3.1. Другие авторы
А.М. Коновалов; 2; Россия; СПИИРАНИ.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Коновалов А.М.Котенко И.В.

9.4. Название публикации
Исследовательское моделирование бот-сетей и механизмов защиты от них

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVIII Общероссийской научно-технической конференции. 29 июня - 2 июля 2009 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
132

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В работе исследуется механизм защиты от инфраструктурных атак бот-сетей на основе подхода, называемого "нервной системой сети". Данный подход предполагает создание интеллектуальной системы защиты, как распределенного механизма сбора и обработки информации, который координирует действия различных сетевых устройств, идентифицирует атаки и принимает меры для их отражения. Структура системы строится по аналогии со структурой нервной системы человека. В каждой подсети выделяется специальный компонент, который, с точки зрения биологического подхода, играет роль "сомы" в нейроне (сома является центральной частью нейрона).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.А. Чечулин; 1; Россия; СПИИРАН

9.2.2. Первый автор (для издания библиографических сборников)
Чечулин А.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; СПИИРАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Обнаружение и противодействие сетевым атакам на основе комбинированных механизмов анализа трафика

9.5. Язык публикации
русский

9.6.1. Полное название издания
Методы и технические средства обеспечения безопасности информации. Материалы XVIII Общероссийской научно-технической конференции. 29 июня - 2 июля 2009 года

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
69

9.12.1. Полное название издательства
Издательство Политехнического университета

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Существующие сетевые атаки можно разделить на четыре основных класса: сбор информации, использующий анализ результата обработки пакетов; атаки, основанные на ошибках в обработке пакетов; сканирование хостов и сетей, базирующееся на использовании ошибок в обработке сессий; сканирование, основанное на корректном установлении соединений. Для каждого класса атак в докладе предлагается разработать свои механизмы защиты (методы фильтрации и нормализации отдельных пакетов, методы анализа сессий, методы анализа сетевого взаимодействия). Также в докладе предлагается реализовать подход к многоуровневому комбинированию алгоритмов в виде системы базовых классификаторов, обрабатывающих данные о трафике, и мета-классификатора, осуществляющего выбор весовых коэффициентов для каждого алгоритма, что позволяет объединить достоинства отдельных методов и уменьшить их недостатки.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
Р.М. Юсупов; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Юсупов Р.М.

9.4. Название публикации
Актуальные проблемы и решения в области защиты компьютерных сетей и систем

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
55-56

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе характеризуются текущее состояние в области безопасности компьютерных и телекоммуникационных технологий, рассматриваются актуальные проблемы в области защиты компьютерных сетей и систем, а также их отдельные решения. Представляется ряд проблем в области защиты компьютерных сетей и систем, а также направления развития технологий защиты информации. Дается описание ряда предложенных решений по защите компьютерных сетей и систем: моделирование кибер-противоборства в сети Интернет с целью исследования атак и перспективных методов защиты; разработка информационно-безопасных распределенных компьютерных систем, основывающихся на механизмах спецификации, верификации, реализации и мониторинга выполнения политики безопасности; анализ защищенности компьютерных систем; защита от эпидемий сетевых червей; создание безопасного кода и противодействия несанкционированному использованию и изменению программного обеспечения.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Тишков; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Тишков А.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Система защиты компьютерной сети, основанная на политике безопасности

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
122-123

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе обсуждается предлагаемый авторами подход к защите компьютерных сетей, основанный на политике безопасности. В соответствии с данным подходом предполагается непрерывное сопровождение политики безопасности в течение всего жизненного цикла существования компьютерной сети: создание политики, ее верификация, анализ защищенности, трансляция на языки сетевых устройств и распространение по сети, а также мониторинг исполнения политики и ее адаптация в соответствии с условиями обстановки.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Модель защиты программ от несанкционированных изменений на основе механизма удаленного доверия

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
81

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа посвящена разработке и анализу модели защиты программного обеспечения на основе механизма удаленного доверия. Цель данного подхода – обнаружение несанкционированных изменений клиентской программы, функционирующей в потенциально враждебном окружении. Рассматриваются атаки, которые могут быть выполнены в рамках данной модели с целью компрометации защищаемой программы. Представлены также дополнительные улучшения, которые могут использоваться для повышения степени устойчивости программы к атакам.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.В. Воронцов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Воронцов В.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Модели обнаружения и сдерживания сетевых червей на основе проактивного подхода

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
47-48

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе рассматривается предлагаемый авторами проактивный подход к защите от сетевых червей, базирующийся на использовании механизмов обнаружения и ограничения интенсивности соединений сетевых червей. Рассматриваются основные аспекты предлагаемого подхода к обнаружению и сдерживанию эпидемий сетевых червей, методика его исследования, а также программный прототип для имитационного моделирования механизмов обнаружения и сдерживания сетевых червей. Проактивный подход к защите от сетевых червей базируется на комбинировании различных механизмов обнаружения и сдерживания сетевых червей и автоматической настройке основных параметров механизмов обнаружения и сдерживания в соответствии с текущей сетевой конфигурацией и сетевым трафиком.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.А. Чечулин; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Чечулин А.А.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Механизмы защиты от сетевых червей на основе метода порогового случайного прохождения

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
70

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В работе представлены результаты анализа механизмов защиты от сетевых червей, базирующихся на методе "порогового случайного прохождения" (Threshold Random Walk, TRW). Для исследования использовался разработанный комплекс моделирования механизмов защиты от сетевых червей. Исследовано два базовых механизма защиты от сетевых червей, основанных на методе "порогового случайного прохождения": метод "порогового случайного прохождения" (Threshold Random Walk) и метод упрощенного "порогового случайного прохождения" ("Simplified TRW").

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.В. Воронцов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Воронцов В.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Механизм обнаружения и ограничения распространения сетевых червей на основе кредитов доверия

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
46-47

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе рассматривается один из механизмов обнаружения и ограничения распространения сетевых червей на основе кредитов доверия, реализованный в предлагаемом программном комплексе для имитационного моделирования механизмов защиты от сетевых эпидемий. Рассматриваемый механизм базируется на учете статистических данных о неудачных сетевых соединениях.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Реализация механизма замещения мобильного модуля на основе парадигмы аспектно-ориентированного программирования

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
49-50

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Одним из элементов предлагаемой модели защиты программного обеспечения от несанкционированных изменений и вмешательств является механизм замещения мобильного модуля. В модели защиты мобильный модуль представляет собой программный компонент, который загружается во время выполнения в клиентскую программу, и предназначен для осуществления проверок состояния программы. Для построения и функционирования мобильного кода в работе предлагается использовать концепцию аспектно-ориентированного программирования (АОП), в соответствии с которой различные функциональности системы программируются отдельно в наиболее естественном для них виде, а затем встраиваются в целевой код. АОП предоставляет возможность проводить динамические изменения программы посредством внедрения небольших фрагментов кода – аспектов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Е.В. Сидельникова; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Сидельникова Е.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Верификация правил фильтрации с помощью исчисления событий и абдуктивного вывода

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
95

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Одной из актуальных задач защиты информации в компьютерных сетях является проверка правильности (верификация) правил фильтрации. В докладе рассматривается задача верификации правил фильтрации межсетевого экрана, основанная на исчислении событий и абдуктивном выводе. Предлагается классификация аномалий в таблице доступа межсетевого экрана и соответствующая классификация механизмов разрешения аномалий. На основе данных классификаций определяется архитектура компонента верификации. Рассматриваются стратегии разрешения аномалий в правилах фильтрации, их классификация, особенности применения стратегий разрешения к различным типам аномалий, результат их применения в зависимости от типа аномалии, а также вида и положения правил в таблице доступа межсетевого экрана.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
О.В. Черватюк; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Черватюк О.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Верификация правил фильтрации политики безопасности методом проверки на модели

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
69-70

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе рассматривается задача верификации правил фильтрации политики безопасности с применением метода проверки на модели. Сущность этого метода заключается в переборе всех состояний верифицируемой системы. При этом моделируется передача сетевого трафика и работа межсетевого экрана для ограниченного набора сетевых пакетов. Набор пакетов формируется так, чтобы задействовать все правила и выявить определенные в виде формальных утверждений аномалии.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.А. Чечулин; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Чечулин А.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Исследование механизмов обнаружения и сдерживания сетевых червей, базирующихся на методике "Virus Throttling"

9.5. Язык публикации
русский

9.6.1. Полное название издания
V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2007

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
99-100

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В работе на основе проведения имитационных экспериментов на разработанном программном средстве моделирования проанализировано несколько механизмов защиты от сетевых червей, базирующихся на методике "Virus throttling": "virus throttling" для реализации на тестовом стенде; "virus throttling" для реализации на свитче; "virus throttling" для реализации на свитче на основе метода CUSUM. Установлены достоинства и недостатки этих механизмов, а также возможные их улучшения.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы
Р.М. Юсупов; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Юсупов Р.М.

9.4. Название публикации
Информационные технологии для борьбы с терроризмом

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
39-40

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе дается всеобъемлющий анализ информационных технологий (ИТ) противодействия терроризму. В простейшем случае эти технологии могут быть подразделены на технологии сбора и анализа данных. Технологии сбора данных, в основном, представляются технологиями реализации различных видов сенсорных устройств и сетей, а также слияния информации из множества различных источников. К ключевым технологиям анализа данных можно отнести технологии взаимодействия лиц принимающих решения, выбора и обоснования решений, анализа текстов, обработки естественного языка, распознавания и анализа образов, прогнозирующего (упреждающего) моделирования возможных событий. В докладе анализируются основные этапы борьбы с террористическими проявлениями и связь этих этапов с базовыми ИТ. Ставится проблема расширения фундаментальных и прикладных исследований в области создания или совершенствования ИТ в интересах борьбы с терроризмом.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Шоров; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Шоров А.В.

9.3.1. Другие авторы
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.3.2. Другие авторы (для издания библиографических сборников)
Котенко И.В.

9.4. Название публикации
Защита компьютерной сети от инфраструктурных атак на основе реализации "нервной системы сети"

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
118-119

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Текущее положение в области безопасности компьютерных сетей (быстрый рост зловредного программного обеспечения, появление новых сетевых атак и др.) обуславливает необходимость создания более устойчивой и интеллектуальной сетевой инфраструктуры защиты. Такая инфраструктура должна быть способна осуществлять автоматическое отслеживание развития атак, производить анализ сетевого трафика и осуществлять генерацию новых сигнатур поведения зловредного кода и правил политики безопасности. В работе рассматриваются механизмы защиты компьютерных сетей от инфраструктурных атак на основе применения подхода к защите, реализующего данные свойства и называемого "нервной системой сети".

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.С. Богданов; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Богданов В.С.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Оптимизация тестирования политики безопасности компьютерных сетей

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
93

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа посвящена задаче тестирования политики безопасности компьютерных сетей, которая заключается в определении правильности функционирования средств защиты и корректном выполнении ими специфицированной политики безопасности.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Разработка и анализ протокола для защиты программ от злонамеренных изменений

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
98-99

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Представляемая работа посвящена разработке и анализу коммуникационного протокола (entrusting-протокола), предназначенного для обеспечения безопасной передачи сообщений в рамках модели защиты программ на основе механизма «удаленного доверия». Данный механизм предполагает использование доверенного сервера (trusted server), который контролирует процесс выполнения функционирующей удаленно клиентской программы: во время работы сервер постоянно получает информацию о текущем состоянии программы, производит ее анализ, после чего принимает решение о том, были ли осуществлены вмешательства в ее работу. Механизм, также, реализует принцип замещения, в соответствии с которым периодически доверенный сервер отправляет клиенту некоторый программный код, который должен заменить собой определенные части исполняемого кода программы.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Д.В. Комашинский; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Комашинский Д.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Проактивная технология обнаружения вредоносного программного обеспечения на базе методов интеллектуального анализа данных (Data Mining)

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
101

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В последнее время наблюдается усиление составляющих скрытности и быстроты выполнения вредоносных программ на атакуемых хостах при минимизации их явной деструктивной функциональности, что вызвано массовым переходом криминального IT-сообщества на деятельность, приносящую материальную выгоду. К сожалению, проблема детектирования всего многообразия вариантов подобных атак до сих пор остается актуальной в силу ограниченности методов статического анализа входящего на хост программного кода и постоянного увеличения количества потенциально уязвимых сред и приложений. Необходимость подобных решений, получивших название проактивных, продиктована наблюдаемым изменением фокуса проблемы сохранения целостности и конфиденциальности информации пользователей, организаций и государственных органов. Предлагаемая к рассмотрению работа представляет один из вариантов построения технологии, направленной на обнаружение вредоносного программного обеспечения, находящегося в завершающей фазе своего жизненного цикла (исполнение приложения атакованным хостом).

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.М. Коновалов; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Коновалов А.М.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Моделирование сетевого трафика в задачах защиты от инфраструктурных сетевых угроз

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
101-102

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа посвящена имитационному моделированию реалистичного сетевого трафика в задачах защиты от крупномасштабных распределённых сетевых угроз на примере атак вида «распределённый отказ в обслуживании», а так же на примере протекания эпидемии заражения сетевым червём крупного сетевого сегмента. Данная работа включает исследование различных сценариев реализации инфраструктурных сетевых атак, выявление характерных особенностей их протекания и формирование набора параметров сетевого трафика, в наибольшей степени определяющих атакующий процесс. С использованием полученных моделей проводится моделирование сетевого трафика с применением различных моделей сдерживания распространения атакующего процесса в сетевой среде. На основе результатов моделирования осуществляется выработка рекомендаций по выбору наиболее подходящих способов защиты.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Д.И. Котенко; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко Д.И.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Построение графа атак для оценки защищенности компьютерной сети

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
102-103

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Основной целью данной работы является исследование механизмов анализа защищенности, разработка архитектуры, моделей и методики функционирования системы анализа защищенности, основанной на оценке возможных действий нарушителя по реализации различных угроз безопасности, и построение графа этих действий. Важной особенностью предлагаемого подхода является возможность учета временного (темпорального) аспекта действий злоумышленников. Это позволяет рассматривать атаки как протяженную во времени деятельность и специфицировать возможные взаимозависимости между различными шагами реализации атаки и совместные действия групп злоумышленников. Такой подход позволяет учитывать большинство классов сетевых атак, в том числе атаки на отказ в обслуживании и распределенный отказ в обслуживании.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
О.В. Полубелова; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Полубелова О.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Верификация правил фильтрации политики безопасности, содержащих временные параметры, методом проверки на модели

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
110-111

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе предлагается решение задачи верификации правил фильтрации, содержащих временные параметры, с применением метода проверки на модели. Данный метод основан на полном переборе всех состояний верифицируемой модели. Его применение позволяет отслеживать динамику изменений состояния системы во времени. Предложенное решение реализовано с использованием программного средства проверки на модели SPIN.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
С.А. Резник; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Резник С.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Комплексный подход к верификации протоколов безопасности на примере протокола RE-TRUST

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
111

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Представляемая работа посвящена разработке комплексного подхода к верификации протоколов безопасности, представляющего собой комбинированное применение различных средств верификации, каждое из которых в отдельности реализует подход, основанный на том или ином формализме. На примере практической задачи по анализу протокола удаленной аутентификации RE-TRUST показывается невозможность полноценной верификации протокола безопасности, основываясь только на одном из существующих средств. Для демонстрации комплексного подхода к верификации протоколов безопасности протокол RE-TRUST проверяется с помощью комбинации средств AVISPA и Isabelle.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Е.В. Сидельникова; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Сидельникова Е.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Абдуктивный конфигуратор правил фильтрации межсетевого экрана

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
112

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Одной из актуальных задач защиты информации в компьютерных сетях является задача построения непротиворечивого множества правил фильтрации межсетевых экранов. Для решения данной задачи в работе представлен подход к моделированию поведения межсетевого экрана (МЭ) при помощи исчисления событий (ИС), а также методы анализа и конфигурации правил МЭ с использованием абдуктивного вывода. ИС рассматривается как аппарат для спецификации действий МЭ, которые задаются предметно-зависимой аксиоматикой ИС.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.А. Чечулин; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Чечулин А.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Защита от сетевых атак методами нормализации протоколов транспортного и сетевого уровня стека TCP/IP

9.5. Язык публикации
русский

9.6.1. Полное название издания
XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
115-116

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Одним из недостатков систем обнаружения вторжения (СОВ) является риск возникновения ситуации, при которой злоумышленник, используя неоднозначности в потоке данных, избегает обнаружения. Эта проблема возникает из-за разницы в обработке протоколов в СОВ и в конечной (атакуемой) системе. В данной работе рассмотрен один из подходов к решению данной проблемы – использование нормализатора сетевого трафика.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Е.В. Сидельникова; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Сидельникова Е.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Верификация политик фильтрации с помощью исчисления событий и абдуктивного вывода

9.5. Язык публикации
русский

9.6.1. Полное название издания
Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции

9.6.2. ISSN издания

9.7. Вид публикации
статья в сборнике

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2008

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
133-136

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В этой статье был описан подход, использующий аксиоматику исчисления событий и абдуктивный вывод для поиска аномалий между правилами межсетевого экрана (МЭ). Основная идея разработки заключается в том, чтобы построить адекватную модель сети, включающую описание политики и описание сети, а также модель поведения системы. Добавляется определение аномалий и модель проверяется на наличие возможных аномалий. Описанный модуль верификации был реализован на языке Java и использует библиотеку CIFF, работающую на базе SICStus Prolog. Выполненные эксперименты показали, что предагаемый подход является применимым к примерам реальных списков ограничения доступа МЭ.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы
9

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
И.В. Котенко; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Котенко И.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Построение и поддержка функционирования интеллектуальных систем защиты информации

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
112

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе рассматривается целостная концепция построения и поддержки функционирования интеллектуальных систем защиты информации и несколько групп подзадач разработки отдельных компонентов такой системы, необходимых для реализации эффективного противодействия современным сетевым атакам и вредоносному ПО: гибридном многоагентном моделировании компьютерного противоборства, реализации адаптивного управления верифицированными политиками безопасности, анализе защищенности ресурсов компьютерных сетей и систем, а также проактивном мониторинге состояния и поведения защищаемых ресурсов на базе интеграции различных методов интеллектуального анализа данных.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Масштабируемость и безопасность механизма защиты на основе принципа удаленного доверия

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
98

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа посвящена разработке методики, делающей возможным достижение компромисса между уровнем предоставляемой защиты (безопасностью) и масштабируемостью механизма. Такой компромисс достигается за счет выбора некоторой комбинации атомарных методов защиты, характеризуемых определенными значениями производительности и безопасности, при заданных ограничениях на потребляемые ресурсы сервера. Помимо этого, каждый метод защиты может иметь свои специфические параметры, также влияющие на характер его работы. В работе также представлены возможные политики безопасности, определяющие поведение доверенного сервера в случае нехватки того или иного ресурса сервера.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
В.А. Десницкий; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Десницкий В.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Конфигурирование механизма защиты при помощи политик безопасности

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
97-98

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа посвящена исследованию механизма защиты программного обеспечения на основе принципа удаленного доверия. В соответствии с данным принципом, контроль над выполнением клиентской программы делегируется специализированной удаленной сущности – доверенному серверу. В работе рассматривается набор отдельных (атомарных) методов защиты, таких как проверка контрольных сумм, метод проверки инвариантов, методы Barrier Slicing, Control Flow Checking, Crypto Guards, Orthogonal Replacement и другие, которые различаются как по уровню предоставляемой защиты, так и принципу защиты.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Ю.В. Зозуля; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Зозуля Ю.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Определение категории Веб-сайта для решения задачи родительского контроля

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
53-54

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа посвящена разработке общего подхода и реализующего его программного комплекса, решающих актуальную в настоящее время задачу категорирования веб-сайтов для программ родительского контроля. Задача родительского контроля сводится к обеспечению защиты ребенка от вредоносной информации при его работе в Интернет, в частности, решению вопроса о запрете доступа ребенка к определенным веб-сайтам, которые содержат неприемлемую информацию. В работе предлагается подход, в которой родитель может определить список категорий, по которым будет оцениваться каждый посещаемый ребенком сайт. Примерами таких категорий могут послужить такие, как: насилие, наркотики, эротическое содержание, вредоносное наполнение сайта и другие. В соответствии с выбранными родителем категориями странице ставится оценка с учетом информации из разных источников. Оценка сайта заносится в базу данных, а затем используется и обновляется при последующем доступе к этому или другим сайтам.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Д.В. Комашинский; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Комашинский Д.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Построение модели статического детектирования вредоносного программного обеспечения на базе методов Data Mining

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
56-57

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Представляемая работа посвящена проблеме выявления вредоносного программного обеспечения (malware) на начальных фазах его жизненного цикла. Результаты работы рассматриваются в качестве базиса, необходимого для формирования общей объединительной модели детектирования malware, использующей сильные стороны существующих процедур извлечения, выделения, конструирования групп признаков и обучения классификаторов, обеспечивающих точное выявление отдельных структурных и функциональных аспектов исследуемых потенциально вредоносных файловых объектов.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.М. Коновалов; 2; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Коновалов А.М.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Моделирование ботнетов а основе множества взаимодействующих интеллектуальных агентов

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
58

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа посвящена моделированию крупномасштабных ботнетов, на основе рассмотрения компонент ботнета в виде обособленных интеллектуальных агентов. Анализируется протекание типичного жизненного цикла ботнета, а так же реализации различных сценариев инфраструктурных атак, проводимых злоумышленниками с их помощью. Проводится исследование стадии формирования ботнета и стадии реализации DDoS-атаки. Основными объектами исследования являются: архитектура ботнета, способы управления ботнетом, механизмы вовлечения новых участников в бот-сеть, типы реализуемых атак посредством ботнета. Работа также включает исследование современных методов обнаружения бот-сетей и методов борьбы с ними, анализ их эффективности и выработку рекомендаций по построению эффективных систем защиты от данного типа угроз.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
С.А. Резник; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Резник С.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Комбинированные подходы к верификации протоколов безопасности

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
122-123

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа посвящена анализу существующих методов верификации протоколов безопасности и разработке комбинированных подходов. Рассматриваются различные методы верификации, анализируются их сильные и слабые стороны. Данный анализ производится на примерах как существующих протоколов безопасности, так и entrusting-протокола, разработанного в рамках проекта RE-TRUST. Предлагаются различные варианты комбинированного использования подходов к верификации протоколов безопасности. Все варианты имеют целью совместить удобство AVISPA-модели с гибкостью, предлагаемой Isabelle. Общей идеей, по-разному воплощаемой в каждом из вариантов, является использование AVISPA-модели в той мере, в какой это возможно, и переход к верификации с помощью Isabelle только там, где без этого не обойтись.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
Е.В. Сидельникова; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Сидельникова Е.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Верификация правил фильтрации политики безопасности компьютерной сети на основе исчисления событий и абдуктивного вывода

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
139-140

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Работа посвящена разработке автоматизированной методики верификации правил фильтрации политики безопасности компьютерной сети на основе исчисления событий и абдуктивного вывода. В работе рассмотрено моделирование поведения межсетевого экрана (МЭ) при помощи исчисления событий. Приведена предметно-независимая аксиоматика исчисления событий, а также модификация аксиоматики для решения рассматриваемой задачи. Рассмотрена предметно-зависимая аксиоматика исчисления событий, используемая для формализации правил МЭ, а также пример работы конкретного МЭ в терминах исчисления событий. Разработаны алгоритмы поиска и разрешения аномалий в правилах фильтрации политики безопасности компьютерной сети при помощи абдуктивного вывода.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.А. Чечулин; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Чечулин А.А.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Обнаружение и противодействие сетевым атакам на основе комбинированных механизмов анализа трафика

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
143-144

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
В докладе предлагается подход к многоуровневому комбинированию алгоритмов в виде системы базовых классификаторов, обрабатывающих данные о трафике, и мета-классификатора, осуществляющего выбор весовых коэффициентов для каждого алгоритма, что позволяет объединить достоинства отдельных методов и уменьшить их недостатки.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА (ДЛЯ ИТОГОВЫХ ОТЧЕТОВ)

9.1. Номер проекта
07-01-00547

9.2.1. Первый автор
А.В. Шоров; 1; Россия; Санкт-Петербургский институт информатики и автоматизации РАН

9.2.2. Первый автор (для издания библиографических сборников)
Шоров А.В.

9.3.1. Другие авторы

9.3.2. Другие авторы (для издания библиографических сборников)

9.4. Название публикации
Анализ биологических подходов для защиты компьютерных сетей от инфраструктурных атак

9.5. Язык публикации
русский

9.6.1. Полное название издания
VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции

9.6.2. ISSN издания

9.7. Вид публикации
тезисы доклада

9.8. Завершенность публикации
опубликовано

9.9. Год публикации
2009

9.10.1 Том издания

9.10.2 Номер издания

9.11. Страницы
145

9.12.1. Полное название издательства
Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления (СПОИСУ)

9.12.2. Город, где расположено издательство
Санкт-Петербург

9.13. Краткий реферат публикации
Для построения новых средств защиты предлагается метафора, основанная на применении биологических подходов. Рассматриваются несколько возможных механизмов защиты от инфраструктурных атак на основе биологических подходов: механизмов, созданных по аналогии с живыми клетками; механизмов, базирующихся на подходе «нервная система сети»; механизмов, основанных на иммунных системах.

9.14. Список литературы (библиография), использованной при подготовке данной научной статьи

9.15. Общее число ссылок в списке использованной литературы

Подпись руководителя проекта

Форма 511. ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ЗАВЕРШЕННОГО ПРОЕКТА РФФИ В ПРИКЛАДНОЙ ОБЛАСТИ

11.1. Номер проекта
07-01-00547

11.2.1. Приоритетное направление развития науки, технологий и техники РФ, в котором, по мнению исполнителей, могут быть использованы результаты завершенного проекта
безопасность и противодействие терроризму

11.2.2. Критическая технология РФ, в которой, по мнению исполнителей, могут быть использованы результаты завершенного проекта
технологии обработки, хранения, передачи и защиты информации

11.3. Предлагаемое авторами название работы в прикладной области
Компоненты интеллектуальных адаптивных систем защиты информации, основывающиеся на моделировании поведения систем защиты, реализации верифицированных политик безопасности, оценке защищенности и проактивном мониторинге

11.4. Ожидаемые результаты работы в прикладной области
Полученные при выполнении проекта результаты являются необходимым базисом для разработки целого класса комплексных адаптивных систем защиты информации (СЗИ) нового поколения и их отдельных компонентов. По сравнению с существующими, такие СЗИ представляют собой взаимоувязанные, многоэшелонированные и непрерывно контролируемые системы защиты используемых информационных, программных и аппаратных ресурсов, способные оперативно реагировать на удаленные и локальные компьютерные атаки и несанкционированные действия (НСД), накапливать знания о способах противодействия, обнаружения и реагирования на атаки и НСД и использовать их для усиления защиты. В соответствии с предлагаемым в проекте подходом для поддержки функционирования таких СЗИ реализуется единая унифицированная подсистема (среда), выполняющая комплекс задач по поддержке всего жизненного цикла СЗИ, включая спецификацию общей политики безопасности и архитектуры (или конфигурации) защищаемой системы, трансформацию политики безопасности с целью ее уточнения (детализации) с учетом описания защищаемой системы, верификацию политики безопасности, определение уровня безопасности и анализ рисков, моделирование поведения системы защиты в различных условиях функционирования, изменение политики в соответствии с требуемым уровнем безопасности и возможностями по использованию различных ресурсов и выделению финансовых средств и на защиту информации, реализации политики безопасности в системе, проактивный мониторинг выполнения политики безопасности, адаптацию поведения в соответствии с условиями функционирования.

11.5. Планируемая продолжительность работы
до 1 года

11.6. Предполагаемые авторами пути дальнейшего продвижения проекта
участие в лотах ФЦП Минобрнауки

11.7. Информация, связанная с интеллектуальной собственностью
патентование потребуется в ходе разработки

11.8. Реквизиты охранных документов (номер патента, исходящий номер заявки на патент)

Подпись руководителя проекта