НОМЕР ПРОЕКТА **10-01-00826**		УЧЕТНАЯ КАРТОЧКА
НАЗВАНИЕ ПРОЕКТА **Математические модели и методы комплексной защиты от сетевых атак и вредоносного программного обеспечения в компьютерных сетях и системах, основывающиеся на гибридном многоагентном моделировании компьютерного противоборства, верифицированных адаптивных политиках безопасности и проактивном мониторинге на базе интеллектуального анализа данных**		
ОБЛАСТЬ ЗНАНИЯ **01 - математика, информатика, механика**		КОД(Ы) КЛАССИФИКАТОРА **01-201 01-202 01-217**
ВИД КОНКУРСА **а - 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**		
ОБЪЕМ СРЕДСТВ, ФАКТИЧЕСКИ ПОЛУЧЕННЫХ ЗА 2010 г. **345000 руб.**	ОБЪЕМ ФИНАНСИРОВАНИЯ, ЗАПРАШИВАЕМЫЙ НА СЛЕДУЮЩИЙ ГОД **600000 руб.**	
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		
Десницкий Василий Алексеевич		
Чечулин Андрей Алексеевич		
Комашинский Дмитрий Владимирович		
Шоров Андрей Владимирович		
Дойникова Елена Владимировна		
Коновалов Алексей Михайлович		
Котенко Дмитрий Игоревич		
ПОДПИСЬ РУКОВОДИТЕЛЯ ПРОЕКТА		ДАТА ПОДАЧИ ОТЧЕТА **07.12.2010**

ОТЧЕТ ЗА 2010 ГОД ПО ПРОЕКТУ РФФИ 10-01-00826-а

Статус отчета: подписан

Дата последнего изменения: 07.12.2010

Отчёт создал: Котенко Игорь Витальевич

Отчет распечатан: 07.12.2010

Форма 501. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1. Номер проекта
10-01-00826

1.2. Руководитель проекта
Котенко Игорь Витальевич

1.3. Название проекта
Математические модели и методы комплексной защиты от сетевых атак и вредоносного программного обеспечения в компьютерных сетях и системах, основывающиеся на гибридном многоагентном моделировании компьютерного противоборства, верифицированных адаптивных политиках безопасности и проактивном мониторинге на базе интеллектуального анализа данных

1.4. Вид конкурса
а - Инициативные проекты

1.5. Год представления отчета
2011

1.6. Вид отчета
этап 2010 года

1.7. Аннотация
Проведен анализ состояния исследований в области моделирования компьютерного противоборства, обнаружения и реагирования против сетевых атак и вредоносного программного обеспечения, а также оценки защищенности ресурсов компьютерных сетей и систем. Осуществлена разработка формальной постановки задачи исследования, основных требований и формальных моделей компонентов гибридного моделирования компьютерного противоборства и механизмов защиты, реализующих обнаружение и реагирование против сетевых атак и вредоносного программного обеспечения, а также анализ защищенности ресурсов компьютерных сетей и систем. Исследованы вопросы реализации компонентов детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных. Выполнена разработка обобщенной методики построения элементов принятия решения о степени вредоносности и зашумленности (искаженности) анализируемых объектов. Разработаны модели улучшения прогностической функции принятия решения, основанных на методах интеллектуального анализа данных, и модели комбинирования отдельных элементов принятия решения за счет формирования иерархических (пошаговых) схем и схем голосования. Кроме того, разработаны отдельные модели безопасности встроенных систем. Выполнена первоначальная экспериментальная оценка полученных результатов.

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"

Форма 502. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ НА АНГЛИЙСКОМ ЯЗЫКЕ

2.1. Номер проекта
10-01-00826

2.2. Руководитель проекта
Kotenko Igor Vitalevich

2.3. Название проекта
Mathematical models and methods of integrated protection against network attacks and malware in computer networks and systems based on hybrid multi-agent modeling and simulation of computer counteraction, verified adaptive security policies and proactive monitoring by data mining

2.4. Год представления отчета
2011

2.5. Вид отчета
этап 2010 года

2.6. Аннотация
The analysis of state-of-the-art in the field of computer counteraction simulation, detection and reaction against network attacks and malware as well as the security evaluation of computer networks and systems was carried out. We developed the formal statement of the research problem, the basic requirements and the formal models of the components for the hybrid simulation of computer counteraction and the protection mechanisms realizing the detection and reaction against network attacks and malware, and also the security evaluation of computer networks and systems. We investigated the issues of implementing the malware detection components on the basis of data mining methods. The generalized technique for constructing the elements of decision-making on a degree of injuriousness and noisiness of analyzed objects was suggested. We developed the models of improving the prognostic functions of decision-making, based on data mining, and the models of combining the particular elements of decision-making by generating the hierarchical (step-by-step) and voting schemes. Besides, particular models of embedded system security were developed. The initial experimental evaluation of these results was carried out.

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

Форма 503. РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер проекта
10-01-00826

3.2. Название проекта
Математические модели и методы комплексной защиты от сетевых атак и вредоносного программного обеспечения в компьютерных сетях и системах, основывающиеся на гибридном многоагентном моделировании компьютерного противоборства, верифицированных адаптивных политиках безопасности и проактивном мониторинге на базе интеллектуального анализа данных

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 2010 год
Основными целями проекта на 2010 год являлись:
(1) анализ состояния исследований в области моделирования компьютерного противоборства, обнаружения и реагирования против сетевых атак и вредоносного программного обеспечения, а также оценки защищенности ресурсов компьютерных сетей и систем;
(2) разработка формальной постановки задачи исследования, основных требований и формальных моделей компонентов гибридного моделирования компьютерного противоборства и механизмов защиты, реализующих обнаружение и реагирование против сетевых атак и вредоносного программного обеспечения, а также анализ защищенности ресурсов компьютерных сетей и систем;
(3) исследование вопросов реализации компонентов детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных;
(4) разработка обобщенной методики построения элементов общей схемы принятия решения о степени вредоносности и зашумленности (искаженности) анализируемых объектов;
(5) разработка моделей улучшения прогностической функции средств принятия решения, основанных на методах интеллектуального анализа данных, и моделей комбинирования отдельных элементов принятия решения за счет формирования иерархических (пошаговых) схем и схем голосования;
(6) первоначальная экспериментальная оценка полученных результатов.

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

3.6. Полученные за отчетный период важнейшие результаты
Важнейшие результаты, полученные за отчетный период, таковы:

1. Проведен детальный анализ состояния исследований в области моделирования компьютерного противоборства, обнаружения и реагирования против сетевых атак и вредоносного программного обеспечения, а также оценки защищенности ресурсов компьютерных сетей и систем.
Основные работы, которые являются базой для моделирования компьютерного противоборства, сосредоточены в области агентно-ориентированного моделирования вида имитационного моделирования, суть которого заключается в представлении сущностей предметной области в виде отдельных автономных интеллектуальных агентов. Множество интеллектуальных агентов, имея простые собственные функции, в процессе функционирования могут включаться (или самоорганизовываться) в системы с существенно более сложным поведением. Данная область знаний представлена широким спектром работ различных исследователей, среди которых следует выделить теоретические подходы теорию разделяемых планов, теорию совместных намерений, гибридный подход, а так же ряд программных реализаций сред многоагентного моделирования.
Для оптимизации функционирования команд агентов были предложены различные комбинации следующих методов и моделей: (1) традиционные BDI-модели (BDI belief-desire-intention), определяемые схемами функционирования агентов, обуславливаемыми зависимостями предметной области; (2) методы распределенной оптимизации на основе ограничений (DCOP distributed constraint optimization), использующие локальные взаимодействия при поиске локального или глобального оптимума; (3) методы распределенного принятия решений на основе частично-наблюдаемых Марковских сетей (distributed POMDPs), позволяющие реализовать координацию командной работы при наличии неопределенности в действиях и наблюдениях; (4) теоретико-игровые модели и модели аукциона, фокусирующиеся на координации различных команд агентов, использующих "рыночные (аукционные)" механизмы принятия решений.
За основу предлагаемого подхода к обнаружению сетевых атак было принято использование нескольких семейств механизмов, в том числе базирующихся на следующих методиках: методике "дросселирования/регулирования вирусов" ("Virus Throttling") и ее модификации; методиках, основанных на анализе неудачных соединений (Failed Connection, FC); методиках, использующих метод "порогового случайного прохождения" (Threshold Random Walk, TRW); методиках ограничения интенсивности соединений на основе кредитов доверия (Credit Based Rate Limiting, CB).
Подходы, применяемые для обнаружения вредоносного программного обеспечебния основываются на реализации одного из конкретных методов анализа приложений: статического, динамического или гибридного. Метод анализа, применяемый в том или ином конкретном подходе, определяется тем, каким образом производится сбор информации, необходимой для принятия решения о вредоносности приложения. В общем случае, статический анализ использует синтаксические или структурные свойства исследуемого объекта. Методы динамического анализа ориентированы на обнаружение фактов, свидетельствующих о наличии вредоносной функциональности приложения при его выполнении или после выполнения. Гибридные методы объединяют преимущества двух вышеупомянутых типов анализа, обеспечивая применение в процессе поиска элементов вредоносности как статической, так и поведенческой информации.

2. Предложена формальная постановка задачи исследования, основные требования и формальные модели компонентов гибридного моделирования компьютерного противоборства и механизмов защиты, реализующих обнаружение и реагирование против сетевых атак и вредоносного программного обеспечения, а также анализ защищенности ресурсов компьютерных сетей и систем.
Предлагаемый подход к моделированию заключается в интеграции моделей и методов агентно-ориентированного моделировании, использования записей трафика, генерации трафика на основе моделей систем защиты, приложений и вредоносных программ и систем, применении методов эмуляции и виртуализации сетевых процессов и имитационного моделирования на уровне сетевых пакетов. Подход базируется на использовании иерархии макро- и микро-уровневых моделей компонентов реализации атаки (эксплоитов, сетевых червей, ботов, бот-сеети в целом и др.) и механизмов защиты от них (аналитических, основанных на имитации сетевых пакетов, базирующихся на эмуляции), а также реальных сетей (имитационных стендов) небольшого размера. Предлагаемый подход и разрабатываемый инструментарий моделирования и эмуляции могут использоваться для анализа текущих и будущих сетевых атак и механизмов защиты, "проигрывания" сценариев кибератак и киберзащиты, анализа защищенности систем защиты, а также применяться для расследований инцидентов, связанных с использованием бот-сетей и сетевых атак. При моделировании сетевых процессов используются модели следующих элементов: топологии сети, каналов передачи данных, протоколов, приложений, узлов, трафика. В зависимости от целей моделирования данные модели представляются с той или иной точностью.

3. Исследованы вопросы реализации компонентов детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных, исследованы устойчивые и потенциально эффективные паттерны обработки исходных данных и применения отдельных методов классификации, кластеризации и поиска ассоциативных правил.
В частности, проведенные исследования показали, что применение позиционно-зависимых признаков, извлекаемых на этапе статического анализа исполняемых файлов, является достаточно эффективным при использовании методов интеллектуального анализа данных, относящихся к группам классификаторов, использующих генерацию правил и построение деревьев решений. Наиболее эффективным показал себя метод RandomForest, интегрирующий в себя общие принципы улучшения качества классификации за счет реализации принципов обобщения результатов работы нескольких сущностей, ответственных за принятие решения.
Была показана и обоснована необходимость учета значимости отдельных областей (регионов) анализируемых объектов и данных, находящихся в них. Данный подход не гарантирует абсолютной точности детектирования вредоносного программного обеспечения, но, в силу показанных особенностей, может быть эффективен на определенных фазах процесса принятия решения о способе дальнейшей обработки объекта и при построении средств детектирования отдельных семейств исполняемых программ. В качестве очевидного примера можно привести задачу автоматизации обнаружения и идентификации использованных средств обфускации или защиты исполняемых файлов, что позволит обеспечить четкую автоматическую процедуру генерации правил детектирования и тем самым предоставляет возможность более корректно определить путь дальнейшего анализа объекта (каким образом настроить средства динамического анализа, каким участкам исследуемого объекта следует уделить внимание в дальнейшем при подтверждении факта его обфускации и т.д.).

4. Разработана обобщенная методика построения элементов общей схемы принятия решения о степени вредоносности и зашумленности (искаженности) анализируемых объектов.
В этой связи определены особенности задач, решаемых в процессе применения средств интеллектуального анализа данных для детектирования вредоносного программного обеспечения, в том числе задач выделения списка потенциально значимых признаков, определения процедуры выявления наиболее значимых признаков, выбора метода классификации, оценки качества созданной модели детектирования, определения используемых инструментальных средств.
В рамках проектирования отдельных средств выявления зашумленных данных предлагается в общей архитектуре системы детектирования вредоносного программного обеспечения использовать отдельные элементы, служащие для выявления зашумленных данных, представляемых отдельными трактами принятия решения и, как следствие, ориентированные на отдельные группы заведомо зашумленных данных, используемых при обучении.

5. Разработаны модели улучшения прогностической функции принятия решения, основанных на методах интеллектуального анализа данных, и модели комбинирования отдельных элементов принятия решения за счет формирования иерархических (пошаговых) схем и схем голосования.
Очевидно, что традиционно узкая направленность отдельных частных подходов к детектированию вредоносного программного обеспечения позволяет произвести достаточно точную оценку их эффективности для поставленных исследователями условий. Вместе с тем, она же ограничивает применимость предлагаемых моделей детектирования вредоносного программного обеспечения на практике.
Поэтому предлагаемые модели улучшения прогностической функции принятия решения основываются на следующих элементах принятия решения: (1) использовании максимального количества объектов фокусной группы (семейства) вредоносного программного обеспечения или уточнении (последовательном ограничении) целевого семейства объектов с последующим ограничением группы фокуса используемого классификатора; (2) обобщении всей доступной информации о специфических признаках вредоносного программного обеспечения и применении дополнительных «резервных» механизмов принятия решения о вредоносности объектов, не попадающих в конкретную фокусную группу; (3) включении в процесс обучения нескольких классификаторов и использовании механизма обобщения результатов их работы, т.е. реализации комбинированных

классификаторов. Модель комбинирования отдельных элементов принятия решения основывается на так называемом «многоходовом» подходе к детектированию, основанном на последовательном уточнении значимых структурных и функциональных аспектов анализируемого объекта.
Первым необходимым шагом в процессе принятия решения является получение ответа на вопрос о том, является ли проверяемый объект защищенным каким-либо средством обфускации. Далее, в зависимости от результата предыдущего шага, объект передается последующему элементу модели, обученному именно на такой группе объектов, которая соответствует результату предыдущего шага принятия решения.

6. Разработаны отдельные модели безопасности встроенных систем.
Предлагаемая абстрактная модель встроенных систем является обобщенным представлением встроенных систем, описывает их характерные свойства, включает процедуры, процессы, компоненты и сценарии функционирования. Модель имеет важные составляющие, каждая из которых охватывает определенный аспект встроенных систем, в том числе, архитектурное представление; представление функций и стадий функционирования; представление легитимного пользователя и атакующего; представление встроенных систем в виде набора свойств безопасности, производительности и иного вида характеристик. В предложенной модели нарушителя для задачи обеспечения безопасности встроенных систем выделено четыре основных класса нарушителей: нарушители, взаимодействующие с устройством по сети; нарушители, находящиеся в непосредственной близости от устройства, но не имеющие физического доступа к нему; нарушители, имеющие физический доступ к устройству без возможности непосредственного доступа к встроенным в него электронным компонентам; нарушители, имеющие физический доступ к устройству и к встроенным в него электронным компонентам. Типы атак, доступных нарушителям, разделяются на несколько уровней по требуемым для их реализации ресурсам. В соответствии с моделью нарушителя каждому классу нарушителя соответствует различные типы угроз безопасности.

7. Проведена первоначальная экспериментальная оценка полученных результатов.
Авторами настоящей работы используется и разрабатывается многоуровневая инструментальная среда имитационного моделирования сетевых процессов для приложений в области защиты информации. Среда представляет собой программный комплекс, включающий в качестве нижнего уровня систему моделирования дискретных событий, реализованный на языке низкого уровня, а так же ряд компонентов, реализующих сущности более высокого уровня. Нижний слой обеспечивает возможность моделирования хронологически упорядоченных последовательностей событий, распространяющихся в сетевых структурах. Промежуточные слои на базе нижнего слоя реализуют сущности, относящиеся к специфике сети Интернет, в том числе основанные на дискретных событиях модели протоколов и типовых сетевых приложений. Промежуточные слои являются базисом для построения слоев более высокого уровня, таких как, например, слой абстракции уровня интеллектуальных агентов и ряда других. Все модули и компоненты системы моделирования находятся во взаимодействии с подсистемой ввода/вывода и, таким образом, посредством данной подсистемы осуществляют обмен данными с внешними источниками данных и с оператором системы. Каждый слой реализован в виде отдельной библиотеки функций с документированным интерфейсом, посредством которого обеспечивается возможность взаимодействия с данной библиотекой со стороны прочих компонент.
Для выполнения экспериментов были реализованы отдельные сценарии функционирования бот-сетей (включая сценарии распространения бот-сети, управления бот-сетью и реализации атак), сценарии сдерживания бот-сети и противодействия атакам, а так же сценарии легитимной деятельности вычислительной сети. Сценарии распространения бот-сети включают сценарии поиска новых узлов, пригодных к компрометации, их идентификации и последующей компрометации и подключения инфицированных узлов в бот-сеть. Сценарий распространения бот-сети, использованный в экспериментах, основывается на модели распространения сетевого червя посредством эксплуатации уязвимостей сетевых служб. Одним из примеров реализованных сценариев атаки бот-сети является атака вида UDP Flood, проводимая по отношению к некоторому узлу (подсети), IP-адрес которого (которой) указан в составе инструкции начала атаки. Реализовано несколько сценариев сдерживания бот-сети и противодействия атакам, направленных на защиту от атак DDoS: без кооперации; с кооперацией типа DefCOM; с кооперацией типа COSSACK и с полной кооперацией. Результаты сценариев распространения бот-сети и защиты от распространения оценивались по количеству зараженных (скомпрометированных) узлов за заданное время, а также по количеству ошибок первого и второго рода (оценки False Positive (FP) и False Negative (FN)), характеризующих обнаружение сканирующих хостов-зомби. Для оценки эффективности сценариев управления бот-сетью и противодействия управлению бот-сетью определялось количество ошибок первого и второго рода, характеризующих обнаружение хостов-зомби, входящих в бот-сеть.

3.7. Степень новизны полученных результатов

Основные научные результаты являются новыми и оригинальными, они основываются на разработках исполнителей проекта, выполненных ранее и выполняемых в настоящее время, а также базируются на современных достижениях в области защиты информации, распределенного искусственного интеллекта, моделирования и др.

3.8. Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения первого года проекта, соответствуют мировому уровню. Авторы проекта опубликовали полученные результаты в нескольких журналах, сборниках и трудах конференций, а также апробировали результаты на множестве различных российских и международных конференций, в частности, на 18-й Европейской (Euromicro) международной конференции по параллельной, распределенной и сетевой обработке информации (PDP 2010, Пиза, Италия. 17-19 февраля 2010 г.), Международной конференции по киберконфликтам (Таллинн, Эстония. 15-18 июня 2010 г.), Международной

конференции "Математические модели, методы и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2010, Санкт-Петербург, 8-10 сентября 2010 г.), Международном семинаре "Научный анализ и поддержка политик безопасности в киберпространстве" (SA&PS4CS 2010, Санкт-Петербург, 11 сентября 2010 г.), Международной конференции "Интеллектуальные распределенные вычисления" (IDC'2010) и Международной школе "Программные агенты, агентские системы и их приложения" (Танжер, Марокко, 15-23 сентября), Международном семинаре "Взаимодействие науки, технологии и безопасности: современные и будущие области приложения" (APCSS'2010, США, Гонолулу, 4-8 октября 2010 г.), Двенадцатой национальной конференции по искусственному интеллекту с международным участием (КИИ-2010, 20-24 сентября 2010 г., г. Тверь, Россия), Двенадцатой конференции "РусКрипто'2010" по криптологии, стеганографии, цифровой подписи и системам защиты информации (Звенигород, 1-4 апреля 2010 г.), XIX Общероссийской научно-технической конференции "Методы и технические средства обеспечения безопасности информации (МТСОБИ 2010)" (Санкт-Петербург, 5-10 июля 2010 г.), XII Санкт-Петербургской Международной Конференции "Региональная информатика-2010 (РИ-2010)" (Санкт-Петербург, 20-22 октября 2010 г.), Шестой международной научной конференции по проблемам безопасности и противодействия терроризму и Девятой общероссийской научной конференции "Математика и безопасность информационных технологий МаБИТ-2010" (Москва, 11-13 ноября 2010 г.), Международном семинаре "Безопасные и надежные вычисления в мобильных и облачных средах" (Дели, Неемрана, Индия, 16-17 декабря 2010 г.) и др.

3.9. Методы и подходы, использованные в ходе выполнения проекта

В качестве базиса для исследований использовались работы в следующих областях: (1) механизмы обеспечения информационной безопасности в компьютерных сетях (в том числе новые технологии обнаружения вторжений и использования ложных информационных систем); (2) методы агентно-ориентированного моделирования, генерации трафика на основе моделей, эмуляции и виртуализации сетевых процессов, имитационного моделирования на уровне сетевых пакетов; (3) объединение (слияние) данных и информации; (4) интеллектуальные агенты, включая модели командной работы агентов; (5) онтологическое представление знаний; (6) системы вывода, основанные на знаниях о выполняемых действиях и предсказании намерений и планов оппонента; (7) рефлексивные процессы, модели антагонистических процессов; (8) основанное на агентских технологиях моделирование; (9) анализ рисков; (10) элементы теории игр; (11) методы верификации сложных систем; (12) методы интеллектуального анализа данных, в том числе на базе статической и динамической информации, комбинирования классификаторов, обучения и классификации на зашумленных наборах данных и др.; (13) методы адаптации и самообучения; (14) методы теории исследования операций и оптимального управления и др.

3.10.1. Количество научных работ, опубликованных в ходе выполнения проекта

44

3.10.2. Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в 2010 г.

11

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

345000 руб.

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/ru/staff/kotenko
http://comsec.spb.ru/en/staff/kotenko
http://comsec.spb.ru/ru/projects/
http://comsec.spb.ru/en/projects

3.16. Библиографический список всех публикаций по проекту

1. Десницкий В.А., Котенко И.В. Комбинированная защита программ от несанкционированных модификаций // Изв. вузов. Приборостроение, Т.53, № 11, 2010, С.36-41. ISSN 0021-3454.

2. Котенко И.В., Коновалов А.М., Шоров А.В. Исследование бот-сетей и механизмов защиты от них на основе методов имитационного моделирования // Изв. вузов. Приборостроение, Т.53, № 11, 2010, С.42-45. ISSN 0021-3454.

3. Чечулин А.А., Котенко И.В. Комбинирование механизмов защиты от сканирования в компьютерных сетях // Информационно-управляющие системы, 2010, № 12, С.21-27. ISSN 1684-8853.

4. 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). М., 2010.

5. Kotenko I. Agent-Based Modelling and Simulation of Network Cyber-Attacks and Cooperative Defence Mechanisms // Discrete Event Simulations. Sciyo, In-teh. 2010. P.223-246. ISBN 978-307-115-2

6. 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. Los Alamitos, California. IEEE Computer Society. 2010. P.617-623. ISSN 1066-6192. ISBN 978-0-7695-3939-3.

7. Kotenko I., Konovalov A., Shorov A. Agent-based Modeling and Simulation of Botnets and Botnet Defense // Conference on Cyber Conflict. Proceedings 2010. CCD COE Publications. Tallinn, Estonia, June 15-18, 2010. P.21-44.

ISBN 978-9949-9040-1-3.

8. Kotenko I., Scormin V. (Eds.) Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag, Vol. 6258. The Fifth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2010). September 8-10, 2010, St. Petersburg, Russia. 346 p. ISSN 0302-974

9. Saenko I., Kotenko I. Genetic Optimization of Access Control Schemes in Virtual Local Area Networks // Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag, Vol. 6258. The Fifth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2010). September 8-10, 2010, St. Petersburg, Russia. P.209-216. ISSN 0302-9743

10. Desnitsky V., Kotenko I. Security and Scalability of Remote Entrusting Protection // Lecture Notes in Computer Science, Springer-Verlag, Vol. 6258. The Fifth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2010). September 8-10, 2010, St. Petersburg, Russia. P.298-306. ISSN 0302-9743

11. Kotenko I., Konovalov A., Shorov A. Simulation of Botnets: Agent-based approach // Intelligent Distributed Computing IV. Studies in Computational Intelligence. Springer-Verlag, Vol.315. Proceedings of 4th International Symposium on Intelligent Distributed Computing – IDC 2010. September 16-18, 2010. Tangier, Morocco. Springer. P. 247–252.

12. Комашинский Д.В., Котенко И.В. Концептуальные основы использования методов Data Mining для обнаружения вредоносного программного обеспечения // Защита информации. Инсайд, 2010. № 2, С.74-82.

13. Котенко И.В., Коновалов А.М., Шоров А.В. Агентно-ориентированное моделирование функционирования бот-сетей и механизмов защиты от них // Защита информации. Инсайд, 2010. № 4, С.36-45. № 5, С.56-61.

14. Котенко И.В., Саенко И.Б., Юсупов Р.М. Международная конференция «Математические модели, методы и архитектуры для защиты компьютерных сетей» // Защита информации. Инсайд, 2010. № 6, С.16-18.

15. Комашинский Д.В., Котенко И.В., Шоров А.В. Подход к обнаружению вредоносного программного обеспечения на основе позиционно-зависимой информации // Труды СПИИРАН, Выпуск 10. СПб.: Наука, 2010. С.144-159. ISBN 978-5-02-025507-4.

16. Котенко И.В., Коновалов А.М., Шоров А.В. Моделирование функционирования команд интеллектуальных агентов бот-сетей и систем защиты // Двенадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2010 (20-24 сентября 2010 г., г. Тверь, Россия): Труды конференции. Т. 3. – М.: Физматлит, 2010. С. 44-51. ISBN 978-5-7995-0543-1.

17. Десницкий В.А., Котенко И.В. Разработка и анализ протокола удаленного доверия // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Труды конференции. СПб., 2010. С.121-129. ISBN 978-5-904031-95-4.

18. Десницкий В.А., Котенко И.В. Защита программного обеспечения на основе принципа удаленного доверия // Пятая международная научная конференция по проблемам безопасности и противодействия терроризму. МГУ. 29-30 октября 2009 г. Том 2. Материалы Восьмой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2009). Москва, Издательство МЦНМО, 2010. С.159-163. ISBN 978-5-94057-693-8.

19. Комашинский Д.В., Котенко И.В. Обнаружение malware на основе обработки статической позиционной информации методами Data Mining // Пятая международная научная конференция по проблемам безопасности и противодействия терроризму. МГУ. 29-30 октября 2009 г. Том 2. Материалы Восьмой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2009). Москва, Издательство МЦНМО, 2010. С.136-140. ISBN 978-5-94057-693-8.

20. Комашинский Д.В., Котенко И.В. Комбинирование методов Data Mining для статического детектирования Malware // Двенадцатая Международная конференция "РусКрипто'2010". Московская область, г.Звенигород, 1-4 апреля 2010 г. http://www.ruscrypto.ru/

21. Чечулин А.А. Защита от сетевых атак на основе комбинированных механизмов анализа трафика // Двенадцатая Международная конференция "РусКрипто'2010". Московская область, г.Звенигород, 1-4 апреля 2010 г. http://www.ruscrypto.ru/

22. Зозуля Ю.В., Котенко И.В. Блокирование Web-сайтов с неприемлемым содержанием на основании выявления их категорий // Двенадцатая Международная конференция "РусКрипто'2010". Московская область, г.Звенигород, 1-4 апреля 2010 г. http://www.ruscrypto.ru/

23. Коновалов А.М., Шоров А.В., Котенко И.В. Агентно-ориентированное моделирование бот-сетей // Двенадцатая Международная конференция "РусКрипто'2010". Московская область, г.Звенигород, 1-4 апреля 2010 г. http://www.ruscrypto.ru/

24. Котенко И.В. Исследование бот-сетей и механизмов защиты от них на основе агентно-ориентированного моделирования // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.40-41.

25. Десницкий В.А., Котенко И.В. Комбинированные механизмы защиты программ от несанкционированных модификаций // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.100-101.

26. Коновалов А.М., Котенко И.В., Шоров А.В. Среда моделирования для имитации сетевых атак и механизмов защиты // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.38-39.

27. Степашкин М.В., Котенко И.В., Чечулин А.А., Тулупьев А.Л., Тулупьева Т.В., Пащенко А.Е. Подход к анализу защищенности автоматизированных систем с учетом социо-инженерных атак // Методы и технические

средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.128-129.

28. Котенко И.В., Степашкин М.В., Чечулин А.А., Дойникова Е.В., Котенко Д.И. Инструментальные средства анализа защищенности автоматизированных систем // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.115-116.

29. Чечулин А.А. Интеграция механизмов защиты от сканирования и выбор их оптимальных параметров // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.25-26.

30. Десницкий В.А. Методика поиска оптимальной комбинации методов защиты для защиты программ от вмешательств // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.9-10.

31. Комашинский Д.В. Комбинирование методов интеллектуального анализа данных для детектирования вредоносных программ // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.112-113.

32. Шоров А.В. Моделировании стадии формирования и сдерживания распространения бот-сети // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.50-51.

33. Десницкий В.А., Чечулин А.А., Котенко И.В. Конфигурационная модель встроенных систем // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.41-42. ISBN 978-5-904031-99-2.

34. Коновалов А.М., Котенко И.В. Библиотека модулей для моделирования бот-сетей // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.110-111. ISBN 978-5-904031-99-2.

35. Десницкий В.А., Чечулин А.А. Абстрактная модель встроенных систем // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.40-41. ISBN 978-5-904031-99-2.

36. Дойникова Е.В. Подходы к оценке рисков на основе графов атак // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.99-100. ISBN 978-5-904031-99-2.

37. Дойникова Е.В. Использование нечетких множеств для оценки рисков на основе графов атак // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.100. ISBN 978-5-904031-99-2.

38. Комашинский Д.В. Вредоносные программы: анализ метаданных средствами Data Mining // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.109-110. ISBN 978-5-904031-99-2.

39. Котенко Д.И. Анализ существующих подходов к построению графов атак и обеспечения их масштабируемости для корпоративных сетей // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.113-114. ISBN 978-5-904031-99-2.

40. Чечулин А.А. Интеграция механизмов обнаружения вредоносного трафика // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.149. ISBN 978-5-904031-99-2.

41. Чечулин А.А., Десницкий В.А., Степашкин М.В. Модель нарушителя в задаче обеспечения безопасности встроенных систем // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.150. ISBN 978-5-904031-99-2.

42. Шоров А.В. Анализ DDOS-Атак и механизмов защиты от них и требования к их моделированию // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.152. ISBN 978-5-904031-99-2.

43. Шоров А.В. Анализ биоинспирированных подходов в области защиты компьютерных систем // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.151. ISBN 978-5-904031-99-2.

44. Чечулин А.А., Котенко И.В. Комбинирование механизмов обнаружения сканирования // Девятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2010). Москва, МГУ, 2011.

45. Десницкий В.А., Котенко И.В., Чечулин А.А. Абстрактная модель встроенных безопасных систем // Девятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2010). Москва, МГУ, 2011.

46. Коновалов А.М., Котенко И.В., Шоров А.В. Эксперименты по исследованию бот-сетей // Девятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2010). Москва, МГУ, 2011.

47. Чечулин А.А., Десницкий В.А. Модель нарушителя в задаче обеспечения безопасности встроенных систем // Девятая общероссийская научная конференция «Математика и безопасность информационных

технологий» (МаБИТ-2010). Москва, МГУ, 2011.

48. Котенко И.В., Саенко И.Б., Юсупов Р.М. Аналитический обзор докладов Международной конференции "Математические модели, методы и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2010) // Труды СПИИРАН, Выпуск 12. СПб.: Наука, 2010.

49. Котенко И.В., Саенко И.Б., Юсупов Р.М. Аналитический обзор докладов Международного семинара "Научный анализ и поддержка политик безопасности в киберпространстве" (SA&PS4CS 2010) // Труды СПИИРАН, Выпуск 10. СПб.: Наука, 2012.

50. Kotenko I., Stepashkin M., Doynikova E. Security Analysis of Computer-aided Systems taking into account Social Engineering Attacks // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). Ayia Napa, Cyprus, 9-11 February, 2011. Los Alamitos, California. IEEE Computer Society. 2011.

51. Saenko I., Kotenko I. Genetic Algorithms for Role Mining Problem // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). Ayia Napa, Cyprus, 9-11 February, 2011. Los Alamitos, California. IEEE Computer Society. 2011.

52. Desnitsky V., Kotenko I., Chechulin A. An abstract model for embedded systems and intruders // Proceedings of the Work in Progress Session held in connection with the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). Ayia Napa, Cyprus, February 2011. SEA-Publications. 2011.

53. Kotenko I., Chechulin A., Doynikova E. Combining of Scanning Protection Mechanisms in GIS and Corporate Information Systems // Information Fusion and Geographic Information Systems. Proceedings of the Fourth International Workshop. Brest, France, 2011. Lecture Notes in Geoinformation and Cartography. Springer. 2011.

54. Kotenko I. Software agents for network security // NATO Science for Peace and Security Series, Software Agents, Agent Systems and Their Applications, 2011. Edited by Mohammad Essaaidi, Maria Ganzha, and Marcin Paprzycki. IOS Press. 2011.

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

*3.18. Критическая технология РФ, в которой, по мнению исполнителей, могут быть использованы результаты данного проекта*технологии обработки, хранения, передачи и защиты информации