

Лаборатория интеллектуальных систем

Заведующий лабораторией д.т.н., проф., Заслуженный деятель науки РФ **Городецкий Владимир Иванович** – искусственный интеллект, в частности, многоагентные системы, машинное обучение, извлечение знаний из баз данных, интеллектуальные системы планирования и составления расписаний, многоагентные модели комплексной защиты компьютерных сетей, агентно-ориентированное моделирование, а также методы скрытия данных в цифровых изображениях.

gor@mail.iias.spb.su

<http://space.iias.spb.su/ai/english/gorodetski.htm>

Общая численность - 5 человек

Научные сотрудники и краткое наименование направления работ

Д.т.н., профессор, в.н.с. **Котенко Игорь Витальевич** – искусственный интеллект, в частности, многоагентные системы, агентно-ориентированное моделирование, модели комплексной защиты компьютерных сетей, математические модели распределенных атак на компьютерные сети, ложные информационные системы, системы поддержки принятия решений, телекоммуникационные системы.

ivkote@iias.spb.su

<http://space.iias.spb.su/ai/kotenko/kotenko.jsp>

К.т.н., с.н.с. **Карсаев Олег Владиславович** – искусственный интеллект, в частности, инструментальные средства разработки многоагентных систем, анализ и объединение данных для принятия решений, индуктивное обучение, технология многоагентных систем, планирование и составление расписаний, модели комплексной защиты компьютерных сетей.

ok@mail.iias.spb.su

<http://space.iias.spb.su/ai/karsaev/karsaev.jsp>

Н.с. **Самойлов Владимир Владимирович** – искусственный интеллект, в частности, многоагентные системы, распределенное обучение, многоагентные модели защиты компьютерных сетей, протоколы координации поведения агентов, а также методы скрытия данных в цифровых изображениях

samovl@iias.spb.su

<http://space.iias.spb.su/ai/samoilov/samoilov.jsp>

Н.с. **Конюший Виктор Григорьевич** - инструментальные средства разработки многоагентных систем, планирование и составление расписаний, программирование.

kvg@iias.spb.su

<http://space.iias.spb.su/ai/konyushiy/konyushiy.jsp>

Н.с. **Маньков Евгений Викторович** – формальные грамматики, синтаксический анализ, модели атак на компьютерные сети, инструментальные средства разработки многоагентных систем, программирование.

mankov@iias.spb.su, Toltec@pisem.net

<http://space.iias.spb.su/ai/mankov/mankov.jsp>

Гранты и проекты

Городецкий В.И. Разработка методов извлечения знаний из распределенных баз данных, полученных из разных источников. Программа МНТЦ-ЕОАРД, проект №1993Р (2000-2003), <http://space.iias.spb.su/ai/projects/project1993p.jsp>.

Котенко И.В. Математическая модель распределенных атак на компьютерную сеть и программный прототип имитатора атак. Программа МНТЦ-ЕОАРД, проект №1994Р (2000-2003), <http://space.iias.spb.su/ai/projects/project1994.jsp>.

Котенко И.В. Многоагентная модель обучения обнаружению вторжений в компьютерную сеть. Программа МНТЦ-ЕОАРД, проект №1994Р (2000-2003), <http://space.iias.spb.su/ai/projects/project1994.jsp>.

Карсаев О.В. Автономные интеллектуальные системы планирования операций и составления расписаний. Программа МНТЦ-ЕОАРД, проект №1992Р (2000-2003), <http://space.iias.spb.su/ai/projects/project1992p.jsp>.

Городецкий В.И. Математические модели и методы распределенного обучения многоагентных систем объединения данных, полученных из различных источников. Грант РФФИ № 01-01-00109 (2001-2003).

Самойлов В.В. Математические модели и методы распределенного обучения многоагентных систем объединения данных, полученных из различных источников. Грант РФФИ – МАС № 03-01-06150 (2003).

Котенко И.В. Математические модели и методы защиты информации в компьютерных сетях, основывающиеся на многоагентных технологиях, и их экспериментальная оценка. Грант РФФИ № 01-01-00108 (2001-2003).

Маньков Е.В. Математические модели и методы защиты информации в компьютерных сетях, основывающиеся на многоагентных технологиях, и их экспериментальная оценка. Грант РФФИ – МАС № 03-01-06139 (2003).

Городецкий В.И. "Стохастическое моделирование конкурирующих распределенных систем, работающих в среде Интернет." Проект по программе фундаментальных исследований Отделения информационных технологий и вычислительных систем РАН "Фундаментальные основы информационных технологий и систем." Контракт № 10002-251/ОИТВС-01/097-110/210503-176 от 6 мая 2003 г.

Котенко И.В. "Математические модели активного анализа уязвимостей, обнаружения вторжений и противодействия сетевым атакам в компьютерных сетях, основывающиеся на многоагентных технологиях" Проект по программе фундаментальных исследований Отделения информационных технологий и вычислительных систем РАН "Оптимизация вычислительных архитектур под конкретные классы задач, информационная безопасность сетевых технологий". Контракт № 3.2/03 от 26.05.2003 г., номер регистрации РАН 10002-251/ОИТВС-04/103-110/260503-209.

Участие в конференциях

1. 5 Международная конференция "Проблемы управления и моделирования в сложных системах". Самара, июнь 18-22, 2003 (В.И.Городецкий, 1 доклад).
2. Международная конференция "Fusion 03", Кернс, Австралия, Июль 2003 (В.И.Городецкий-1 доклад).
3. IEEE Международная конференция "Технология интеллектуальных агентов" (IAT03), Галифакс, Канада, Октябрь 2003. (В.И.Городецкий-1 доклад и И.В.Котенко-1 доклад).
4. Международная летняя школа НАТО (NATO Advanced Study Institute) "Слияние данных для мониторинга ситуаций, обнаружения инцидентов, тревог и мониторинг реакций", Ереван, Август 17-29, 2003 (В.И.Городецкий-3 часовая лекция).
5. 3 Международная конференция Центральной и Восточной Европы по многоагентным системам (SEEMAS 2003), Июнь 15-17, 2003, Прага, Чехия (О.В.Карсаев-1 доклад и И.В.Котенко-1 доклад).
6. Международный семинар "Математические модели, методы и архитектуры для защиты компьютерных сетей". Санкт-Петербург, Россия, Сентябрь 21–23, 2003 (В.И.Городецкий и В.В.Самойлов-1 доклад, И.В.Котенко и Е.В.Маньков-1 доклад, О.В.Карсаев, В.Г.Конюший)
7. Международный конгресс «Доверие и безопасность в информационном обществе», СПб, 21-22 апреля, 2003 (И.В.Котенко- 1 доклад)
8. 4 Международная конференция "Агентно-ориентированное моделирование" (ABS-4)", Монтпелье, Франция, Апрель 28-30, 2003 (И.В.Котенко-1 доклад).
9. 3 Международная конференция "Военно-морской флот и кораблестроение в современных условиях" (NSN'2003). Санкт-Петербург, Россия, Июнь 26 – 28, 2003, (И.В.Котенко-1 доклад).
10. Международная конференция по мягким вычислениям и измерениям. SMC'2003, СПб: СПбГЭТУ, 2003 (И.В.Котенко- 2 доклада).
11. Международная научно-техническая конференций "Интеллектуальные системы (IEEE AIS'03), Дивногорское, Россия, 5-10 сентября 2003 (И.В.Котенко- 1 доклад, О.В.Карсаев, Е.В.Маньков).
12. Научная Школа "Моделирование и Анализ Безопасности и Риска в Сложных Системах (МА БР–2003), Санкт-Петербург, 20-23 августа, 2003 (И.В.Котенко- 1 доклад).
13. IEEE Международная конференция "Компьютерные сети и мобильные вычисления" (ICCNMC-03). Шанхай, КНР, Октябрь 20-23, 2003 (И.В.Котенко- 1 доклад).

14. III Международная конференция "Информационная безопасность регионов России" ("ИБРР-2003") 25-27 ноября 2003, Санкт-Петербург, 2003 (И.В.Котенко- 3 доклада).
15. XI Российская научно-техническая конференция (по Северо-западному региону) "Методы и технические средства обеспечения безопасности информации". СПбГПУ, Санкт-Петербург, 25-27 ноября 2003 (И.В.Котенко- 2 доклада).
16. Российско-Китайская конференция "Интеллектуальная обработка данных" (CRBCIP-2003), октябрь 19-23, 2003, Шанхай, КНР (И.В.Котенко- 2 доклада).
17. Международная конференция "Автономные агенты и многоагентные системы" , Мельбурн, Австралия, июль 16-18, 2003 (В.И.Городецкий).
18. Международный семинар "Военные приложения систем принятия решений на основе распределенных источников данных", Аделаида, Австралия, июль 14-15, 2003 (В.И.Городецкий).
19. Летняя школа НАТО "Технология доказательств и вычислений", Марктобердорф, Германия, 30 июля–9 августа 2003 (В.В.Самойлов–участник школы).

Международное сотрудничество

Городецкий В.И. - Участие в программных комитетах следующих международных конференций и семинаров:

Второй международный семинар "Математические методы, модели и архитектуры систем защиты компьютерных сетей (MMM-ACNS-2003), Со-председатель программного комитета, Санкт-Петербург, 20-24 сентября, 2003.

3 Международная конференция Центральной и Восточной Европы по многоагентным системам (CEEMAS-03), Прага, Чешская Республика, июнь, 2003.

IEEE Международная конференция "Технология интеллектуальных агентов" (IAT03), Галифакс, Канада, Октябрь 2003

Международная IEEE конференция "Искусственные интеллектуальные системы" (IEEE AIS-03). Дивноморск, Россия, 3-10 сентября 2003.

Китайско-Российский семинар "Интеллектуальная обработка данных", 19-23 ноября 2003, Шанхай, КНР.

Котенко И.В. - Участие в программных комитетах следующих международных конференций и семинаров:

Второй международный семинар "Математические методы, модели и архитектуры систем защиты компьютерных сетей (MMM-ACNS-2003), Санкт-Петербург, Сентябрь 20-24, 2003.

Китайско-Российский семинар "Интеллектуальная обработка данных", 19-23 октября 2003, Шанхай, КНР.

III Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2003"). СПб, 25-27 ноября 2003.

Международное сотрудничество с European Office of Aerospace Research and Development (США), Office of Naval Research International Field Office (США), Naval Postgraduate School (Monterey, CA, США), AgentLink (Проект Европейской программы FP5), KNet (Проект Европейской программы FP5), Institute of Computer Technology (Китай), Binghamton University (США), Fraunhofer First Institute (Германия).

Членство в российских и международных организациях

Городецкий В.И.–Член Российской и Европейской ассоциаций искусственного интеллекта, IEEE и IEEE Computer Society, International Society of Information Fusion (ISIF).

Котенко И.В. – Член Российской и Европейской ассоциаций искусственного интеллекта.

Награды, почетные и ученые звания, премии, стипендии

Городецкий В.И. – Заслуженный деятель науки РФ.

Области исследований

Теория и технология многоагентных систем. Системы объединения данных, полученных из различных источников. Многоагентные модели планирования операций.

Многоагентные модели комплексной защиты компьютерных сетей. Математические модели распределенных атак на компьютерные сети. Методы скрытия данных в цифровых изображениях. Технология распределенного обучения распределенного принятия решений

Новые результаты исследований

1. Разработана методология, технология и инструментальное средство для создания и программной реализации многоагентных систем распределенного обучения и принятия решений. Разработанная методология определяет базовые принципы, готовые модели (рекомендуемые решения), методы и конкретные алгоритмы распределенного обучения и принятия решений на основе распределенных гетерогенных источников данных. Новизна этой методологии состоит в том, что она базируется на проблемной и предметной онтологиях, использует иерархическую структуру принятия решений и специальные процедуры мета-обучения и объединения решений и ориентирована на создание распределенных баз знаний, в которых роль мета-уровня играет онтология. Эта методология положена в основу разработанной технологии и инструментального средства для создания и программной реализации многоагентных систем распределенного обучения ([1-8]). На базе этой технологии и с использованием упомянутого инструментального средства разработана технология обучения обнаружению вторжений. Разработаны архитектура, модели функционирования, структуры и экземпляры данных обучения и тестирования, а также прототипы отдельных компонент. Проведена экспериментальная оценка разработанных компонент обучения [9, 26].

2. Разработан комплекс математических моделей для имитации атак на компьютерные сети, основанный на аппарате формальных грамматик и автоматов. Разработаны модели действий злоумышленника, модели атакуемой компьютерной сети и хостов; модели вычисления вероятностей успешного выполнения атак и модели реакции хостов на действия злоумышленника. Разработаны концептуальные модели многоагентного моделирования сложных распределенных скоординированных атак на компьютерные сети, в частности атак "распределенный отказ в обслуживании" (DDoS-атак). Предложен подход к многоагентному моделированию противоборства команд программных агентов в компьютерных сетях. Разработанные модели реализованы программно в виде прототипов многоагентных систем моделирования. ([9, 12-29, 31, 33, 35, 36]).

3. Разработана методология многоагентного планирования и составления расписаний, в которой координация поведения агентов основана на использовании модели аукциона и идеи отложенных решений. Разработана технология создания систем названного класса, а также инструментальное программное средство, поддерживающее процесс формального описания, программной реализации и развертывания сложных систем указанного класса, в частности, в области транспортной логистики. Разработаны математические модели для формального задания протоколов кооперативного решения задач множеством распределенных агентов. Методология решения, технология и программное инструментальное средство использованы для разработки прототипа многоагентной системы, решающей задачи транспортной логистики со множеством ограничений, среди которых наиболее существенным является ограничения в виде временных окон на доставку грузов [3, 4, 10].

Список публикаций

1. В. Городецкий, О. Карсаев, В. Самойлов. Многоагентная технология принятия решений в задачах объединения данных. Труды СПИИРАН, №1, 2003.
2. В. В. Самойлов. Системы объединения данных из разных источников: Принципы реализации и архитектура обработки данных для обучения систем принятия решений. Труды СПИИРАН, № 1, 2003.
3. В.И. Городецкий, О.В. Карсаев, В.Г. Конюший, В.В. Самойлов, А.Хабалов. Среда разработки многоагентных приложений MASDK. Информационные технологии и вычислительные системы, №1, 2003.

4. В.И.Городецкий, О.В.Карсаев. Технология многоагентных систем и ее приложения в управлении и моделировании. Труды 5 Международной конференции "Проблемы управления и моделирования в сложных системах". Под редакцией В.П.Мясникова, Н.А.Кузнецова и В.А.Виттиха. Самара, 2003, стр. 271-283.
5. В.И.Городецкий, О.В.Карсаев, В.В.Самойлов. Распределенное обучение объединению данных: Многоагентный подход. В Трудах Международной конференции Fusion 03, Кернс, Австралия, июль 8-11, 2003.
6. В.И. Городецкий, О.В. Карсаев, В.В. Самойлов. Многоагентная технология распределенного извлечения знаний из данных для решения задач классификации. В Трудах Международной IEEE конференции "Технология интеллектуальных агентов" (IAT' 03), Галифакс, Канада, октябрь 13-17, стр.438-441, 2003.
7. В.И. Городецкий, О.В. Карсаев, В.В. Самойлов. Программный инструментарий для создания многоагентных систем извлечения знаний из распределенных данных. Труды Международной IEEE конференции "Интеграция интеллектуальных многоагентных систем" (KIMAS 03), Бостон, США, октябрь 2003, стр.710-715.
8. В.И. Городецкий, О.В. Карсаев, В.В. Самойлов. Многоагентные системы для слияния данных и информации: Архитектура, методология, и инструментальные средства поддержки технологии. Принято для публикации в книге "Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Monitoring" под ред. Э.Шахбазян и П.Валлин. Будет опубликовано в издательстве Kluwer Academic Publishers.
9. Городецкий В.И., Котенко И.В., Карсаев О.В. Многоагентные технологии для обеспечения безопасности компьютерных сетей: имитация атак, обнаружение вторжений и обучение обнаружению вторжений. Международный журнал по компьютерным наукам и инженерии, 2003, № 4, Англия, стр.191-200.
10. В.И.Городецкий, О.В.Карсаев, В.Г.Конюший. Многоагентная система распределения ресурсов и составления расписаний. Труды 3 Международной конференции Центральной и Восточной Европы по многоагентным системам. (CEEMAS 2003). Под ред. В.Маржек, Й.Мюллер и М.Пехоучек. Lecture Notes in Artificial Intelligence, Springer-Verlag, том 2691 стр.236-246.
11. В.И.Городецкий, В.В.Самойлов. Экспериментальное исследование свойств метода встраивания скрытой информации в цифровые изображения, основанного на использовании сингулярного разложения. Под ред. В.И.Городецкого, В.А.Скормина и Л.Попьяка. Lecture Notes in Computer Science, Springer-Verlag, том 2776, "Теория и практика защиты компьютерных сетей. Труды 2 Международной конференции "Математические модели, методы и архитектуры для защиты компьютерных сетей". Санкт-Петербург, Россия, сентябрь, 21-23, 2003, стр.349-359.
12. Котенко И.В. Многоагентные технологии активного анализа уязвимостей и обнаружения вторжений для создания информационно-безопасных распределенных вычислительных систем. Международный конгресс "Доверие и безопасность в информационном обществе", Санкт-Петербург, 21-22 апреля, 2003.
13. Котенко И.В., Маньков Е.В. Агентно-ориентированное моделирование атак на компьютерные сети. Четвертый Международный семинар "Агентно-ориентированное моделирование" (ABM-4). Сборник трудов, 28-30 апреля, Монтпелье, Франция, 2003. стр.121-126.
14. И.В.Котенко. Командная работа хакеров Формальное описание и компьютерное моделирование координированных распределенных атак на компьютерные сети. Труды 3 Международной конференции Центральной и Восточной Европы по многоагентным системам. (CEEMAS 2003). Под ред. В.Маржек, Й.Мюллер и М.Пехоучек. Lecture Notes in Artificial Intelligence, Springer-Verlag, том.2691, стр.464-474.
15. В.И.Городецкий, И.В.Котенко, Б.Дж.Майкл. Многоагентное моделирование распределенных атак "Отказ в обслуживании" на компьютерные сети. Третья Международная конференция "Военно-морской флот и судостроение в современных условиях" (NSN'2003). Санкт-Петербург, 26 - 28 июня, 2003. Сборник трудов. стр.38-47.
16. Алексеев А.С., Котенко И.В. Командная работа агентов по защите от распределенных атак "отказ в обслуживании". Международная конференция по мягким вычислениям и измерениям (SMC'2003). Сборник докладов. Санкт-Петербург, СПбГЭТУ, 2003, стр.294-297.

17. Котенко И.В., Степашкин М.В. Интеллектуальная система моделирования атак на Web-сервер для анализа уязвимостей компьютерных систем. Международная конференция по мягким вычислениям и измерениям (SMC'2003). Сборник докладов. Санкт-Петербург, СПбГЭТУ, 2003, стр.298-301.
18. Котенко И.В., Станкевич Л.А. Командная работа агентов в реальном времени. Новости искусственного интеллекта, № 3, 2003, стр.25-31.
19. Котенко И.В. Модели противоборства команд агентов по реализации и защите от распределенных атак "отказ в обслуживании". Труды Международных научно-технических конференций "Интеллектуальные системы (IEEE AIS'03)" и "Интеллектуальные САПР (CAD-2003)". Изд-во Физико-математической литературы, 2003, том.1, стр. 422-428.
20. Нестеров С.А., Котенко И.В. Анализ рисков безопасности компьютерных систем на основе использования имитатора сетевых атак. VIII Санкт-Петербургская Международная Конференция "Региональная информатика-2002" ("РИ-2002"). Труды конференции. Санкт-Петербург, 2003, стр.185-189.
21. Котенко И.В., Алексеев А.С. Моделирование DDoS-атак на основе командной работы агентов. VIII Санкт-Петербургская Международная Конференция "Региональная информатика-2002" ("РИ-2002"), Труды конференции, Санкт-Петербург., 2003, стр.180-184.
22. И. В. Котенко, С. А. Нестеров. Проектирование систем защиты информации на основе интеграции процедур анализа рисков и активного аудита безопасности. Международная Научная Школа "Моделирование и анализ безопасности и риска в сложных системах (МА БР-2003), Санкт-Петербург, 20-23 августа, 2003, стр.396-402.
23. И.В.Котенко., Е.В.Маньков. Эксперименты по моделированию атак против компьютерных сетей. Под ред. В.И.Городецкого, В.А.Скормина и Л.Попьяка. Lecture Notes in Computer Science, Springer-Verlag, том 2776, "Теория и практика защиты компьютерных сетей". Труды 2 Международной конференции "Математические модели, методы и архитектуры для защиты компьютерных сетей. Санкт-Петербург, Россия, сентябрь, 21–23, 2003, стр.187-198.
24. Котенко И.В., Алексеев А.С., Маньков Е.В. Формальный подход к моделированию и имитации DDoS-атак, основанный на командной работе агентов-хакеров. IEEE Международная конференция по технологии интеллектуальных агентов (IAT-03), Галифакс, Канада, 13-16 октября 2003, стр.507-510.
25. Котенко И.В.. Активный анализ уязвимостей компьютерных сетей на основе имитации сложных распределенных атак. IEEE Международная конференция по компьютерным сетям и мобильным вычислениям (ICCNMC-03), Шанхай, Китай, 20-23 октября 2003. Сборник трудов. 2003, стр.40-47.
26. Городецкий В.И., Карсаев О.В., Котенко И.В., Самойлов В.В., Степашкин М.В. Многоагентная система обучения обнаружению атак. III Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2003"). Материалы конференции. Часть 1, Санкт-Петербург, 2003, стр.118.
27. Комашинский Д.В., Котенко И.В. Модель распространения вирусов в сети Internet на основе многоагентной технологии. III Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2003"). Материалы конференции. Часть 1, Санкт-Петербург, 2003, стр.127-128.
28. Котенко И.В. Моделирование кибервойны на основе агентских технологий. III Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2003"). Материалы конференции. Часть 1, Санкт-Петербург, 2003, стр.70-71.
29. Алексеев А.С., Котенко И.В. Многоагентная система моделирования DDoOS-атак. XI Российская научно-техническая конференция (по Северо-западному региону) "Методы и технические средства обеспечения безопасности информации". Тезисы докладов. Санкт-Петербург. Издательство СПбГПУ. 2003, стр.101-102.
30. Котенко И.В., Степашкин М.В. Прототип ложной информационной системы. XI Российская научно-техническая конференция (по Северо-западному региону) "Методы и технические средства обеспечения безопасности информации". Тезисы докладов. Санкт-Петербург. Издательство СПбГПУ. 2003, стр.57-58.
31. Котенко И.В., Маньков Е.В. Стохастическая автоматная модель атак на компьютерные сети. Информатизация и связь, № 1-2, 2003, стр.61-67.

32. Котенко И.В., Городецкий В.И. Многоагентные системы для обнаружения вторжений. Труды двухсторонней российско-китайской конференции по интеллектуальной обработке информации (CRBCIIP-2003), 19-23 октября 2003, Шанхай, Китай. 2003.
33. Котенко И.В. Многоагентное моделирование и имитация атак на компьютерные сети, основанных на моделях командной работы и формальных грамматиках, Труды двухсторонней российско-китайской конференции по интеллектуальной обработке информации (CRBCIIP-2003). 19-23 октября 2003, Шанхай, Китай, 2003.
34. Котенко И.В. Анализ уязвимостей и обнаружение вторжений: применение многоагентных технологий для защиты информации в компьютерных сетях. Информационные технологии и вычислительные системы, 2003. (принято к печати)
35. Котенко И.В., Алексеев А.С. Моделирование распределенных атак “Отказ в обслуживании” на основе реализации командной работы агентов. Информационные технологии и вычислительные системы, 2003. (принято к печати)
36. Котенко И.В. Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях. Конфидент, 2003. (принято к печати)

Laboratory of Intelligent Systems

Head of the Laboratory –Ph.D., Doctor of Technical Sciences, Honored Scientist of Russia Professor **Gorodetski Vladimir Ivanovich** – Artificial Intelligence, in particular, multi-agent systems, machine learning, data mining and knowledge discovery from databases, data and information fusion, multi-agent knowledge-based systems for operation planning and scheduling, multi-agent technology for integrated assurance of computer networks, formal modeling and simulation of distributed attacks against computer networks, transparent embedding data into digital images for hidden communications and watermarking.

gor@mail.iias.spb.su,

<http://space.iias.spb.su/ai/russian/gorodetski.htm>

Laboratory Stuff - 5

Research Fellows

Ph.D., Doctor of Technical Sciences. Leading Research Scientist Professor **Kotenko Igor Vitalievich** –Artificial Intelligence, in particular, multi-agent systems, agent-based simulation, computer network and information assurance, modelling and simulation of distributed attacks against computer networks, deception systems, decision support systems, telecommunication.

ivkote@iias.spb.su

<http://space.iias.spb.su/ai/kotenko/kotenko.jsp>

Ph.D., Senior Researcher, **Karsaev Oleg Vladislavovich** – Artificial Intelligence, in particular, multi-agent systems technology and software tools, machine learning, data mining and knowledge discovery from databases, multi-agent knowledge-based systems for operation planning and scheduling, multi-agent technology for integrated assurance of computer networks, formal modeling and simulation of distributed attacks against computer networks.

ok@mail.iias.spb.su,

<http://space.iias.spb.su/ai/karsaev/karsaev.jsp>

Research Fellow **Samoilov Vladimir Vladimirovich** – Artificial Intelligence, in particular, multi-agent systems, data mining and knowledge discovery from databases and data warehouses, data and information fusion, multi-agent technology for integrated assurance of computer networks, simulation of distributed attacks against computer networks, transparent embedding data into digital images for hidden communications and watermarking.

samovl@iias.spb.su,

<http://space.iias.spb.su/ai/samoilov/samoilov.jsp>

Research Fellow **Konushy Victor Grigorievich** – Multi-agent software tool, operation planning and scheduling, software design and code writing.

kvg@iias.spb.su

<http://space.iias.spb.su/ai/konyushiy/konyushiy.jsp>

Research Fellow **Man'kov Eugene Victorovich** – Formal grammars, syntactical analysis, modeling and simulation of attacks against computer networks, multi-agent software tool, software design and code writing.

mankov@ias.spb.su, Toltec@pisem.net

<http://space.ias.spb.su/ai/mankov/mankov.jsp>

Grants and Projects

Gorodetski V.I. – Autonomous Information Collection, Knowledge Discovery Techniques and Software Tool Prototype for Knowledge-Based Data Fusion (Partner Project # 1993P, Task 1, ISTC and EOARD), 2000-2003, <http://space.ias.spb.su/ai/projects/project1993p.jsp>.

Kotenko I.V. – Formal grammar-based framework, model and software tool prototype for simulation of distributed attacks against computer network (Partner Project # 1994P, Task 1, ISTC and EOARD), 2000-2003, <http://space.ias.spb.su/ai/projects/project1994.jsp>.

Kotenko I.V. – Mathematical foundations, basic algorithms, architecture, principles of implementation and software prototypes of multi-agent learning components of network security systems focused on supporting intrusions detection (Partner Project # 1994P, Task 2, ISTC and EOARD), 2000-2003, <http://space.ias.spb.su/ai/projects/project1994.jsp>.

Karsaev O.V. – Advanced Computer Technologies Supporting Dynamic Planning and Execution (Partner Project # 1992P from ISTC and EOARD), 2000-2003, <http://space.ias.spb.su/ai/projects/project1992p.jsp>.

Gorodetski V.I. Mathematical models and techniques for distributed learning of the multi-agent data fusion systems (Project from Russian Foundation of Basic Research, #01-01-00109, 2001-2003).

Samoilov V.V. Mathematical models and techniques for distributed learning of the multi-agent data fusion systems (Project from Russian Foundation of Basic Research, #03-01-06150, 2003).

Kotenko I.V. Mathematical models of information security assurance in computer networks based on multi-agent technologies and their experimental evaluation. (Project from Russian Foundation of Basic Research, #01-01-00108, 2001-2003).

Man'kov E.V. Mathematical models of information security assurance in computer networks based on multi-agent technologies and their experimental evaluation. (Project from Russian Foundation of Basic Research, #03-01-06139, 2003).

V.Gorodetsky. "Stochastic modeling and simulation of competing distributed system operating in the Internet" Program "Fundamentals of Information Technologies and Systems" of the Russian Academy of Sciences Branch "Information Technologies and Computer Systems" Contract #10002-251/OITBC-01/097-110/210503-176, May 6, 2003.

Kotenko I.V. "Mathematical models of active analysis of vulnerabilities, intrusion detection and network attacks counteraction in computer networks based on multi-agent technologies" Program "Optimization of computer architectures to particular classes of tasks, information assurance of network technologies" of the Russian Academy of Sciences Branch "Information Technologies and Computer Systems". Contract #10002-251/OITBC-04/103-110/260503-209, May 6, 2003.

Conferences

1. 5 International Conference "Problems of Control and Simulation in Large Scale Systems", Samara, June 18-22, 2003 (V.Gorodetsky-1 paper).
2. International Conference "Fusion 03", Cairns, Australia, July 2003 (V.Gorodetsky-1 paper).
3. IEEE Conference Intelligent Agent Technology (IAT03), Halifax, Canada, October 2003. (V.Gorodetsky-1 paper and I.Kotenko-1 paper)
4. Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Monitoring, NATO Advanced Study Institute, Yerevan, August 17-29, 2003 (V.Gorodetsky-3 hours lecture)
5. Third International/Central and Eastern European Conference on Multi-Agent Systems (CEEMAS 2003), June 15-17, 2003, Prague, Czech Republic (O.Karsaev-1 paper and I.Kotenko-1 paper).

6. International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security, St. Petersburg, Russia, September 21–23, 2003 (V.Gorodetsky and V.Samoilov.- 1 paper, I.Kotenko and E.Man'kov - 1 paper, O.Karsaev, V.Konushy)
7. International Congress "Trust and safety in informational society", St. Petersburg, April 21-22, 2003, 21-22 апреля, 2003 (I.Kotenko-1 paper)
8. 4 International Conference Agent-Based Simulation 4 (ABS 4)", April 28-30. Montpellier. France. 2003 (I.Kotenko- 1 paper)
9. Third International Conference "NAVY AND SHIPBUILDING NOWADAYS" (NSN'2003). St.Petersburg, Russia. June 26 – 28, 2003, (I.Kotenko- 1 paper)
10. International Conference on Soft Computing and Measurements. SMC'2003. Saint-Petersburg, Russia. June 25 – 27, 2003, (I.Kotenko-2 papers).
11. International Conferences "Artificial Intelligence Systems" (IEEE AIS'03)" and "Intelligent CAD" (CAD-2003). Divnomorskoe, September 3-10, 2003 (I.Kotenko - 1 paper, O.Karsaev, E.Man'kov)
12. International Conference "Modeling and Analysis of Safety and Risk in Complex Systems" (MA SR - 2003). Saint-Petersburg, August 20-23, 2003 (I.Kotenko- 1 paper)
13. IEEE International Conference on Computer Networks and Mobile Computing. ICCNMC-03. Shanghai, China, October 20-23, 2003 (I.Kotenko- 1 paper)
14. III Inter-regional Conference "Information Security of Russia Regions". Saint-Petersburg, November 25-27, 2003 (I.Kotenko-3 papers).
15. XI Russian Conference "Methods and tools of information assurance". Saint-Petersburg, November 26-27, 2003. (I.Kotenko- 2 papers)
16. China-Russia Bilateral Conference on Intelligent Information Processing. CRBCIIP-2003. October 19-23, 2003, Shanghai, China (I.Kotenko- 2 paper)
17. International Conference "Autonomous Agent and Multi-agent Systems", Melbourne, Australia, July 16-18, 2003 (V.Gorodetsky)
18. International Workshop "Defense Application of Information Fusion, Adelaide, Australia, July 14-15, 2003 (V.Gorodetsky).
19. NATO Science Committee Summer School "Proof Technology and Computation". Marktoberdorf, Germany, July-29–August 9, 2003 (V.Samoilov–participant of the School).

International Cooperation

V.I.Gorodetski – participation in Program Committees of the following International conferences and workshops:

- The 3rd International/Central and Eastern European Conference on Multi-Agent Systems (CEEMAS 2003), June 16 – 18, 2003, Prague, Czech Republic (Steering and Program Committee member)
- The IEEE International Conference Artificial Intelligence Systems IEEE ICAIS'03, Russia, Divnomorskoe, September 3 10, 2003 года
- The 2003 IEEE/WIC International Conference on Intelligent Agent Technology" (IAT 2003), October 13-17, Halifax, Canada.
- The Second International Workshop "Mathematical Methods, Models and Architectures for Computer Networks Security", September 20-24, 2003, St. Petersburg, Russia (Program Committee Co-Chairman)
- China-Russia Bilateral Conference on Intelligent Information Processing, Shanghai, China, October 19-23, 2003.

I.V.Kotenko – participation in Program Committees of the following International conferences and workshops:

- International Workshop "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2003), September 20-24, 2003, St. Petersburg, Russia.
- China-Russia Bilateral Conference on Intelligent Information Processing, Shanghai, China, October 19-23, 2003.
- III Inter-regional Conference "Information Security of Russia Regions". Saint-Petersburg, November 25-27, 2003.

International cooperation with European Office of Aerospace Research and Development (USA), Office of Naval Research International Field Office (USA), Naval Postgraduate School

(Monterey, CA, USA), AgentLink (FP5 Program of EU), KNet (FP5 Program of EU) Institute of Computer Technology (China), Binghamton University (USA), Fraunhofer First Institute (Germany)

Membership in International Societies

V.Gorodetski – Member of Russian and European Associations of Artificial Intelligence, IEEE, IEEE Computer Society and International Society of Information Fusion (ISIF).

I.Kotenko – Member of Russian and European Associations of Artificial Intelligence.

Awards

V.Gorodetski – Honored Scientist of Russia.

Research Activities

Theory and technology of multi-agent systems, data fusion, data mining and knowledge discovery from databases, multi-agent operation planning and scheduling systems, multi-agent technology for integrated assurance of computer networks, formal modeling and simulation of distributed attacks against computer networks, transparent embedding data into digital images for hidden communications and watermarking, distributed learning technology, telecommunication, telematic.

Recent Results

1. Methodology, technology and software tool destined for design, implementation and deployment of multi-agent distributed data mining, distributed decision making and data and information fusion are developed. The developed methodology determines basic principles, ready models (recommended solutions) methods and particular algorithms of distributed data mining and decision making when the data are heterogeneous and distributed. The methodology novelty is determined by such its peculiarities as use of problem and application ontology as upper level of distributed knowledge base, hierarchical structure of producing and combining of decisions, use of distributed knowledge bases with ontology on the top of it. This methodology forms the basis of the developed technology and supporting software tool making it more rapid the prototyping of multi-agent distributed data mining and data and information fusion systems ([1-8]). The mentioned technology and software tool were used as a basis for multi-agent technology of intrusion detection learning system. For the latter application the operation model, training and testing data (models and respective samples)/ technology for training and testing and also the software prototypes of the basic components of multi-agent intrusion detection learning system were developed, implemented and deployed within a computer network. The developed theoretical basis and technology of multi-agent intrusion detection learning were validated via simulation [9, 26].

2. The formal-grammar- and state machine-based framework aiming at formal specification of the adversary interactions of a team of hackers performing coordinated distributed attacks against computer network, on the one side, and a team of defensive means of computer network, on the other side, was developed in depth. The conceptual models of agent-based models of sophisticated distributed coordinated attacks, in particular, DDoS attacks were developed. The formal basis for specification of adversary interactions of teams is developed. The basic model were validated via simulation of such interactions on the basis of the developed multi-agent software prototypes ([9, 12-29, 31, 33, 35, 36]).

3. A methodology of multi-agent planning, scheduling and resource allocation in which an auction model and deferred decision paradigm are used as the basis for formal specification of coordination mechanisms was developed. A technology and components of the software tool supporting this technology aiming at engineering, implementation and deployment of complex system of the above indicated class, in particular, applied to the transportation logistics scope, were developed. The above methodology, technology and software tool were used for the design, implementation and deployment of the software prototype destined to solve a computationally complex class of tasks from transportation logistics scope ([3, 4, 10]).

Publications

1. V.Gorodetsky, O.Karsaeyv, and V.Samoilov. Multi-agent technology of data fusion. Transactions of SPIIRAN, #1, 2003 (in Russian).
2. V.Samoilov. Data fusion task: Principles of formalization and architecture of training and testing. Transactions of SPIIRAN, #1, 2003 (in Russian).
3. V.Gorodetsky, O.Karsaeyv, V.Konushy, A.Khabalov and V.Samoilov. Technological environment for multi-agent systems design, implementation and deployment. Information Technologies and Computer Systems, # 1, 2003 (in Russian).
4. V.Gorodetsky, O.Karsaeyv. Multi-agent technology and its applications to control and simulation. Proceedings of 5 International Conference "Large-scale Systems: Problems of Control and Simulation". V.P.Miasnikov, N.A.Kuznetsov and V.A.Vittikh (Editors), Samara, 2003, pp. 271-283 (in Russian).
5. V.Gorodetsky, O.Karsaeyv, and V.Samoilov. Distributed Learning of Information Fusion: A Multi-agent Approach. Proceedings of the International Conference "Fusion 03", Cairns, Australia, July 2003.
6. V.Gorodetsky, O.Karsaeyv, and V.Samoilov. Multi-agent Technology for Distributed Data Mining and Classification. Proceedings of the IEEE Conference Intelligent Agent Technology (IAT03), Halifax, Canada, October 2003.
7. V.Gorodetsky, O.Karsaeyv, and V.Samoilov. Software Tool for Agent-Based Distributed Data Mining. Proceedings of the IEEE Conference Knowledge Intensive Multi-agent Systems (KIMAS 03), Boston, USA, October 2003.
8. V.Gorodetsky, O.Karsaeyv, and V.Samoilov. Multi-agent Data and Information Fusion: Architecture, Methodology, Technology and Software Tool. Accepted for publication in the book "Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Monitoring" E.Shakhbasyn and P.Vallin (Editors). To be published in Kluwer Academic Publishers.
9. V.Gorodetsky, I.Kotenko, and O.Karsaev. Multi-agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning. International Journal of Computer Systems Science and Engineering. vol.18, No.4, July 2003, pp.191-200.
10. V.Gorodetski, O.Karsaev, V.Konushy. Multi Agent System for Resource Allocation and Scheduling. Proceedings of the Third International/Central and Eastern European Conference on Multi-Agent Systems (CEEMAS 2003). V.Marik, J.Muller, M.Pechoucek (Editors). Lecture Notes in Artificial Intelligence, Springer-Verlag, vol.2691, pp.236-246.
11. V.Gorodetsky, V.Samoilov. Simulation-based Exploration of SVD-based Technique for Hidden Communication by Image Steganography Channel. Lecture Notes in Computer Science, Springer-Verlag, V.2776, "Theory and Practice of Computer Network Security". Proceedings of the International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security, St. Petersburg, Russia, September 21–23, 2003, pp.349-359.
12. I.Kotenko. Multi-agent technologies of active vulnerabilities analysis and intrusion detection for creating secure distributed computer systems. Proceedings of International Congress "Trust and safety in informational society", St. Petersburg, April 21-22, 2003, (in Russian).
13. I. Kotenko, E. Man'kov. Agent-Based Modeling and Simulation of Computer Network Attacks. Proceedings of Fourth International Workshop "Agent-Based Simulation 4 (ABS 4)". Jean-Pierre Muller, Martina-M.Seidel (Editors). April 28-3, Montpelier, France, 2003, pp.121-126.
14. I. Kotenko. Teamwork of Hackers-Agents: Modeling and Simulation of Coordinated Distributed Attacks on Computer Networks. Proceedings of The 3rd International/Central and Eastern European Conference on Multi-Agent Systems (CEEMAS 2003). Prague, Czech Republic. June 16 – 18, 2003. "Multi-Agent Systems and Applications III". V.Marik, J.Muller, M.Pechoucek (Editors), Lecture Notes in Artificial Intelligence, Springer-Verlag, vol.2691, pp.464-474.
15. V.I.Gorodetsky, I.V.Kotenko, J.B.Michael. Multi-agent Modeling and Simulation of Distributed Denial of Service Attacks on Computer Networks. Proceedings of Third International Conference "NAVY AND SHIPBUILDING NOWADAYS" (NSN'2003). St. Petersburg, Russia, June 26 – 28, 2003, pp.38-47.
16. A.Alexeev, I.Kotenko. Teamwork of agents protecting from distributed attacks "Denial of service". Proceedings of International Conference on Soft Computing and Measurements (SMC'2003). St-Petersburg, Russia. June 25 – 27, 2003, pp.294-297 (in Russian).

17. I.Kotenko., M.Stepashkin. Intelligent system for simulating attacks on Web-server for computer systems vulnerabilities analysis. Proceedings of International Conference on Soft Computing and Measurements (SMC'2003). St. Petersburg, Russia, June 25 – 27, 2003, pp.298-301 (in Russian).
18. I.Kotenko, L.Stankevich. Real-time Teamwork of Agents. AI News, № 3, 2003. pp.25-31 (in Russian).
19. Котенко И.В. I.Kotenko. Models of Opposition of Agents Teams in realizing of and protecting from distributed attacks "Denial of service". Proceedings of International Conferences "Artificial Intelligence Systems" (IEEE AIS'03) and "Intelligent CAD" (CAD-2003). Divnomorskoe, September 3-10, 2003. vol.1. pp.422-428 (in Russian).
20. S.Nesterov, I.Kotenko. Risk analysis of computer systems on the basis of using network attack simulator. Proceedings of the VIII International Conference "Regional informatics-2002", St. Petersburg, 2003. pp.185-189 (in Russian).
21. I. Kotenko, A.Alexeev. Modeling of DDoS-attacks on the basis of agents' teamwork. Proceedings of the VIII International Conference "Regional informatics-2002". St. Petersburg, 2003. pp.180-184 (in Russian).
22. I.Kotenko, S.Nesterov. Information assurance systems design by integrating the procedures of risk analysis and active security audit. International Conference "Modeling and Analysis of Safety and Risk in Complex Systems" (MA SR - 2003). St. Petersburg, August 20-23, 2003. pp.396-402 (in Russian).
23. I.Kotenko, E.Man'kov. Experiments with simulation of attacks against computer networks. Lecture Notes in Computer Science, Springer-Verlag, vol.2776. Theory and Practice of Computer Network Security. Proceedings of the International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security, St. Petersburg, Russia, September 21–23, 2003, pp.187-198.
24. I.Kotenko, A.Alexeev, E.Man'kov. Formal Framework for Modeling and Simulation of DDoS Attacks Based on Teamwork of Hackers-Agent. Proceedings of 2003 IEEE/WIC International Conference on Intelligent Agent Technology, Halifax, Canada, October 13-16, 2003, IEEE Computer Society. 2003, pp.507-510.
25. I.Kotenko. Active Assessment of Computer Networks Vulnerability by Simulation of Complex Remote Attacks. Proceedings of 2003 International Conference on Computer Networks and Mobile Computing (ICCNMC-03). Shanghai, China, October 20-23, 2003. IEEE Computer Society, 2003, pp.40-47.
26. V.Gorodetsky, O.Karsaev, I.Kotenko, V.Samoilov, M.Stepashkin. Multi-agent system of intrusion detection learning. Proceedings of III Inter-regional Conference "Information Security of Russia Regions", vol.1. St. Petersburg, November 25-27, 2003. p.118 (in Russian).
27. D.Komashinski, I.Kotenko. Multi-agent technology for modeling of virus expansion within Internet. Proceedings of the III Inter-regional Conference "Information Security of Russia Regions", vol.1. St. Petersburg, November 25-27, 2003, pp.127-128. (in Russian).
28. I.Kotenko. Modeling of cyber war on the basis of agents' technologies. Proceedings of III Inter-regional Conference "Information Security of Russia Regions", vol.1. St. Petersburg, November 25-27, 2003. P.70-71 (in Russian).
29. A.Alexeev, I.Kotenko. Multi-agent system of DDOS-attacks simulation. Proceedings of XI Russian Conference "Methods and tools of information assurance". St. Petersburg, SPbSPU, November 26-27, 2003, pp.101-102. (in Russian).
30. I.Kotenko, M.Stepashkin. Prototype of honeypot system. Proceedings of XI Russian Conference "Methods and tools of information assurance". St. Petersburg, SPbSPU., November 26-27, 2003, pp.57-58 (in Russian).
31. I.Kotenko, E.Man'kov. Stochastic model of attacks on computer networks based on state machines. Informatization and communication, № 1-2, 2003. pp.61-67 (in Russian).
32. I.Kotenko, V.Gorodetski. Multi-agent Systems for Intrusion Detection. Proceedings of China-Russia Bilateral Conference on Intelligent Information Processing (CRBCIIP-2003), October 19-23, 2003, Shanghai, China.
33. I.Kotenko. Multi-agent Modeling and Simulation of Computer Network Attacks based on Teamwork Models and Formal Grammars. Proceedings of China-Russia Bilateral Conference on Intelligent Information Processing (CRBCIIP-2003), October 19-23, 2003, Shanghai, China.

34. I.Kotenko. Vulnerabilities analysis and intrusion detection: Application of multi-agent technologies for information assurance in computer networks. Information Technologies and Computer Systems, 2003 (accepted for publication) (in Russian).
35. I.Kotenko, A.Alexeev. Modeling of Distributed Denial of Service Attacks based on agents' teamwork. Information Technologies and Computer Systems, 2003 (accepted for publication) (in Russian).
36. I.Kotenko. Multi-agent technologies of vulnerabilities analysis and intrusion detection in computer networks. Confident, № 6, 2003 (accepted for publication) (in Russian)