1.1. 01-01-00108
1.2. Котенко Игорь Витальевич
1.3. Математические модели и методы защиты информации в компьютерных сетях, основывающиеся на многоагентных технологиях, и их экспериментальная оценка
1.4. а
1.5. 2004
1.6. 1
1.7. Проект направлен на решение фундаментальной научной проблемы защиты информации в компьютерных сетях на основе использования новых подходов, основанных на многоагентных технологиях. Основные результаты проекта - математические основы, архитектуры, модели и методы функционирования, принципы реализации и программные прототипы компонентов систем анализа уязвимостей, обнаружения вторжений и обучения обнаружению вторжений в компьютерные сети, а также результаты исследовательского компьютерного моделирования их функционирования и рекомендации по созданию перспективных систем защиты информации в компьютерных сетях. В рамках проекта получены следующие частные результаты. Проведен анализ и классификация внешних и внутренних компьютерных атак. Разработаны основанные на сценариях спецификации представительного множества сетевых атак. Предложены модели и методики восстановления формальных грамматик, задающих модели атак. Создан комплекс формальных моделей для имитации атак (в том числе моделей генерации атак командой злоумышленников и моделей атакуемой компьютерной сети). Разработана архитектура многоагентной системы защиты информации (основное внимание уделено компонентам обнаружения вторжений). Предложены модели и методы функционирования отдельных компонентов (агентов) многоагентной системы защиты. Разработана онтология предметной области защиты информации в компьютерных сетях. Построена модель распределенной базы знаний системы защиты информации в форме моделей представления распределенных знаний, убеждений и намерений агентов защиты. Разработана модель взаимодействия агентов. Построена формальная модель языка коммуникации агентов и соответствующие протоколы их взаимодействия. Разработана онтология задач обучения обнаружению вторжений в компьютерные сети. Произведено распределение задач обучения между типовыми агентами обучения, и разработана архитектура многоагентной системы обучения. Выбраны и разработаны математические методы реализации функций типовых

агентов обучения различных классов. Для проверки основных теоретических результатов разработаны объектно-ориентированные проекты и прототипы (макеты) многоагентных систем моделирования атак, обнаружения вторжений и обучения обнаружению вторжений в компьютерные сети. С целью оценки качества разработанных моделей и методов проведено компьютерное моделирование функционирования прототипов.

1.8. Санкт-Петербургский институт информатики и автоматизации РАН

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

Руководитель проекта
Доктор технических наук профессор

И.В.Котенко