В.А.ВИШНЯКОВ[1], С.А.АПАНАСЕВИЧ[2]

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЗАЩИТЕ ИНФОРМАЦИИ

[1]Учреждение образования «Высший государственный колледж связи», Республика Беларусь,
[2]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Республика Беларусь.

Интеллектуальные системы защиты информации (ИСЗИ) посвящены обнаружению атак, в качестве интеллектуального инструмента в которыхх используются экспертные системы (ЭС), нейронные сети (НС) и многоагентные системы (МА). В ИСЗИ ЭС содержат описание классификационных правил, соответствующим профилям легальных пользователей и сценариям атак на систему. Недостатки ИСЗИ на базе ЭС: система не является адаптивной; не всегда обнаруживаются неизвестные атаки [1]**.** В системах обнаружения атак можно выделить применение НС, дополненных ЭС. Чувствительность системы возрастает, так как ЭС получает данные только о событиях, которые рассматриваются в качестве подозрительных. Если НС за счет обучения стала идентифицировать новые атаки, то ЭС следует обновить [1]. Использование гибридных нейро-экспертных или нейро-нечетких систем позволяет отразить в структуре системы нечеткие предикатные правила, которые автоматически корректируются в процессе обучения НС. Свойство адаптивности нечетких НС позволяет решать задачи идентификации угроз, автоматически формировать новые правила при изменении поля угроз [1].

Технологии Вэб-семантик позволяют воспринимать информацию в Вэб-пространстве интеллектуальными агентами (ИА) и осуществлять обработку данных. ИА позволяют выполнять: поиск по нескольким критериям; сбор, анализ, обработку данных; обмен с другими агентами и онтологиями; способность самообучаться. Онтологии включают метаданные, описывающие семантическую структуру предметной области [2]. Новым направлением в ИСЗИ является использование ИА, работающих в распределенной системе и запрограммированных на поиск, как вторжения, так и аномалий [2,3]. Выделены следующие области использования ИА в защите информации: автоматизация проведения исследований по системам обнаружения атак (СОА); автоматизация поиска по ЗИ (организаций, технологий, услуг и т.д.); интеллектуализация принятия решений по ЗИ [3]. Рассмотрим использование мультиагентных систем в ЗИ [3]. В этом случае необходимо исследовать распространенные атаки на информационную систему и процесс реализации атак, исследовать существующие системы обнаружения атак и методы обнаружения атак, разработать структуру и состав многоагентной системы обнаружения атак; разработать структуру агентов системы обнаружения атак, разработать модель представления знаний агентов о состоянии информационной системы, разработать метод совместного анализа агентами данных о состоянии информационной системы.

Архитектура многоагентной СОА может включать в себя множество взаимодействующих интеллектуальных агентов, выделенные типовые компоненты информационной системы (ИС), источники сведений, подлежащих анализу для задачи обнаружения атак [3]. Структура агентов включает модули управления, получения и обработки данных, их анализа, обучения, реакции, генерации сообщения, принятия решения. Методика работы с разработанной многоагентной СОА включает шаги: размещение агентов по блокам ИС; сбор данных, формирование обучающей выборки, обнаружение атак, сообщение об этом администратору.

Список использованных источников

1. Черкасова Ю.М. Защита информации в автоматизированных информационных технологиях управления / Ю.М. Черкасова / В кн. Информационные технологии управления. М.: Дело, 2011. – С.215-274.

2. Вишняков, В.А. Модели и средства интеграции приложений, маркетинга, аутсорсинга, обработки знаний в компьютерных сетях: монография / В.А. Вишняков, Ю.В. Бородаенко, Д.С. Бородаенко. Минск, МИУ, 2011. – 350 С.

3. Никишова А.В. Принципы функционирования многоагентной системы обнаружения атак / А.В. Никишова // Известия ЮФУ. Тематический выпуск. «Информационная безопасность» – Таганрог: ТТИ ЮФУ, 2012, №12 (137), С. 28-33.