АНАЛИЗ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ АГЕНТОВ ДЛЯ ЕЕ СОВЕРШЕНСТВОВАНИЯ

Вишняков В. А.
Кафедра менеджмента, Минский институт управления
Минск, Республика Беларусь
E-mail: {vish2002}@list.ru

Проведен анализ методов и средств защиты информации в информационных системах. Выделено направление интеллектуальных систем в защите информации (ИСЗИ). Рассмотрено применение экспертных систем, нейронных сетей, их комбинирование. В качестве перспективного метода ИСЗИ рассмотрено использование интеллектуальных агентов.

Введение

Дестабилизирующие факторы в функционировании информационных систем [1]: 1. Количественная недостаточность - физическая нехватка одного или нескольких компонентов АИС для обеспечения требуемой защищенности информации по рассматриваемым показателям; 2. Качественная недостаточность - несовершенство конструкции или организации одного или нескольких компонентов АИС, в силу чего не обеспечивается требуемая защищенность информации; 3. Отказ - нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им своих функций; 4. Сбой - временное нарушение работоспособности какого-либо элемента АИС, следствием чего может быть неправильное выполнение им в этот момент своих функций; 5. Ошибка - неправильное (одноразовое или систематическое) выполнение элементом системы одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния; 6. Стихийное бедствие - спонтанно возникающее неконтролируемое явление, проявляющееся как разрушительная сила; 7. Злоумышленные действия - действия людей или средств, специально направленные на нарушение защищенности информации.

I. Методы и средства защиты информации

К методам защиты информации относятся: управление, препятствие, регламентация, побуждение, принуждение, маскировка информации. Средства защиты информации включают: формальные (технические, программные), неформальные (организационные, законодательные, морально-этические) [1]. Уровни защиты информации могут быть: аппаратно-программные; процедурный; административный; законодательный. Компоненты организации системы защиты: область физической безопасности; безопасность персонала, правовая безопасность; безопасность оборудования; безопасность программного обеспечения; безопасность телекоммуникационной среды. Организационные меры защиты определяют порядок: ведения системы защиты от несанкционированного доступа; ограничения доступа в помещения; назначения полномочий по доступу; контроля и учета событий; сопровождения ПО; контроля за системой защиты. Управление доступом - метод защиты информации регулированием использования всех ресурсов системы, включающий функции: идентификация ресурсов системы; установление подлинности объектов; проверка полномочий; разрешение и создание условий; регистрация обращений к защищаемым ресурсам; реагирование при попытках несанкционированных действий Внедрение системы защиты информации проходит этапы: решение и концепция, проект системы, внедрение, поддержание, санкции. Это: инженерно-техническое обследование и описание информационных ресурсов системы; определение наиболее критичных, мест системы; вероятностная оценка угроз безопасности информационным ресурсам; экономическая оценка возможного ущерба; стоимостной анализ возможных методов и средств защиты информации; определение рентабельности применения системы защиты информации. С точки зрения ПО данные должны быть защищены от: потери (резервное копирование); недействительный доступ (зашифровать, ограничить доступ); недействительная модификация (электронная подпись). Различают два основных способа шифрования: симметричное шифрование – с закрытым ключом; ассиметричное шифрование – с открытым ключом. Вместе с традиционными средствами защиты корпоративных систем: антивирусы, детекторы уязвимостей, межсетевые экраны и детекторы вторжений, применяются средства автоматизации защиты, включающие корреляторы событий, программы обновлений, средства аутентификации, авторизации и администрирования, системы управления рисками.

II. Интеллектуальные средства защиты информации

Интеллектуальные системы защиты информации (ИСЗИ) посвящены системам обнаружения атак, в качестве интеллектуального инструмента в которых используются нейронные сети, системы нечеткой логики и основанные на правилах экспертные системы. Схемы обнаружения атак включают в себя обнаружение злоупотреблений и аномалий [2]. В ИСЗИ экспертные системы в базе содержат описание классификационных правил, соответствующим профилям легальных пользователей и сценариям атак га ИС. Недостатки ИСЗИ на базе ЭС: система не является адаптивной; не всегда обнаруживаются неизвестные атаки [2]. Если НС представлена в виде отдельной системы обнаружения атак, при обработке трафика происходит анализ информации на наличие злоупотреблений. Случаи с указанием на атаку перенаправляются к администратору безопасности. Подход быстродейст-вующий, поскольку используется один уровень анализа. Одним из основных недостатков нейронной сети является "непрозрачность"формирования результатов анализа. В системах обнаружения атак можно выделить применение нейронных сетей, дополненных ЭС. Чувствительность системы возрастает, так как экспертная система получает данные только о событиях, которые рассматриваются в качестве подозрительных. Если нейронная сеть за счет обучения стала идентифицировать новые атаки, то экспертную систему следует обновить. [3]. Использование гибридных нейро-экспертных или нейро-нечетких систем позволяет отразить в. структуре системы нечеткие предикатные правила, которые автоматически корректируются в процессе обучения нейронной сети. Свойство адаптивности нечетких нейронных сетей позволяет решать отдельно взятые задачи идентификации угроз, сопоставления поведения пользователей с имеющимися в системе шаблонами, автоматически формировать новые правила при изменении поля угроз [3].

III. Интеллектуальные агенты в защите информации

Технологии семантик Вэб позволяют воспринимать информацию в Web интеллектуальными агентами и осуществлять обработку данных. Интеллектуальный агент это запрограммированная пользователем программа на выполнение в сети задач [4]. Интеллектуальные агенты позволяют выполнять: поиск по нескольким критериям; сбор, анализ, обработка данных; обмен с другими агентами данными и онтологиями; способность самообучаться. Онтологии это метаданные, описывающие семантическую семантическую структуру предметной области. Новым направлением в ИСЗИ является использование интеллектуальных агентов, работающих в распределенной ИС и запрограммированных на поиск, как вторжения, так и аномалий [5,6]. 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 [5]. Рассматривается использование мультиагентных систем ЗИ [6]. 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 СОА; 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 включает в себя множество взаимодействующих интеллектуальных агентов, выделенные типовые компоненты информационной системы (ИС), источники сведений, подлежащих анализу для задачи обнаружения атак Предложена структура агентов, включающая модули управления, получения и обработки данных, их анализа, обучения, реакции, генерации сообщения, принятия решения. Описываются функции модулей. Методика работы с разработанной многоагентной СОА включает шаги; размещение агентов по блокам ИС; сбор данных, формирование обучающей выборки, обнаружение атак, сообщение об этом администратору.

IV. Список литературы

1. Черкасова, Ю. М. Защита информации в автоматизированных информационных технологиях управления. В кн. Информационные технологии управления / Ю. М. Черкасова. – М.: Дело, 2011. – С. 215–274.
2. Нестерук, Г. Ф. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов / Г. Ф. Нестерук, Л. Г. Осовецкий, А. Ф. Харченко. – СПб.: СПбГУЭФ, 2003. – 125 с.
3. Калач, А. М. Интеллектуальные средства и моделирование систем защиты информации / А. М. Калач, Е. С. Немтина // Интернет-журнал "Технологии техносферной безопасности"(http://ipb.mos.ru/ttb) – 2011. – № 3. – С. 3–11.
4. Вишняков, В. А. Модели и средства интеграции приложений, маркетинга, аутсорсинга, обработки знаний в компьютерных сетях: монография / В. А. Вишняков, Д. С. Бородаенко, Ю. В. Бородаенко. – Минск: МИУ, 2011. – 350с. 25.01.2006.
5. Вишняков, В. А. Обзор и анализ интеллектуальных средств защиты информации / В. А. Вишняков // Тез.докл.XI Белорусско–Российской НТК "Технические средства защиты информации". – Минск.: БГУИР, 2013. – С. 96.
6. Никишова, А. В. Принципы функционирования многоагентной системы обнаружения атак / А. В. Никишова // Известия ЮФУ. Технические науки. Тематический выпуск. «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2012. – № 12. – С. 28–33.