УДК 681.5:004(07)

НАПРАВЛЕНИЕ ИНТЕЛЛЕКТУАЛЬНОСТИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.А. АПАНАСЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
mjdel@tut.by

В последнее время в области информационной безопасности начали активна развиваться интеллектуальные средства защиты информации. Такие как интеллектуальные агенты, искусственные нейронные сети, искусственные иммунные системы. Это обусловлено тем, что за последнее десятилетий прогрессивна, развиваются различные способы атак и вторжений в информационные системы, а с учетом их большое разнообразие невозможно оперативно и адекватно реагировать на эти атаки. Но интеллектуальные системы защиты информации могут изменить эту ситуацию.

Ключевые слова: интеллектуальные агенты, искусственные нейронные сети, искусственные иммунные системы, аномалии, атаки.

В последнее время большой проблемой стало увеличившееся количество вирусов, и хакерских атак на информационные ресурсы, банковские систему и т.д.

С каждым днем появляются новые виды атак на информационные ресурсы. В связи с этим возникает большая проблема: пока будет распознан данная атака, проанализирована, приняты адекватные меры по ее отражению, выпущены соответствующие обновления для ПО, проходит приличное количество времени, на протяжении которого информационные ресурсы не защищены и подвержены угрозам. По этому в сфере информационной безопасности нужно переходить к интеллектуальным средствам защиты информации.

Под интеллектуальными средствами защиты информации понимают такие средства, которые на основе своего опыта или имеющихся знаний, могут самостоятельно принять решение является ли данная ситуация аномальной или нет.

К ним относятся интеллектуальные агенты, нейронные сети, искусственные иммунные системы и др. Одни из них применятся на этапе обнаружения угрозы, другие на этапах анализа и нейтрализации угрозы. Поэтому эти средства нужно применять комплексно.

В отличие от статических средств защиты интеллектуальные, способны принимать самостоятельно решение, есть ли сейчас угроза, и если она есть находить тут же адекватные меры.

Любой интеллектуальный агент представляет собой открытую систему, помещенную в некоторую среду, причем эта система обладает собственным поведением, удовлетворяющим некоторым экстремальным принципам. Таким образом, интеллектуальный агент считается способным воспринимать информацию из внешней среды с ограниченным разрешением, обрабатывать ее на основе собственных ресурсов, взаимодействовать с другими агентами и действовать на среду в течение некоторого времени, преследуя свои собственные цели. Другими словами интеллектуальных агентов можно представить как сеть, в которой каждый агент отвечает за свою «территорию», при это при обнаружении аномалии, сообщает о ней другим агентам сети. Что позволяет оперативно и адекватно реагировать всей системе на атаки злоумышленников или вирусов.

Нейронные сети – класс аналитических методов, построенных на (гипотетических) принципах обучения мыслящих существ и функционирования мозга и позволяющих прогнозировать значения некоторых переменных в новых наблюдениях по данным других наблюдений (для этих же или других переменных) после прохождения этапа, так называемого обучения на имеющихся данных.

Основные преимущества и достоинства нейронных сетей перед традиционными вычислительными системами.

1. Решение задач при неизвестных закономерностях
2. Устойчивость к шумам во входных данных
3. Адаптированные к изменениям окружающей среды
4. Потенциальное сверхвысокое быстродействие
5. Отказоустойчивость при аппаратной реализации нейронной сети

Основным недостатком нейронных сетей является узкий диапазон применения, она может, эффективна, работать только после прохождения обучения нахождения определённого класса атак. Нейронные сити лучше всего использовать на этапах обнаружения, квалификации аномалий и нахождения способов ее нейтрализации.

Искусственная иммунная система (ИИС) – это адаптивная вычислительная система, использующая модели, принципы, механизмы и функции, описанные в теоретической иммунологии, которые применяются для решения прикладных задач.

Иммунная система представляет большой интерес как система, способная эффективно обрабатывать значительные объемы данных. В частности, она выполняет большой объем сложных высокопараллельных распределенных вычислений. Поведение иммунной системы в целом определяется всей совокупностью локальных взаимодействий.

Основные достоинства ИИС:

1. Наличие большого числа детекторов приводит к отказоустойчивости и надежности системы. Отсутствие единой точки отказа.

2. При увеличении количества узлов среды распределенных вычислений в предложенной системе повышается уровень защищенности.

3. Все столкновения детекторов с вредоносными объектами заносятся в память. Это позволяет проводить обучение детекторов.

Основные недостатки:

1. Возможна аутоиммунная реакция.

2. Возможен иммунодефицит, особенно при малом количестве узлов среды распределенных вычислений.

ИИС эффективна, использовать на этапе обнаружения и выявления аномалий и атак злоумышленников. Таким образом, можно сделать вывод, что в современном мире нужно создавать глубоко эшелонирование, интеллектуальные системы защиты информации, которые смогут адекватна реагировать и защищать информационные ресурсы от несанкционированного доступа, атак злоумышленников, а так же вредоносного ПО и вирусов.

Список литературы

1. *Васильев В.И.* Интеллектуальные системы защиты информации. «Машиностроение». М., 2013.

2 Гвозденко А. Искусственные иммунные системы как средства сетевой самозащиты [Электронный ресурс]. – Режим доступа: http://itc.ua/node/4270/

3. *Рутковский Л.* Методы и технологии искусственного интеллекта: пер. с польск. – М.: Горячая Линия-Телеком, 2010.