УДК 004.056.5

АНАЛИЗ ИНТЕЛЛЕКТУАЛЬНЫХ АЛГОРИТМОВ И ВЫБОР НАИБОЛЕЕ РАЦИОНАЛЬНОГО ПРИ СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ.

С.В.Михальченко

студентка института приоритетных технологий кафедры информационной безопасности

Волгоградский государственный университет

lana.mixalchenko@yandex.ru

Аннтотация: В последнее время все чаще наблюдается тенденция роста количества угроз, совершенных злоумышленниками. Так, согласно статистике индекса уровня нарушения (BREACH LEVEL INDEX), в 2016 году было зафиксировано 707 миллионов нарушения записей, а в 2017 уровень возрос до 1,378 миллиарда нарушений, что на 86% больше, чем в прошлом году. Чтобы огородить себя от таких угроз различают два принципиально разных метода обнаружения: метод сигнатурного анализа (основан на том, что все угрозы уже известны и их можно отследить) и метод обнаружения аномальных отклонений. Метод обнаружения аномалий больше подходит для всесторонней защиты информационной системы. Но в последнее время наблюдается тенденция роста атак с использованием методов интеллектуального анализа данных. Такие методы более быстро реализуют атаки и считывают данные. Они могут выполняться с помощью систем искусственного интеллекта. Несмотря на то, что данные методы часто используются при нарушении информационной безопасности, они также могут служить и для защиты информации. В данной статье рассматриваются различные алгоритмы систем искусственного интеллекта, для выбора наиболее рациональных при реализации системы защиты.

Ключевые слова: информационная безопасность, метод обнаружения аномальных отклонений, СИИ, генетические алгоритмы, экспертные системы, искусственные иммунные системы, искусственные нейронные сети.

ANALYSIS OF INTELLECTUAL ALGORITHMS AND CHOICA THE MOST RATIONAL TO CREATE SYSTEM OF THE INFORMATION SECURITY

S.V.Mikhalchenko

Student of the Institute of Priority Technologies of the Information Security Department

Volgograd State University

lana.mixalchenko@yandex.ru

Annotation: Recently, there has been an increasing trend in the number of threats made by hackers. Thus, according to statistics of the violation level index (BREACH LEVEL INDEX), in

2016 707 million records were recorded, and in 2017 the level increased to 1.378 billion violations, which is 86% more than last year. In order to fence oneself from such threats, two fundamentally different detection methods are distinguished: a signature analysis method (based on the fact that all threats are already known and can be traced) and an anomalous deviation detection method. Anomaly detection method is more suitable for comprehensive protection of an information system. But lately there has been a growing trend of attacks using data mining methods. Such methods more quickly implement attacks and read data. They can be performed using artificial intelligence systems. Despite the fact that these methods are often used in violation of information security, they can also serve to protect information. This article discusses the various algorithms of artificial intelligence systems, to select the most rational when implementing a protection system.

Key words: information security, method of control of anomalous deviations, SII, genetic algorithms, expert systems, artificial immune systems, artificial neural networks.

Под СИИ понимается техническая или программная система, выполненная на базе ЭВМ, которая способна решать задачи, не подлежащие алгоритмизации, требующие принятия каких-либо «осмысленных» решений.

В настоящее время, существует большое количество СИИ, из них можно выделить [3]:

1. Генетические алгоритмы.
2. Экспертные системы.
3. Искусственные иммунные системы.
4. Искусственные нейронные сети.

Генетические алгоритмы

В основе генетических алгоритмов лежит взятый у природы принцип выживания более приспособленных особей. Этот алгоритм используется в задачах на оптимизацию, составление расписаний, настройка и обучение нейронной сети и во многих других.

Принцип действия алгоритма:

1) Инициализация или выбор исходной популяции хромосом, где популяцией считается набор всех пробных решений, а хромосомой – одно решение. Происходит случайный выбор хромосом, которые представляются в двоичном виде.

2) Оценка приспособленности хромосом в популяции. Здесь составляется и рассчитывается функция приспособленности.

3) Проверка условия остановки алгоритма. Зависит от того, где применяется алгоритм, от того приводит ли его выполнение к каким-то результатам, и от сколько времени прошло. Если остановка выполнена, то переход к 7 шагу. Если не выполнена, то следующий шаг.

4) Селекция хромосом. Происходят выборка тех хромосом, которые будут участвовать в создание потомков для следующей популяции. Здесь отбираются значения самых больших функций приспособленности.

5) Применение генетических операторов. Операторы бывают двух видов: скрещивания или мутации. При скрещивании пары хромосом, случайным образом определяется, из каких генов состоит потомок (первого родителя или второго). При мутации изменяется значение гена на противоположное.

6) Формирование новых хромосом. Повторяется шаг 3-4, пока не будет сгенерировано новое поколение.

7) Выбор наилучшей хромосомы. Если выполнен шаг 3, то выводится хромосома с наибольшей функцией приспособленности.

Экспертные системы

Экспертные системы (ЭС) – вычислительные системы, которые моделируют процесс принятия решений экспертом в какой-либо предметной области.

ЭС нужны для того, чтобы решать задачи в некоторых областях, где база знаний высококвалифицированного специалиста играет важную роль. Области применения: медицинская диагностика, прогнозирование, планирования, диагностики неисправностей разного вида устройств, мониторинг.

Общая структура ЭС приведена на рисунке 2 [7]:

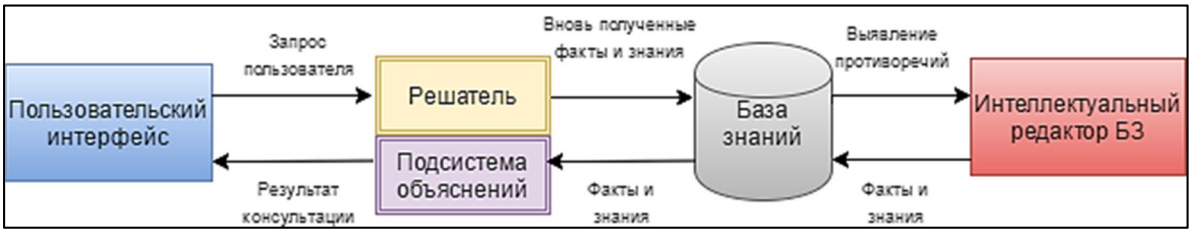

Рисунок 2 – Структура ЭС

Но это лишь обобщенная структура, в реальности модулей намного больше, это лишь обязательные элементы.

Классификация ЭС:

1. По способу формирования решения: анализирующие и синтезирующие. Здесь осуществляется выбор решения из множества известных решений на основе анализа знаний или решения синтезируется из отдельных фрагментов знаний.

2. По способу учета временного признака: статические и динамические. Первые предназначены для решения задач с неизменяемыми в процессе решения данными и знаниями, а динамические разрешают такие изменения.

3. По видам используемых данных и знаний: детерминированные и с неопределенными знаниями.

4. По числу используемых источников решения знаний: с одним или несколько.

Недостатками ЭС считается:

1) Сложность формализации знаний экспертов.

2) *Неспособность дать объяснения своему решению, ЭС описывает лишь шаги в процессе поиска решения.

3) Сложная отладка и тестирование ЭС.

Но не смотря на эти недостатки, все равно ЭС доказала свою эффективность во многих областях.

Искусственные иммунные системы

Искусственные иммунные системы (ИИС) - это адаптивная вычислительная система, использующая модели, принципы, механизмы и функции, описанные в теоретической иммунологии, которые применяются для решения прикладных задач [1].

ИИС успешно применяются для решения таких задач как: оптимизация, классификация, применимы для сжатия информации, кластеризации, машинного обучения, распознание образов.

ИИС основывается на модели, взятой из иммунологии, которая называется «свой-чужой», когда в организме антигены распознаются как «чужие», потом классифицируется, а после лимфоциты синтезируют антитела для борьбы с ними. После разрушения или нейтрализации часть антител остается в организме для того, чтобы при повторной атаке, организм быстрее среагировал.

Модели на основе функционирования иммунитета применяются в область информационной безопасности, например:

— Обнаружение вирусов. Используется алгоритм отрицательного отбора. Он легко обнаруживает изменения в зараженных файлах. Но он имеет ограниченное применение — он предназначен только для защиты постоянных файлов данных или программ.

— Мониторинг процессов в системе UNIX. Используется всё тот же алгоритм. Обнаруживать источники аномальной активности позволяют короткие последовательности вызовов системы.

— Альтернативный метод обнаружения вирусов. Суть состоит в том, что программа обнаружения вирусов непрерывно сканирует программное обеспечение на наличие признаков вирусной инфекции. Процесс выявления таких признаков включает запуск программ-приманок, единственной целью активности которых является их инфицирование вирусом.

Искусственные нейронные сети

Искусственные нейронные сети (НС) – один из многочисленных видов искусственного интеллекта. Они созданы по упрощенной модели биологических нейронных сетей [2].

Интерес в исследование НС велик, потому что спектр решаемых ими задач различен. С помощью НС можно распознавать текст, части изображения, считать приближенные уравнения, прогнозировать завтрашнюю цену акций на финансовом рынке и многое другое.

Но не каждую задачу можно решить с помощью НС. Должна быть известна некоторая определенная информация, с помощью которой можно узнать неизвестную информацию. Также, нужно знать множество входных и выходных величин, и как они связаны друг с другом.

Важным этапом является обучение нейронной сети. Обучение бывает с учителем и без.

При обучении с учителем НС показывается выборка обучающих примеров. Каждый образец подается на входы сети, затем проходит обработку внутри структуры НС, вычисляется выходной сигнал сети. Затем по определенному правилу вычисляется ошибка, и происходит изменение весовых коэффициентов связей внутри сети в зависимости от выбранного алгоритма. И так делается до того, как коэффициент достигнет приемлемого значения.

При обучении без учителя обучающий алгоритм выстраивает значения весов сети так, чтобы они были оптимальными.

Алгоритмов обучения достаточно много, принципиальная разница между ними состоит в том, какой виды НС применяется: однослойные или многослойные.

Для того, чтобы выбрать определенную область СИИ, необходимо их сравнить между собой. В таблице 1 представлен сравнительный анализ СИИ:

Таблица 1 – Анализ видов СИИ

Название СИИ	Необходимость обучения	Сложность функционирования	Решаемые задачи

Генетические алгоритмы	нет	низкая	- Оптимизация;
Экспертные системы	да	средняя	- Прогнозирование; - Оптимизация.
Искусственные иммунные системы	да	высокая	- Оптимизация; - Распознавание образов; - Классификация.
Искусственная нейронная сеть	Да	средняя	- Оптимизация; - Распознавание образов; - Прогнозирование; - Классификация.

Исходя из того, что НС обладает наилучшим набором критериев, а также способна решать наибольшее количество задач, было выбрано именно это перспективное направление.

Литература

1. Чернышев Ю.О., Венцов Н.Н., Григорьев Г.В. Искусственные иммунные системы: обзор и современное состояние //Международный журнал "Программные продукты и системы" № 4 2014 год. [136-142]с.
2. Д.В.Смолин Введение в искусственный интеллект: конспект лекций. – М.: ФИЗМАТЛИТ, 2004. – [138]с
3. Михальченко С.В. Исследование программ интеллектуального анализа событий информационной системы // Международный студенческий научный вестник. – 2018. – № 1.; [Электронный ресурс] Режим доступа: свободный. URL: http://www.eduherald.ru/ru/article/view?id=18110 (дата обращения: 15.05.2018).
4. Breach level index [Электронный ресурс] Режим доступа: свободный. http://breachlevelindex.com/ (дата обращения 23.09.18)
5. Threats Report April 2017 [Электронный ресурс] Режим доступа: свободный. https://www.mcafee.com/ru/resources/reports/rp-quarterly-threats-mar-2017.pdf (дата обращения 26.09.18)