УДК 004.056.5

ИССЛЕДОВАНИЕ ПРОГРАММ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

С.В.Михальченко

студентка института приоритетных технологий кафедры информационной безопасности

Волгоградский государственный университет

lana.mixalchenko@yandex.ru

Аннотация: Для обеспечения защиты информационной системы требуется постоянно анализировать события, происходящие в ней, чтобы обнаруживать попытки реализации атак и вовремя среагировать. Согласно статистике, постоянно появляются новые виды атак на информационные системы, такие атаки невозможно выявить с помощью обычного антивирусного программного обеспечения и других видов защиты на основе сигнатурного метода. Поэтому рационально использовать специальный методы обнаружения аномалий, к их числу относят и интеллектуальный анализ. Он анализирует события, происходящие в информационной системе с помощью нейронных сетей, позволяя обнаруживать новые виды атак. В статье проанализировано пять программ интеллектуального анализа событий информационной системы, использующие нейронные сети: STATISTICA Automated Neural Networks, Deductor Studio, Neural network toolbox, MemBrain Neural Network, Neuro Solutions и сформулированы критерии для их оценки. Разработано программное средство, позволяющее производить автоматизированный расчет обобщенной оценки программ анализа. Проведены экспериментальные исследования, в ходе которых определена наиболее рациональная программа интеллектуального анализа событий информационной системы.

Ключевые слова*:* информационная безопасность, интеллектуальный анализ, нейронные сети, STATISTICA Automated Neural Networks, Deductor Studio, Neural network toolbox, MemBrain Neural Network, Neuro Solutions.

RESEARCH MINING PROGRAMS OF INFORMATION SYSTEM

S. V. Mikhalchenko

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

Volgograd state University

lana.mixalchenko@yandex.ru

Annotation: o ensure the protection of information systems, it is required to constantly analyze its events to detect attempts to implement attacks. According to statistics, there are always new types of attacks on information systems, such attacks can not be detected using conventional anti-virus software and other types of protection based on the signature method. Therefore, it is rational to use special methods for detecting anomalies, including intellectual analysis. He analyzes the events occurring in the information system with the help of neural networks,

allowing to detect new types of attacks. Programs of mining of information system's events are analyzed and the criteria for their evaluation are formulated. Software tool that allows you to produce automated calculation of the generalized evaluation of programs of analysis is developed. Experimental studies in which we determined the most rational program of intelligent analysis of information system's events are carried out.

Key words: information security, mining, neural networks, STATISTICA Automated Neural Networks, Deductor Studio, Neural network toolbox, MemBrain Neural Network, Neuro Solutions.

По статистике количество образцов новых атак, совершаемых на системы, постоянно растет.

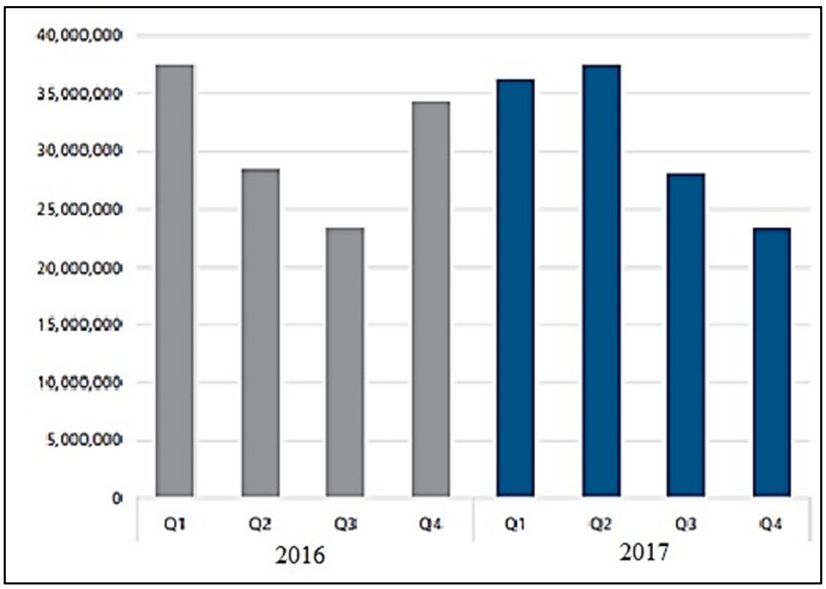

Рис. 1 – Количество новых типов атак за 2015-2016гг

Неспособность обнаруживать новые образцы атак – недостаток современных систем обнаружения атак. Чтобы устранить данный недостаток внедряются интеллектуальные подходы к анализу данных для обнаружения атак.

Под интеллектуальным анализом будем понимать анализ с использованием систем искусственного интеллекта. В настоящее время, существует большое количество СИИ, из них можно выделить:

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

Для того, чтобы выбрать определенную область систем искусственного интеллекта, необходимо их сравнить между собой. В таблице 1 представлен сравнительный анализ систем искусственного интеллекта (СИИ), произведенный на основе экспертной оценки:

Таблица 1

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 нейронная сеть обладают наилучшим набором критериев, исходя из спектра решаемости задач и сложности функционирования для дальнейшей реализации было выбрано именно это направление в системах искусственного интеллекта.

Ввиду этого актуальным является выбор наиболее рациональной программы интеллектуального анализа событий информационной системы (ИС) с помощью нейронных сетей [1, С.162].

Существует множество программ для интеллектуального анализа событий ИС, но здесь будет рассмотрено 5 программ, наиболее функциональных и популярных:

1. STATISTICA Automated Neural Networks (SANN) - программный пакет для создания и обучения нейронных сетей, который решает большой спектр задач [2, С. 168].
2. Deductor Studio – аналитическая платформа, которая позволяет на базе единой архитектуры пройти все этапы построения аналитической системы: от консолидации данных до построения моделей и визуализации полученных результатов [3, С. 37].
3. Neural network toolbox (NNTool) – пакет расширения MATLAB, содержащий средства для проектирования, моделирования, разработки и визуализации нейронных сетей [2, С. 169].
4. MemBrain Neural Network – представляет собой мощный графический редактор и симулятор нейронных сетей, поддерживающий нейронные сети различных архитектур любого размера.
5. Neuro Solutions - сверхсовременный программный пакет совмещает модульный, с иконным представлением, интерфейс разработки нейронной сети, с реализацией усовершенствованных процедур обучения [5].

Чтобы оценить качество выделенных программ были сформулированы критерии для их оценки [4]:

— Скорость обучения (К1) – определяет время, затрачиваемое на расчет величин весов связей между нейронами, отвечающих требованиям точности;

— Понятный графический интерфейс (К2) – наличие удобного и интуитивно понятного пользователю интерфейса;

— Наглядность информации (К3) – наличие возможности графического представления информации по окончанию обучения и моделирования нейронной сети (НС);

— Реализация основных видов НС и алгоритмов обучения (К4) – возможность реализация как можно большего количества стандартных видов НС и алгоритмов их обучения;

— Создание своих структур НС (К5) – возможность создания собственных структур НС, позволяющих указывать такие параметры как: тип сети, количества, размера скрытых слоев и т.д.;

— Использование собственных алгоритмов (К6) – возможность подключения собственных алгоритмов обучения в виде программных модулей;

— Автоматизированное формирование НС (К7) – возможность подбора наилучших параметров автоматически, что облегчает использование такой программы;

— Процедура импорта результатов (К8) –возможность сохранять результаты в различные файлы и передавать их в приложения;

— Генератор исходного кода (К9) – возможность сгенерировать исходный программный код нейросетевых моделей на различных языках программирования;

— Взаимосвязь (корреляция) событий (К10) – возможность учитывать то, как события связаны между собой. Если в пакете предусмотрено такая функция, то это позволяет обнаруживать атаки, которые состоят из нескольких шагов.

В таблице 2 приведены качественные значения критериев для выделенных программ.

Таблица 2

Нейросетевые программы	Критерии оценки									
	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10
STATISTICA Automated Neural Networks	высокая	да	средняя	высокая	да	да	да	средняя	да	да

Deductor Studio	высокая	да	высокая	средняя	нет	нет	нет	высокая	нет	да
Neural network toolbox	низкая	нет	низкая	средняя	нет	нет	нет	низкая	нет	да
MemBrain Neural Network	высокая	нет	низкая	низкая	да	да	да	средняя	да	нет
Neuro Solutions	средняя	нет	средняя	средняя	да	да	нет	средняя	да	нет

Так как ни одна из программ не обладает наилучшим набором значений критериев, необходимо разработать программное средство для автоматизации выбора наиболее рациональной программы интеллектуального анализа событий информационной системы.

Для этого нужно разработать математическую модель, реализующую эту оценку.

Сформируем вектор критериев $K = (K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8, K_9, K_{10})$, где критерии принимают следующие значения:

$$K_{1,3,4,8} = \begin{cases} 0, \text{низкая} \\ 0.5, \text{средняя} \\ 1, \text{высокая} \end{cases}$$

$$K_{2,5,6,7,9,10} = \begin{cases} 0, \text{нет} \\ 1, \text{да} \end{cases}$$

Существует наилучший вектор K^*, в котором все значения критериев соответствуют максимальным значениям. Для всех критериев это значение 1.

$$K^* = (1, 1, 1, 1, 1, 1,1,1,1,1).$$

Для оценки качества нейросетвых пакетов вводится скалярная величина, равная Эвклидовому расстоянию между наилучшим вектором и вектором критериев, полученным для i-го оцениваемого метода:

$$K^i = (K_1^i, K_2^i, K_3^i, K_4^i, K_5^i, K_6^i, K_7^i, K_8^i, K_9^i, K_{10}^i)$$

Эвклидово расстояние рассчитывается по формуле (1).

$$P^i = \sqrt{\sum_{j=1}^{10} (K_j^* - K_j^i)^2}\,. \qquad (1)$$

Нейросетевой пакет, для которого расстояние до наилучшего вектора окажется наименьшим, можно считать наиболее рациональным пакетом для работы с нейронными сетями.

Было проведено 5 экспериментов, в результате которых получены следующие значения обобщенных оценок для каждого нейросетевого пакета, представленные на рис. 1:

1. STATISTICA Automated Neural Networks 0,7071067811865;

2. Deductor Studio - 2,0615528128088;

3. Neural network toolbox - 2,8722813232690;

4. MemBrain Neural Network - 2,0615528128088;

5. Neuro Solutions – 2.

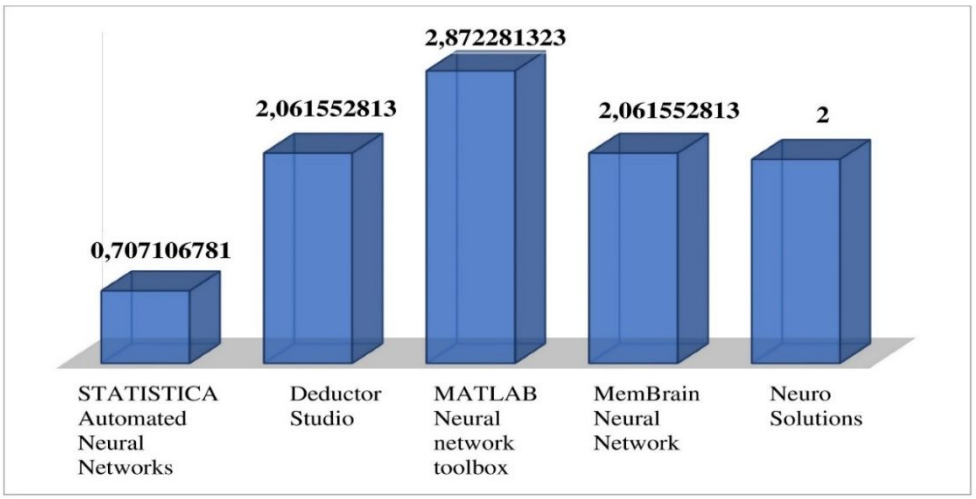

Рис. 2 – Обобщенные оценки нейросетевых пакетов

Сравнив полученные результаты, можно прийти к выводу, что наиболее рациональной программой является STATISTICA Automated Neural Networks. У этой программы значения критерия 4 «Реализация основных видов НС и алгоритмов обучения» и критерия 7 «Наличие автоматизированной НС» имеют наивысшие показатели, среди всех анализируемых программ.

Литература

1. Варлатая С.К. Кирьяненко А.В. Анализ угроз нарушения информационной безопасности информационных систем, существующие Модели и методы противодействия компьютерным атакам. // Актуальные проблемы технических наук в России и за рубежом / Сборник научных трудов по итогам международной научно-практической конференции. № 2. -Новосибирск, 2015. 162 с.

2. А.Я.Туровский, Сравнительный анализ программных пакетов для работы с искусственными нейронными сетями/ Я. А. Туровский, С. Д. Кургалин, А. А. Адаменко// Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. -2016. -№ 1. -С. 161-168.

3. А. Н. Никулин, И. В. Чернышев Аналитическая платформа «Дедуктор» – применение в информационных системах экономики: методические указания – Ульяновск : УлГТУ, 2012. – 37 с.

4. Д.Рутковская , М.Пилиньский , Л.Рутковский Нейронные сети, генетические алгоритмы и нечеткие системы перевод с польского И.Д.Рудинского - М.: -Горячая линия-Телеком – 2006г – [126-136]с.

5. Neuro Solutions [Электронный ресурс] Режим доступа: свободный. http://www.neurosolutions.com/ (дата обращения 23.01.18)