***Д.А.Котина, Т.И.Паюсова***
*Тюменский государственный университет, г.Тюмень*

**УДК 004.891.3**

# НЕЙРОСЕТЕВОЕ МОДЕЛИРОВАНИЕ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Аннотация.** В статье проводится анализ методического материала, который содержит лабораторные работы для студентов.

Методический материал предназначен для студентов информационной безопасности для оказания помощи в изучении материала и формировании экспериментальных умений, как теоретических, так и практических.

**Ключевые слова:** информационная безопасность, искусственные нейронные сети, нейросетевые архитектуры, нейросетевое моделирование, нейросеть, экспертные системы.

Современный мир движется к тому, что скоро невозможно будет обойтись без интеллектуальных систем информационной безопасности. Также стремительно растет и перечень задач информационной безопасности, решаемых с использованием интеллектуальных методов и средств.

Получается, что первой актуальной задачей в сфере информационной безопасности, которая использует методы и средства искусственного интеллекта, является обнаружение вторжений и атак на автоматизированные системы. Как показывает практика, достижение приемлемых уровней защиты информационных ресурсов от атак на систему не всегда возможна на основе существующих алгоритмов и программно-аппаратных решений. Современные же средства по обнаружению атак должны включать в себя, по крайней мере, в качестве составной части, интеллектуальные подсистемы. Основой же для этих подсистем являются искусственные нейронные сети и экспертные системы. [1]

Существуют и другие задачи информационной безопасности, которые могут эффективно решаться с помощью методов и средств искусственного

интеллекта. И так как нейросетевое моделирование до конца не изучено, а потребность в этом всё растет с каждым днем, нужно привлекать новых людей, а в частности студентов, для изучения данной темы. И для того, чтобы лучше разобраться в системе нейросетевого моделирования в информационной безопасности, было принято решение разработать методический комплекс и создать виртуальную лабораторию. Это поможет натолкнуть студентов на изучение нейронных сетей и, возможно, дальнейшее привлечение их к самостоятельному изучению и созданию новых интеллектуальных систем.

Также занятия по методическому комплексу и в лаборатории позволяют повысить активность и самостоятельность учебной работы студентов, улучшить восприятие учебного материала благодаря его мультимедийности, использовать внеаудиторное время для изучения конструкций в виде домашних заданий, облегчить процесс обучения и заинтересовать студентов.

**Применение искусственных нейронных сетей для решения задач ИБ**

Всё чаще для повышения информационной безопасности системы стали использовать искусственные нейронные сети, что является удобной основой для информационных моделей.

Нейронные сети сравнительно легко обучаются с помощью обучающих данных, которые представляют собой входные и приравнивающиеся к ним выходные данные. В свою очередь, сети учатся устанавливать связи между ними. Достаточно хорошо обученная сеть, сама в состоянии делать выводы на основе данных, и такую сеть можно использовать тогда, когда выходные значения неизвестны. В отличие от человека, нейросеть может научиться решать такие задачи, для которых нет теоретического обоснования, или же нет рабочих алгоритмов, то есть она имеет способность адаптироваться. [2]

Итак, перечислим основные задачи, доступные для решения методами искусственного интеллекта в сфере обеспечения информационной безопасности:

1) быстрое опознание сигнатур угроз;
2) ускорение поиска источников вредоносного воздействия и аномалий;
3) выявление дополнительных данных в процессе обучения, для дальнейшего построения на их основе более мощной системы защиты.

Данные задачи могут браться за основу при построении целостной системы защиты на основе искусственной нейронной сети или могут быть раздельно реализованы различными методами для оптимизации процесса разработки и внедрения.

Раздельная реализация различных методов позволяет безопасно включать в работу все новые и новые подключаемые модули, такие как:

- решаемые задачи;
- функции, графики которых строятся ядром программы;
- реализации различных алгоритмов генетического программирования;
- реализации различных представлений особей и операций скрещивания и мутации для алгоритмов генетического программирования;
- визуализаторы особей (автоматов) и управляемых ими объектов (они зависят от конкретной задачи и от конкретного представления особи).

**Структура лабораторных работ**

Для того чтобы методический комплекс приносил плоды, было принято решение разделить всё на этапы. Это было сделано с той целью, чтобы точно понять, что требуется как от самих лабораторных, так и от студентов. В результате это поможет правильно и без ошибок создать удобную виртуальную лабораторию.

Далее рассмотрим и опишем все этапы, которые надо пройти, чтобы точно выполнить поставленные задачи.

На первом этапе пользователь определяет задачу, с которой предстоит работать. Назовем этот этап этапом идентификации экспертных систем. Экспертная система — это программа, которая заменяет эксперта в той или иной области, по-простому говоря, это наш методический комплекс или наша лаборатория. Отсюда вытекает простой вывод – всё, что мы изучаем в курсе "Нейросетевое моделирование в ИБ ", ставит конечной целью разработку экспертной системы. [3]

Результатом данного этапа является ответ на вопрос, что надо сделать и какие ресурсы необходимо задействовать (идентификация задачи, определение участников процесса проектирования и их роли, выявление ресурсов и целей).

Выбор осуществляется исходя из задач и имеющегося набора данных:

- распознавание образов и классификация;
- принятие решений и управление;
- кластеризация;
- прогнозирование;
- аппроксимация;
- сжатие данных и ассоциативная память;
- анализ данных;
- оптимизация данных.

На втором этапе пользователь выбирает топологию будущей сети из списка, имеющегося методическом комплексе. Выбор должен основываться на том, будет ли сеть обучаться самостоятельно или с помощью набора выходных данных для сравнения.

Следует учесть классификацию нейросетей, которая является основой.

Для каждого типа сетей в лабораторной работе должны присутствовать готовые шаблоны, в которые уже включены алгоритмы обучения сети, с возможностью выбора алгоритма, если для данной топологии существует несколько применимых.

Также студент должен иметь возможность строить полностью пользовательские сети на основе описываемого вручную шаблона, содержащего основную информацию о типе связей, группировке нейронов, функциях вычисления и методике обучения.

На третьем этапе, который назовем этапом формализации, студент должен изучить и определить параметры, влияющие на обучение сети, такие как момент и скорость обучения, количество скрытых слоев, количество нейронов в слое, наличие нейронов смещения и другие, зависящие от указанных ранее параметров. [2]

Другими словами, этот этап нужен для определения средств и способов представления для того, чтобы определить какая будет готовая модель сети, в шаблонной или написанной схеме.

Сам перечень параметров должен быть включен в шаблон топологии сети. Часть параметров в лабораторных работах должна описываться статически, как например количество входных и выходных нейронов – исходя из количества и типа полей в СУБД. Эти параметры студент будет использовать, как необходимые и неизменяемые.

Четвертым этапом является построение сети, случайная инициализация весов связей нейронов и дальнейшее обучение на массиве предоставленных пользователем данных. На данном этапе также будет представлен готовый шаблон построения, который следует изучить студенту и использовать в дальнейшем.

Чтобы построить нейросетевую модель, следует производить отбор входных данных, который может повлиять на ожидаемый результат. Всё, что не будет относиться к предмету изучения, надо исключить. Также не стоит забывать, что для обучения искусственной нейронной сети должно быть необходимое количество примеров для обучения. За основу можно взять эмпирическое правило, которое описывает рекомендации соотношения обучающих примеров, то есть входных данных, и точные и правильные ответы нейронной сети.

В начале для обучающей выборки следует провести её анализ и также проанализировать как сами возможные изменения, так и их диапазон изменений.

И для того, чтобы перейти к обучению нейронной сети, описывается проектирование ее архитектуры (число слоев и число нейронов в каждом слое). Структура искусственной нейронной сети формируется до начала обучения, поэтому важно правильно, без ошибок, произвести проектирование.

В итоге студент должен произвести обучение сети. Существуют два подхода по обучению сети, это конструктивный и деструктивный подходы. И студент должен выбрать, какой же подход обучения ему приемлем.

Первый подход обучения искусственных нейронных сетей строится на том, что имеется сеть небольшого размера, которая постепенно увеличивается до нужных размеров, достигая требуемую точность по результатам тестирования. Второй же подход, деструктивный, основывается на том, что есть сеть с изначально избыточным объемом, и из неё начинают удалять лишние нейроны, а также примыкающие к ним связи. Деструктивный подход предоставляет хорошую возможность изучения влияния удаленных связей на точность сети. Уточняя весовые коэффициенты для отдаленных узлов, происходит процесс обучения сети, на основе постоянного увеличения входной и выходной информации.

Конечным этапом является проверка нейросети на новом наборе данных, размер которого должен соответствовать размеру конечной ошибки и быть для сети абсолютно новым. Данный этап можно назвать этапом тестирования.

В ходе данного этапа студент, по уже полученным знаниям, подбирает параметры, которые дают возможность проверить все возможности разработанной сети. То есть дается оценка выбранного способа представления знаний в экспертной системе.

Встречаются такие источники неудач в функционировании системы:

- тестовые примеры;
- ввод-вывод;

- правила вывода;
- управляющие стратегии.

Во время подготовки тестовых примеров их можно подразделять их по подзадачам предметной области, обозначая частые события, выясняя границы трудных случаев. Ввод-вывод характеризуется данными, полученными в процессе взаимодействия с пользователем, и выводами, вынесенными ЭС в ходе работы. Способы получения данных могут не давать ожидаемых результатов, так как, например, задавались некорректные вопросы или собранная информация недостаточна. Кроме того, вопросы системы могут быть трудными для понимания, многозначными и не соответствующими знаниям, которыми обладает студент.[4]

Выходные сообщения системы, по различным причинам, могут оказаться непонятны студенту. Например, их может быть чересчур много, или наоборот критически мало. Правило может являться ошибочным, если даже при правильном задании его условия и корректности действия нарушено соответствие между ними. Очередность рассмотрения данных ЭС не только влияет на эффективность работы системы, но и может привести к изменению финального результата.

**Выводы**

Использование искусственных нейронных сетей для повышения информационной безопасности важное, быстроразвивающееся и очень перспективное направление в сфере ИБ. Обеспечение наглядности и удобности восприятия информации студентами в процессе обучения в области нейронных сетей может обеспечить хороший темп развития данного направления за счет роста количества молодых специалистов.

## СПИСОК ЛИТЕРАТУРЫ

1. Брюхомицкий Ю.А. Нейросетевые модели для систем информационной безопасности. Учебное пособие. – Таганрог: Изд-во ТРТУ, 2005. – 160 с.

2. Савельев А.В. На пути к общей теории нейросетей. К вопросу о сложности. // Журнал Нейрокомпьютеры: разработка, применение№4-5,2006 г., с. 4
3. Тоискин В.С. Интеллектуальные информационные системы: Учебное пособие. Часть 1. – Ставрополь: Изд-во СГПИ, 2009. – 181 с.
4. Хайкин, Саймон. Нейронные сети: полный курс, 2-е издание. : Пер. с англ. — М. : Издательский дом “Вильямс”, 2006. — 1104 с.