DOI: 10.17117/na.2016.02.01.154

Поступила (Received): 21.02.2016

<http://ucom.ru/doc/na.2016.02.01.154.pdf>

Ефремова Е.В. Нейронные сети в информационной безопасности

Efremova E.V.
Neural network used in information security

В статье рассмотрены преимущества нейронных сетей для обеспечения информационной безопасности. Приведены особенности обучения данных систем и применения их на практике. Выявлены сложности, с которыми сталкивается пользователь на начальном этапе

Ключевые слова: нейронные сети, информационная безопасность, обучение нейронных сетей

The article describes the advantages of neural networks for information security. Author explores the peculiarities of training these systems and their application in practice. In addition, the difficulties of using revealed

Key words: neural network, information security, training of neural network

Ефремова Екатерина Владиславовна

Студент

Российский экономический университет им. Г.В.

Плеханова

г. Москва, Стремянный пер., 36

Efremova Ekaterina Vladislavovna

Student

Russian university of economics named G.V.

Plekhanov

Moscow, Stremyanny Lane, 36

Научный руководитель: доцент, канд. эконом. наук, Хачатурова С.С.

В истории исследований в области нейронных сетей, как и в истории любой другой науки, есть победы и неудачи. Значительный импульс ее развитию дал американский нейрофизиолог Френк Розенблатт, предложивший в 1962 году свою *кибермодель* нейронной сети. На протяжении вот уже более полувека было предложено очень много интересных разработок.

В XXI веке все цивилизованное мировое сообщество перешло на новый этап – этап информатизации. Компьютерные технологии с каждым днем развиваются все быстрее, внедряясь во многие сферы деятельности человека и становятся неотъемлемой частью практически всех профессий, они прочно входят в наш быт, образование и культуру [6]. Стремительное развитие информационных технологий требует от современного человека как высокого уровня теоретических знаний в данной сфере, так и умений применять инновационные открытия на практике. Профессиональная деятельность требует повышенного внимания, так как речь, как правило, идет о конфиденциальности информации и защите ценных цифровых данных.

Повышение уровня сложности и разнообразия данных технологий приводит к возникновению противоречий. Растущая необходимость защиты большого объема данных приводит к непрерывному поиску все новых средств и способов обеспечения максимально высокого уровня информационной безопасности. Одним из перспективных направлений в данном вопросе является исследование и оценка эффективности инновационных способов защиты.

Учеными и исследователями разработаны различные подходы к решению данной проблемы. Одним из подходов является применение искусственных нейронных сетей.

Искусственные нейронные сети построены по принципу функционирования биологических нейронных сетей. Многослойные сети способны нелинейно анализировать информацию, чем принципиально отличаются от общепринятых экспертных систем. Этим обусловлено расширение спектра возможностей защитной системы и, как следствие, рост востребованности. В отличие от необучаемых экспертных систем, нейронные сети получают способность давать оценку о соответствии информации, заложенной в базе данных и приходящей извне. В дальнейшем система становится обучаемой. Получая все новые и новые сигналы, сначала производится анализ на основе заложенных в программу критериев, затем происходит выделение скрытых закономерностей, и идентификация выходит на более новый уровень.

Суммируя вышесказанное, выделяют следующие преимущества применения искусственных нейронных сетей:

1. Быстрое распознавание угроз.
2. Оптимизация процесса поиска вредоносных источников.
3. Принятие во внимание тех сведений о системе, которые могут показаться несущественными неинтеллектуальной системе защиты.
4. Борьба с вредоносным ПО, которое так же является самообучающимся.
5. Вынесение определенных сведений в процессе обучения и построение на их основе более мощной системы защиты.
6. Обслуживание средств управления идентификацией и доступом к ресурсам и средств администрирования доступа.
7. Совершенствование современного антивирусного программного обеспечения.
8. Применение в средствах обнаружения атак.

Потенциальный пользователь обучающихся нейронных сетей понимает, что необходимо провести процесс обучения системы. Учеными разработаны ключевые схемы обучения нейросетей, однако до сих пор существуют сложности в их осуществлении.

Алгоритм обучения представляет собой следующую последовательность действий:

1. Поступление стимула из внешней среды.
2. Изменение свободных параметров нейронной сети.
3. Изменение внутренней структуры
4. Ответ на возбуждение, исходя из структурных изменений.

Важно понимать: не существует универсального алгоритма обучения, существует лишь набор различных средств. Каждый из них частично может отвечать требованиям той ли иной архитектуры нейронных сетей.

На сегодняшний день применение нейронных сетей в системах обнаружения атак является перспективным направлением, однако отсутствие четкого алгоритма обучения затрудняет широкомасштабное применение нейросетевых технологий в информационной безопасности.

Данная проблема будет рассмотрена автором настоящей работы в дальнейшем.

Список используемых источников:

1. Заенцев И.В. Нейронные сети: основные модели. М., 1999.
2. Крыжановский А.В. Применение искусственных нейронных сетей в системах обнаружения атак // Доклады ТУСУРа. 2008. № 2.
3. Слеповичев И.И., Ирматов П.В., Комарова М.С., Бежин А.А. Обнаружение DDoS атак нечеткой нейронной сетью // Известия Саратовского университета. 2009.
4. Калач А.В., Немтина Е.С. Интеллектуальные средства и моделирование систем защиты информации // Технологии техносферной безопасности. 2009. №3.
5. Михайлов А.С., Староверов Б.А. Проблемы и перспективы использования искусственных нейронных сетей для идентификации и диагностики технических объектов // Вестник Ивановского государственного энергетического университета им. В.И. Ленина. 2013.
6. Хачатурова С.С. Организация предпринимательской деятельности. Создание собственного дела. М.: РАЕ, 2012.