УДК 004.89

В.Ю. Бондарев, А.С. Сорокин, Е.Л. Кротова

V.Yu. Bondarev, A.S. Sorokin, E.L. Krotova

Пермский национальный исследовательский
политехнический университет

Perm National Research Polytechnic University

ИСКУССТВЕННАЯ НЕЙРОННАЯ СЕТЬ ДЛЯ ВЫЯВЛЕНИЯ ЗЛОУМЫШЛЕННИКА В АВТОМАТИЗИРОВАННОЙ РАБОЧЕЙ СИСТЕМЕ

ARTIFICIAL NEURAL NETWORK TO IDENTIFY THE ATTACKER IN AUTOMATEDOPERATING SYSTEM

Рассматривается один из способов решения задачи, связанной с поиском и выявлением злоумышленника в информационной среде. Обычно искусственная нейронная сеть используется для решения вопросов статистической классификации и оценивания. Она также может предсказывать действия посетителей, что мы и используем для решения поставленной проблемы.

Ключевые слова: искусственная нейронная сеть, нейроны, обучение и симулирование искусственной нейронной сети, статистическое оценивание, выявление злоумышленника.

This article discusses one way of solving the problem associated with the search and identification of the attacker in the information environment. Typically, an artificial neural network is used to solve problems of statistical classification and assessment, and the network can predict the actions of visitors, which we use to solve problems.

Keywords: artificial neural network, neurons, learning and simulation of artificial neural networks, statistical estimation, identification of the attacker**.**

Искусственная нейронная сеть (ИНС) представляет систему соединенных и взаимодействующих между собой искусственных нейронов (рис. 1) [1, 2]. Нейроны ищут сложную зависимость между входными и выходными данными, применяя которую ИНС может предсказать результат выходных данных. Для нахождения этой зависимости сеть обучается, и в процессе обучения находит коэффициенты связей между нейронами.

Искусственную нейронную сеть мы используем для выявления потенциальных злоумышленников [3]. Для этого нам нужны данные, в которых уже были определены клиенты, сделавшие или нет целевое действие. Исходя из этого, мы сможем искать злоумышленников среди посетителей сайта.

Допустим, у нас есть такие данные в виде бинарного потока, состоящего из множества 1 и 0, которое обозначает сигнатуру посетителя. Обозначим

поведение посетителей сайта следующим образом: 1 – сделал целевое действие, 0 – не сделал. Для выявления злоумышленника из большого количества клиентов мы построим нейронную сеть. Чтобы это реализовать, используем пакет MatLab и выберем тип сети, которая обучается с учителем. Мы выбираем обучение нейронной сети с учителем, потому что она предполагает, что для каждого входного вектора из обучающего множества существует требуемое значение выходного вектора, называемого целевым, что подходит для наших данных. Эти векторы образуют обучающую пару.

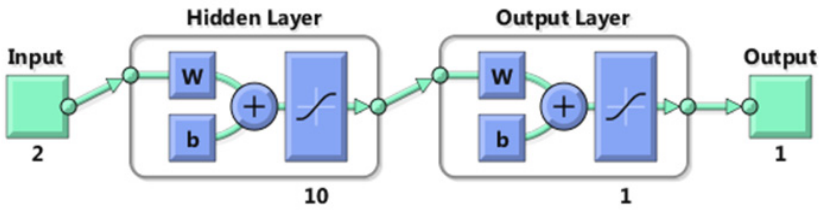

Рис. 1. Структура искусственной нейронной сети

Поскольку бинарный вектор посетителя очень длинный, берем, к примеру, первые 30 значений двоичного числа и находим корреляцию, т.е. статистическую взаимосвязь, между входными и выходными значениями. Для этого нам подойдет коэффициент Пирсона, где значения коэффициента больше. Те значения мы и возьмем на вход. Выбрав эти значения, обучаем сеть. Число нейронов подберем экспериментально, путем сравнения. Для начала возьмем 10 нейронов и посмотрим, как обучится сеть (рис. 2).

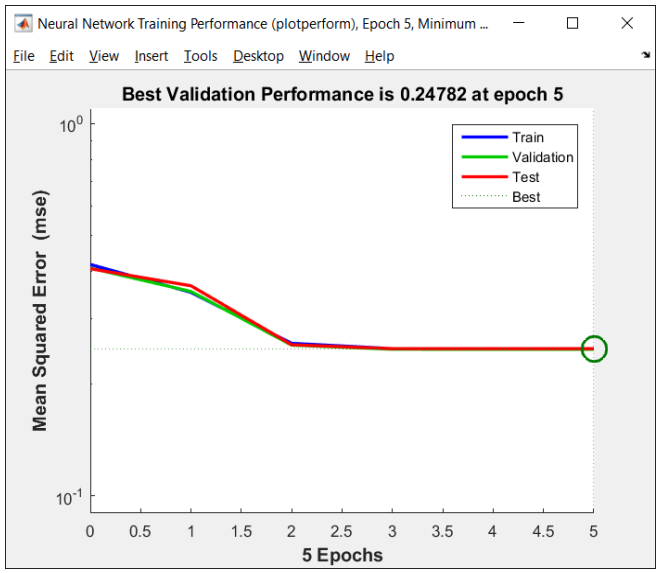

Рис. 2. Обучение нейронной сети с 10 нейронами во внешнем слое

Теперь рассмотрим, как ведет себя сеть при обучении с 50 нейронами (рис. 3).

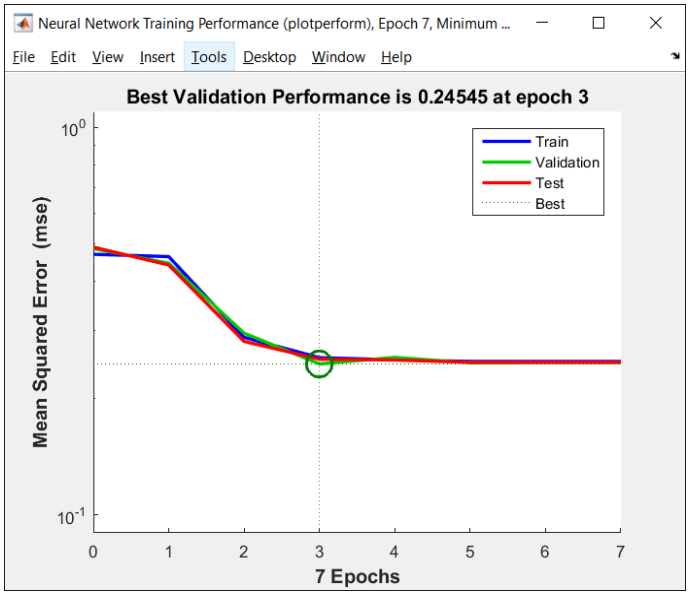

Рис. 3. Обучение нейронной сети с 50 нейронами во внешнем слое

Для третьего случая возьмем 250 нейронов (рис. 4).

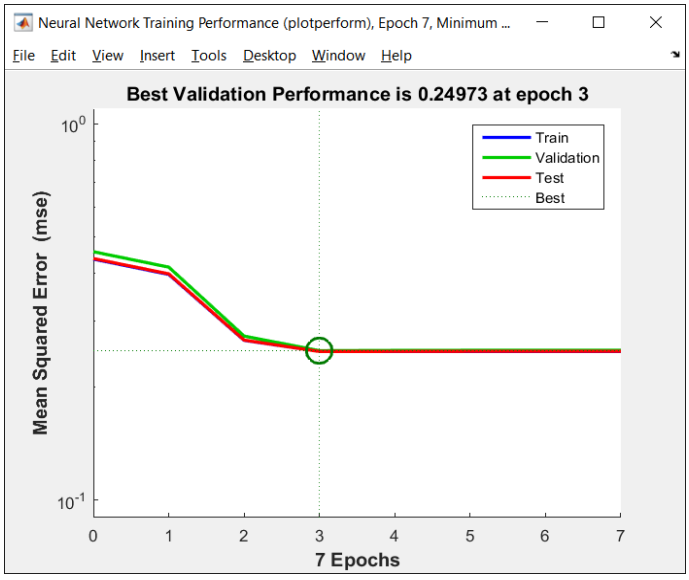

Рис. 4. Обучение нейронной сети с 250 нейронами во внешнем слое

Сравнив графики, мы увидим, что при 250 нейронах сеть обучилась лучше (линии практически совпадают друг с другом, более адекватны, чем у сети при обучении с 50 нейронами) и имеет наилучшую проверку с меньшей итерацией (по сравнению с сетью при обучении с 10 нейронами).

Проверим, пригодна ли наша сеть. Для этого возьмем другие похожие данные и найдем коэффициент искажения. Нейронная сеть будет пригодна для анализа данных, если коэффициент искажения будет не более 25 %. Для этого найдем отношение количества ошибок к количеству всех значений. После обработки полученных данных коэффициент искажения составляет 21,39 %. Значит, сеть обучилась правильно. Исходя из этого, можно сказать, что наша сеть пригодна для прогнозирования и статистической классификации. Благодаря этому прогнозу мы сможем выявить количество злоумышленников и определить дальнейшие их действия [3]. Таким образом, выявляя подобные аномалии, можно принять меры по предотвращению угроз данного типа.

Список литературы

1. Медведев В.С., Потемкин В.Г. Нейронные сети. MatLab 6 / под общ. ред. В.Г. Потемкина. – М.: Диалог-МИФИ, 2002. – 496 с.

2. Круглов В.В., Борисов В.В. Искусственные нейронные сети. Теория и практика. – 2-е изд., стер. – М.: Горячая линия – Телеком, 2002. – 382 с.

3. Krotov L.N., Krotova E.L., Bogdanov N.V. Identification and counteractions to attacks of malefactors in the automated working system // ARPN Journal of Engineering and Applied Sciences. – 2015. – Vol. 10, № 22. – P. 10387–10391.

Получено 15.09.2016

Бондарев Владислав Юрьевич – студент кафедры «Автоматика и телемеханика», электротехнический факультет, Пермский национальный исследовательский политехнический университет, e-mail: mr.bond1995@mail.ru.

Сорокин Андрей Станиславович – студент кафедры «Автоматика и телемеханика», электротехнический факультет, Пермский национальный исследовательский политехнический университет, e-mail: sly-kyper@yandex.ru.

Кротова Елена Львовна – кандидат физико-математических наук, доцент кафедры «Высшая математика», факультет прикладной математики и механики, Пермский национальный исследовательский политехнический университет, e-mail: lenkakrotova@yandex.ru.