DOI: 10.17117/na.2015.11.03.448

<http://ucom.ru/doc/na.2015.11.03.448.pdf>

Поступила (Received): 13.11.2015

Цырульник В.Ф., Кадочникова Н.А. Применение искусственных нейронных сетей в решении практических задач информационной безопасности

Tsyurulnik V.F., Kadochnikova N.A.
**The use of artificial neural networks in the solution
of practical tasks of information security**

В данной статье рассматривается одно из перспективных направлений в возможности решения практических задач информационной безопасности – искусственные нейронные сети. Приведен пример их практического применения на выбранной подсистеме, связанной с идентификацией и аутентификацией пользователей. В ходе проведения анализа предлагается один из способов построения граф – схемы выполнения системы логических выражений

Ключевые слова: искусственные нейронные сети, идентификация, аутентификация, дестабилизирующие факторы, передаточная функция, веса связей, порог возбуждения

In this article one of the perspective directions in the solution of practical problems of information security – artificial neural networks is considered. The example of their practical application is given on the chosen subsystem connected with identification and authentication of users. During the analysis one of ways of creation of columns – schemes of system of logical expressions is offered

Key words: artificial neural networks, identification, authentication, destabilizing factors, transfer function, weight connection, excitation threshold

Цырульник Валерия Федоровна

Студент

Омский государственный технический университет

г. Омск, пр. Мира, 11

Tsyurulnik Valeria Fedorovna

Student

Omsk state technical university

Omsk, Mira ave., 11

Кадочникова Наталья Александровна

Студент

Омский государственный технический университет

г. Омск, пр. Мира, 11

Kadochnikova Natalia Alexandrovna

Student

Omsk state technical university

Omsk, Mira ave., 11

Научные достижения в областях информатики, таких как математическое моделирование состояния внешнего мира, искусственный интеллект, теория принятия решений, обработка изображений, сигналов и сцен распознавание образов, оптимальное управление, и многие другие позволяют говорить о реальной возможности перехода к новому поколению средств информационной защиты – интеллектуальным системам информационной безопасности. Из многих методов и средств искусственного интеллекта в сфере информационной защиты и информационного противодействия в качестве теоретического базиса

могут быть эффективно использованы и уже используются искусственные нейронные сети. Они являются одним из перспективных направлений в возможности решения практических задач информационной безопасности. Обзору известных исследований в области нейронных сетей и их практическим реализациям посвящена данная статья.

Искусственная нейронная сеть (НС) является совокупностью моделей биологических нейронных сетей. Структура НС представляет собой сеть элементов, т.е. искусственных нейронов, которые связаны между собой синоптическими связями. НС обрабатывает входную информацию и в процессе изменения своего состояния формирует совокупность выходных сигналов[2].

В данной работе предлагается заняться одним из проблемных вопросов, связанным с подсистемами информационной безопасности, это вопрос идентификации и аутентификации пользователей. Данная группа средств, в современных автоматизированных системах обработки информации, подвергается значительному числу угроз и наибольшее число из них совершаются успешно. Перечень угроз, связанных с данной подсистемой, выбран из банка данных угроз, сформированных ФСТЭК России:

1. Угроза восстановления аутентификационной информации.
2. Угроза использования информации идентификации/аутентификации, заданной "по умолчанию".
3. Угроза несанкционированного доступа к аутентификационной информации.
4. Угроза несанкционированного создания учётной записи пользователя.
5. Угроза подключения к беспроводной сети в обход процедуры аутентификации.
6. Угроза удаления аутентификационной информации.
7. Угроза несанкционированного изменения аутентификационной информации [1].

Но, прежде чем приступить к построению граф-схемы, необходимо обучить нейронную сеть принимать правильные решения, т.е. настроить параметры сети для решения поставленной задачи. Параметрами сети будут выступать синаптические коэффициенты (веса связей) и пороги (смещения). Целью обучения выступает достижение желаемой выходной реакции сети на некоторое множество входных сигналов, называемое обучающей выборкой. Входное и выходное множества сигналов удобно интерпретировать как вектора. Процесс обучения искусственной нейронной сети осуществляется путем последовательного предъявления входных векторов из обучающей выборки с одновременной подстройкой параметров сети в соответствии с некоторой процедурой, называемой алгоритмом обучения. Процедура обучения производится до тех пор, пока не будет достигнута желаемая выходная реакция искусственной нейронной сети для всей обучающей выборки.

Для формирования процесса обучения необходимо иметь модель внешней среды, в которой функционирует искусственная нейронная сеть, т.е. опреде-

лить доступную для сети информацию. Эта модель определяет парадигму обучения. В рамках определенной парадигмы обучения далее определяются правила подстройки параметров, т.е. конкретный алгоритм обучения.

Существуют три парадигмы обучения: «с учителем», «без учителя» и смешанная.

Обучение с учителем предполагает, что искусственная нейронная сеть располагает правильными ответами (выходными векторами) на каждый входной образ (входной вектор) [3,4]. При обучении каждому входному вектору обучающей выборки учитель ставит в соответствие целевой вектор, т.е. правильную реакцию сети. Пара входного и целевого вектора называется обучающей парой. Параметры сети подстраиваются так, чтобы ответы были максимально близкими к правильным.

Процесс обучения начинается после задания начальных значений весов сети. В общем случае они могут быть произвольными, например, нулевыми. При наличии априорной информации об особенностях процесса обучения, начальные значения весов могут выбираться из каких-либо дополнительных соображений. При предъявлении очередного входного вектора обучающей выборки выходной вектор сравнивается с целевым вектором, и по разности этих векторов алгоритм обучения производит коррекцию весов (а возможно и порогов), с целью минимизировать эту разность (ошибку). Процедура повторяется для всего обучающего множества до тех пор, пока ошибка по всему обучающему множеству не достигнет приемлемо низкого уровня.

Основное и самое очевидное правило обучения – коррекция по ошибке. Это правило применяется в алгоритме обучения с учителем.

Правило коррекции по ошибке. Для каждого входного сигнала обучающей выборки учителем задается правильный (целевой) выходной сигнал Z_T . После подачи входного сигнала сеть выдает реальный выходной сигнал Z_A , который может совпадать или не совпадать с целевым. Сигнал разности или ошибки $(Z_T - Z_A)$ используется для модификации весов с целью уменьшения этой ошибки.

Теперь на уже обученной НС возможно разобрать более подробно одну из угроз, например, угрозу под номером 5.

Работу информационной системы можно представить автоматной моделью, где входными параметрами будет являться совокупность действий пользователей и дестабилизирующих факторов, а соответствующая реакция средств защиты информационной системы будут являться выходными значениями.

Составление перечня дестабилизирующих факторов и исследования возможности их воздействия на систему обработки информации довольно трудоемко, поэтому будет составлен перечень дестабилизирующих факторов приведенных в литературе.

Выбранная группа: *подключение к беспроводной сети в обход процедуры аутентификации.*

X_1 = «если нарушителем возможен физический доступ к беспроводной точке доступа»;

X_2 = «если нарушителем не возможен физический доступ к беспроводной точке доступа»;

Таблица 1

X_3 = «если пользователь подключился к беспроводной сети в полуавтоматическом режиме»;

X_4 = «если пользователь подключился к беспроводной сети без ввода ключа шифрования»;

X_5 = «пользователь имеет право на вход в систему»;

X_6 = «если пользователь не смог подключиться к беспроводной сети в полуавтоматическом режиме»;

X_7 = «пользователь не имеет право на вход в систему»;

X_8 = «если пользователь не смог подключиться к беспроводной сети без ввода ключа шифрования»;

X_9 = «если пользователь обладает ключами шифрования»;

Реакция средств защиты на вышеперечисленные факторы:

R_1 = «предоставить доступ»;

R_2 = «отказать в доступе»;

R_3 = «нейтрализация».

Логическое описание средств защиты информации:

$R_1 \rightarrow \{X_1 X_5 \vee X_3 X_5 \vee X_9 X_5\}$,

$$R_2 \rightarrow \{X_2X_5 \vee X_5X_6 \vee X_5X_8 \vee X_7X_9\},$$

$$R_3 \rightarrow \{X_1X_7 \vee X_3X_7 \vee X_4X_7\}.$$

Граф-схема выполнения системы логических выражений представлена в таблице 1.

Так как данная система основана на неполных и недостоверных данных, необходимо задавать действительные значения входным данным, которые основываются на достоверности, вероятности и экспертной оценке. Согласно этому фактору, на входе должна использоваться не точная информация, а лишь оценка этой информации. Оценки должны быть относительными, т.е. отображать принцип «больше – меньше», так как этого достаточно для моделирования ассоциативного мышления.

Связь между входными и выходными данными осуществляет передаточная функция, обладающая свойством ассоциативности, т.е. позволяет «собирать» сигнал независимо от пути прохождения возбуждения. Выбрав передаточную функцию, предположим, что веса всех связей равны единице.

Немаловажную роль при построении граф-схемы играет порог сигнала возбуждения. Если правильно подобрать пороги для всех нейронов, то «нужные» нейроны будут возбуждаться, а «побочные эффекты» гаситься. Тем самым, важно выбирать существенные события для нейронных сетей.

Правильно подобрав передаточную функцию, порог и веса связей, тем самым достигается правильное решение сети.

Заключение. Как показал анализ, искусственные нейронные сети являются актуальными для решения определенных задач информационной безопасности, так как они обладают свойством самообучения, т.е. создавать обобщение. Данное свойство позволяет нейронным сетям решать сложные задачи, которые на сегодняшний день являются трудноразрешимыми.

В ходе построения граф-схемы была выполнена логическая схема системы принятия решений, которая является структурой обученной нейронной сети.

Список используемых источников:

1. Банк данных угроз безопасности информации.

URL: <http://bdu.fstec.ru/threat> (дата обращения 20.09.2015).

2. Барский А.Б. Нейронные сети: распознавание, обучение, принятие решений. М.: Финансы и статистика, 2004. 176 с.

3. Галушкин А.И. Теория нейронных сетей. Кн. 1. М.: ИПРЖР, 2000. 368 с.