По результатам прогнозирования, проведенного при помощи нейронной сети, построены аттракторы систем Энона и Лоренца. Объем прогноза для ряда Энона – 2000 значений, для ряда Лоренца – 500 значений. На рис. 1 и рис. 2 представлены соответствующие аттракторы систем Энона и Лоренца, построенные по результатам многошагового прогноза.

По разработанной авторами данной работы методике [1] для описанных хаотических процессов на основе подученных нейросетевых моделей были рассчитаны старшие показатели Ляпунова: для процесса Энона $\lambda = 4,42$; для процесса Лоренца $\lambda = 0,963$. Полученные значения позволяют сделать вывод о пригодности рассматриваемых в работе нейросетевых моделей для решения круга задач, связанных с анализом и обработкой хаотических сигналов.

Таким образом, нейронная сеть, построенная с использованием адаптивной функции активации в скрытом слое, имеет высокую скорость обучения и достаточно малую ошибку при обучении и прогнозировании. Использование адаптивной функции активации позволяет существенно уменьшить количество нейронных элементов в скрытом слое за счет индивидуальной подстройки параметров функций активации для каждого из нейронов скрытого слоя.

Следует, однако, отметить некоторые особенности метода обучения. Поскольку речь идет об одновременной настройке в процессе обучения, как весовых коэффициентов, так и параметров функции активации, то метод является требовательным к выбору размеров шагов обучения α, α_f (а также их соотношения) в рамках отдельной архитектуры сети и обучающей выборки.

ЗАКЛЮЧЕНИЕ

В данной статье описан метод применения функции активации с настраиваемыми параметрами при построении нейронных сетей. Принципиальное отличие предложенного метода – модификация параметров функции активации нейронных элементов наряду с их весовыми коэффициентами в процессе обучения нейронной сети. Изложены математические основы предлагаемого метода и результаты использования нейронной сети с адаптивной функцией активацией для прогнозирования временных рядов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. V. Golovko, Y. Savitsky, N. Maniakov. Neural Networks for Signal Processing in Measurement Analysis and Industrial Applications: the Case of Chaotic Signal Processing // chapter of NATO book “Neural networks for instrumentation, measurement and related industrial applications”. - Amsterdam: IOS Press, 2003, pp. 119-143.
2. Shuxiang Xu, Ming Zhang «Justification of a neuron-adaptive activation function». Proceedings of IEEE 2000.
3. Голловко В.А. Нейроинтеллект: теория и применение. Организация и обучение нейронных сетей с прямыми и обратными связями. – Брест, Изд. БПИ. – 1999. – 264с.

УДК 681.324

Головко В.А., Каменда Д.В., Кочурко П.А.

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ АТАК

1. ВВЕДЕНИЕ

Стремительный и всесторонний рост Интернет-технологий увеличивает важность защиты компьютерных сетей от атак. За последние годы число сетевых атак очень быстро возросло, что привело к значительным проблемам в различных компаниях. К примеру, DoS-атаки (“Denial of Service” – отказ в обслуживании) на такие компании, как Yahoo, принесли им убытки в миллионы долларов.

Системы обнаружения атак (СОА) используются как средство обеспечения безопасности компьютерных сетей и выдают администратору сигнал тревоги в случае атаки. Основная цель СОА – обнаружение и распознавание сетевых атак в режиме реального времени. Сейчас существуют различные подходы к обнаружению атак. Это сигнатурный метод, экспертные системы, встроенные сенсоры, нейронные сети, искусственные иммунные системы [1-6] и т. д. Большинство таких СОА могут обнаруживать известные атаки и имеют очень мало возможностей для обнаружения новых атак.

Данная статья описывает применение нейронных сетей для обнаружения атак путем анализа данных сетевого трафика. Это базируется на том, что отказ в обслуживании и другие сетевые атаки представлены в сетевом трафике. Поэтому использование нейронных сетей позволяет выделить нелинейные зависимости между переменными из сетевого трафика и проектировать системы обнаружения атак реального времени.

В статье описывается система обнаружения атак, которая состоит из двух различных нейронных сетей. Первой нейронной сетью является нелинейная рециркуляционная нейронная сеть (РНС), которая позволяет идентифицировать нормальное или аномальное поведение системы. Вторая сеть – многослойный персептрон (MLP), который может распознавать тип атаки.

Статья организована следующим образом. В разделе 2 описана система обнаружения атак, основанная на нейросетевом подходе. Часть 3 описывает нелинейную РНС и многослойный персептрон для идентификации и классификации компьютерных сетевых атак. В части 4 представлены результаты экспериментов. Выводы даны в части 5.

2. ОПИСАНИЕ СИСТЕМЫ

Рассмотрим блок-схему системы обнаружения атак (рисунок 1). Она состоит из нескольких этапов. В начале система считывает данные сетевого трафика, которые поступают в модуль предобработки. Задача модуля предобработки – сбор необходимых данных для нейронных сетей из сетевого трафика.

Функционирование его базируется на WinPcap, в результате чего из сетевого трафика выделяются элементы, показанные в таблице 1, которые используются в дальнейшем для обучения и тестирования нейронных сетей. Соединение –

Каменда Дмитрий Васильевич, *студент 5-го курса Брестского государственного технического университета.*
Кочурко Павел Анатольевич*, аспирант каф. интеллектуальные информационные технологии Брестского государственного технического университета.*
Беларусь, БГТУ, 224017, г. Брест, ул. Московская, 267.

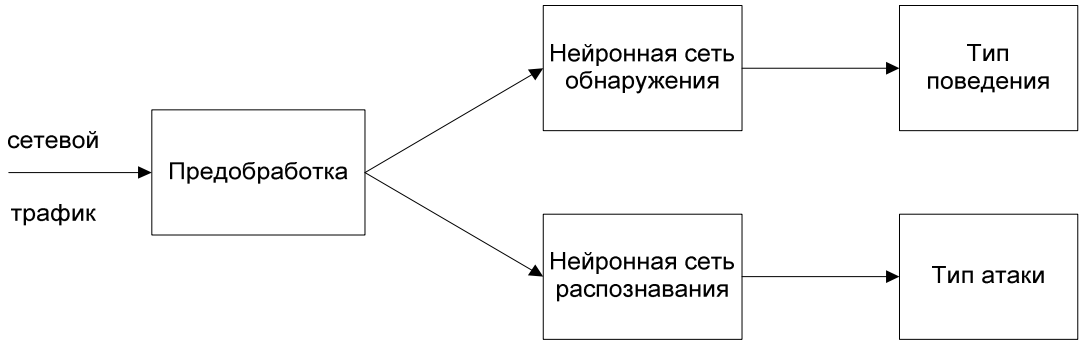


Рис. 1. Блок-схема обработки сетевого трафика нейронными сетями.

Таблица 1. Выбранные параметры сетевого трафика

Имя параметра	Описание	Тип
duration	Продолжительность (в секундах) работы соединения	Непрерывный
protocol_type	Используемый протокол (tcp, udp, icmp)	Дискретный
service	Целевая служба (http, telnet, ftp, ...)	Дискретный
src_bytes	Количество байт, пересланных от источника к приёмнику	Непрерывный
dst_bytes	Количество байт, пересланных от приёмника к источнику	Непрерывный
flags	Флаг TCP/IP результата	Дискретный

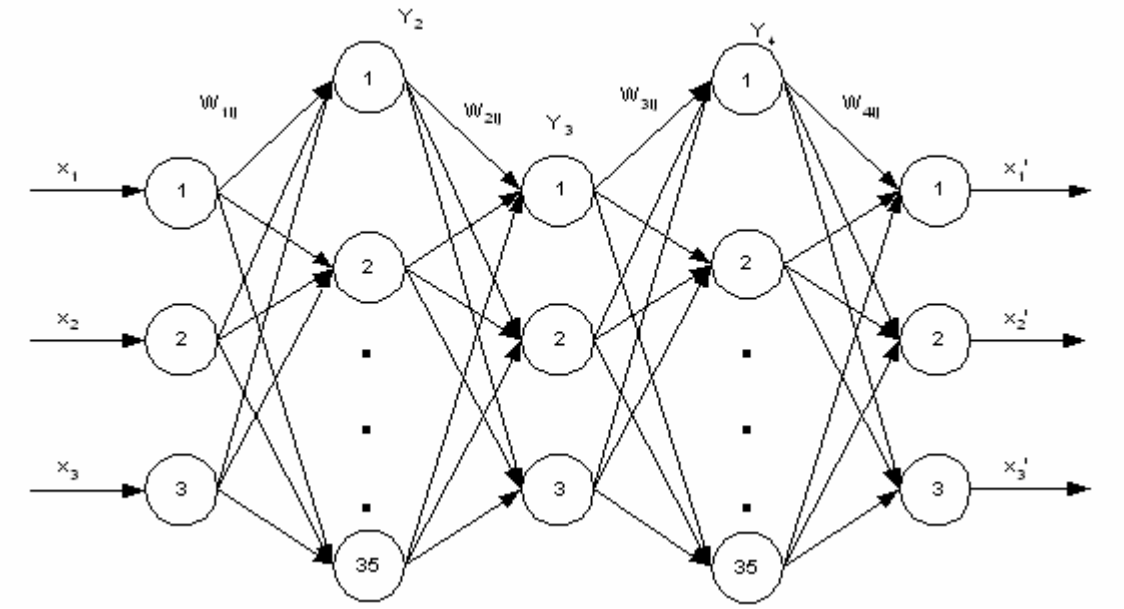


Рис. 2. Архитектура РНС

последовательность TCP пакетов за некоторое конечное время, моменты начала и завершения которого чётко определены, в течение которого данные передаются от IP-адреса источника на IP-адрес приёмника (и в обратном направлении) используя некоторый определённый протокол. Каждое соединение помечено как «нормальное» или «атака». Далее, соединение должно быть одного конкретного типа атаки. Каждая запись о соединении состоит из около 100 байт.

Нейронная сеть для идентификации атак - нелинейная РНС [7]. В качестве входных данных в этом случае используются четыре параметра: служба, продолжительность работы, количество байт от источника, и количество байт от приёмника. Нейронная сеть для распознавания - многослойный персептрон. В этом случае все перечисленные выше параметры (таблица 1) используются как входные данные. Такая система позволяют идентифицировать и распознавать сетевые нападения.

3. СТРУКТУРА НЕЙРОННЫХ СЕТЕЙ

Как упомянуто выше, цель нелинейной РНС состоит в том, чтобы идентифицировать нападение. Архитектура РНС состоит из пяти полносвязных слоёв с 3 входными и 3 выходными нейронами. Количество нейронов в скрытых слоях показано на рисунке 2.

Выход нейрона j в скрытом слое k вычисляется как:

$$Y_{kj} = F(S_{kj}), \qquad (1)$$

$$S_{kj} = \sum_i \omega_{kij} Y_{(k-1)i} \,. \quad (2)$$

Выход j-го нейрона:

$$X'_j = F(S_j)\,, \quad (3)$$

$$S_j = \sum_i \omega_{4ij} Y_{4j}\,, \quad (4)$$

где F - функция активации, S_j - взвешенная сумма, ω_{kij} - вес от i-го нейрона к j-му нейрону слоя k.

Цель РНС состоит в том, чтобы восстановить в выходном слое оригинальный набор данных. Для обучения РНС используется метод послойного обучения [8]. Он состоит из нескольких отдельных стадий обучения. В первой стадии производится определение весовой матрицы последнего слоя ω_4 и желательных выходов 4-ого слоя Y_4. Цель обучения состоит в том, чтобы минимизировать среднеквадратичную ошибку

$$E_S = \frac{1}{2}\sum_{p=1}^{L}\sum_j (\bar{X}_j^p - X_j^p)^2\,, \quad (5)$$

где L - количество тестовых образов. Метод градиентного спуска используется для минимизации выражения (5): в соответствии с ними:

$$\omega_{4ij}(t+1) = \omega_{4ij}(t) - \alpha\frac{\partial E}{\partial \omega_{4ij}}, \quad (6)$$

$$Y_{4i}(t+1) = Y_{4i}(t) - \alpha\frac{\partial E}{\partial Y_{4i}}\,. \quad (7)$$

Функция Y стоимости для одной выборки определяется

$$E = \frac{1}{2}\sum_j (\bar{X}_j - X_j)^2\,. \quad (8)$$

Дифференцируя (8) относительно ω_{4ij} и Y_4 мы можем получить следующие уравнения:

$$\omega_{4ij}(t+1) = \omega_{4ij}(t) - \alpha F'(S_j)(\bar{X}_j - X_j)Y_{4i}, \quad (9)$$

$$Y_{4i}(t+1) = Y_{4i}(t) - \alpha\sum_j F'(S_j)(\bar{X}_j - X_j)\omega_{4ij}\,. \quad (10)$$

На втором этапе определяются весовая матрица следующего слоя ω_3, и выходные значения Y_3. В качестве эталонных значений используется вектор Y_4, который был получен ранее. Тогда цель обучения во второй стадии состоит в том, чтобы минимизировать следующее выражение:

$$E_S = \frac{1}{2}\sum_{p=1}^{L}\sum_j (Y_{4j} - \bar{Y}_{4j})^2\,. \quad (11)$$

Веса и выходные значения этого слоя модифицируются итерационно в соответствии со следующим правилом:

$$\omega_{3ij}(t+1) = \omega_{3ij}(t) - \alpha F'(S_{4j})(Y_{4j} - \bar{Y}_{4j})Y_{3i}, \quad (12)$$

$$Y_{3i}(t+1) = Y_{3i}(t) - \alpha\sum_j F'(S_{4j})(Y_{4j} - \bar{Y}_{4j})\omega_{3ij}\,. \quad (13)$$

Тот же самый подход применен для другого слоя нейронной сети. В результате мы можем обучить РНС воспроизводить оригинальный набор данных.

Необходимо отметить, что первый слой РНС (рис. 1) производит нормализацию входных данных следующим образом:

$$X_i = \frac{1}{1+e^{-\log X_i}}\,. \quad (14)$$

После обучения РНС мы можем определить ошибку реконструкции для каждого входного образа:

$$E(k) = \frac{1}{L}\sum_j (\bar{X}_j^k - X_j^k)^2\,. \quad (15)$$

Таблица 2. Результаты тестирования РНС

Мера	Обнаружено атак, %	Ложных срабатываний, %	Служба
0,001	99,96 (2406)	9,94 (6151)	HTTP
0,0012	99,79 (2402)	9,53 (5898)	
0,0013 – оптим.	99,50 (2395)	9,50 (5580)	
0,0014	98,46 (2370)	9,49 (5872)	
0,0015	10,14 (244)	9,47 (5861)	
0,001	99,76 (424)	2,68 (10)	FTP
0,005	97,65 (415)	1,07 (4)	
0,006 – оптим.	97,41 (414)	0,8 (3)	
0,007	97,18 (413)	0,8 (3)	
0,01	96 (408)	0,8 (3)	
0,0005	36,84 (340)	14,09 (535)	FTP_DATA
0,001	36,84 (340)	9,35 (355)	
0,004	36,84 (340)	3,74 (142)	
0,005	35,97 (332)	3,19 (121)	
0,007	35,97 (332)	2,61 (99)	
0,010	35,97 (332)	1,76 (67)	
0,013 – оптим.	35,97 (332)	0,90 (34)	
0,027	35,97 (332)	0,90 (34)	
0,028	16,79 (155)	0,84 (32)	
0,001	99,2 (124)	77,75 (7462)	SMTP
0,002	99,2 (124)	70,57 (6773)	
0,005	99,2 (124)	59,63 (5723)	
0,01	99,2 (124)	53,76 (5160)	
0,02	99,2 (124)	0,68 (65)	
0,03 – оптим.	99,2 (124)	0,30 (29)	
0,05	98,4 (123)	0,30 (29)	

Таблица 3. Результаты тестирования обнаружения и распознавания атак

Служба	Всего записей	Всего атак	Обнаружено	Ложных	Распознано
auth	328	108	108 (100%)	0	108 (100%)
domain	116	113	113 (100%)	0	112 (99,12%)
eco_i	1642	1253	1253 (100%)	0	1149 (91,7%)
ecr_i	281400	281055	281049 (99,99%)	0	280790 (99,90%)
finger	670	202	200 (99,01%)	3 (0,64%)	180 (90%)
ftp	798	425	414 (97,41%)	3 (0,8%)	409 (98,79%)
ftp_data	4721	923	317 (34,34%)	5 (0,13%)	308 (97,16%)
http	64293	2407	2364 (98,21%)	220 (0,36%)	2362 (99,92%)
IRC	43	1	1 (100%)	31 (73,81%)	1 (100%)
Pop_3	202	123	122 (99,19%)	0	119 (97,54%)
private	110894	103527	103500 (99,97%)	2 (0,03%)	83900 (81,01%)
shell	112	111	111 (100%)	0	111 (100%)
smtp	9723	125	122 (97,6%)	28 (0,29%)	120 (98,36%)
Ssh	105	104	104 (100%)	0	102 (98,08%)
telnet	513	294	250 (85,03%)	3 (1,37%)	246 (98,4%)
time	157	105	103 (100%)	2 (3,85%)	103 (100%)

Таблица 4. Статистика обнаружения и распознавания атак в зависимости от класса атак

Класс	Всего	Обнаружено	Распознано
1 dos	391458	391416 (99,98%)	370404 (94,62%)
2 u2r	52	2 (3,84%)	0 (0%)
3 r2l	1126	509 (45,2%)	497 (97,64%)
4 probe	4107	4057 (98,78%)	3280 (79,86%)

Пусть $E'(k)$ - мера аномальности. Тогда мы можем обнаружить сетевую атаку, сравнивая ошибку реконструкции с мерой аномальности. Если $E(k) > E'(k)$ тогда это - сетевая атака. Иначе - нормальное поведение.

Рассмотрим нейронную сеть для распознавания атак. Эта сеть - многослойный персептрон с 6 входными нейронами, 40 скрытыми нейронами и N выходными нейронами, где N определено количеством различных типов атак в обучающем наборе данных. Для базы данных KDD это 23 типа атак (сюда включается и значение «normal», т. е. отсутствие атаки). Для обучения сети используется алгоритм обратного распространения ошибки.

Для каждой службы на выборке записей о соединениях, использующих только эту службу, обучается своя РНС для обнаружения атак и свой персептрон для распознавания типа атаки. Результаты экспериментов обсуждены в следующем разделе.

4. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТОВ

Чтобы оценить эффективность предложенного подхода обнаружения вторжения, эксперименты проводились на наборе данных KDD [9]. Тренировочные наборы данных для обнаружения аномалий состояли из 400-700 случайным образом выбранных записей о нормальных соединениях для каждой службы, а для распознавания атак – из нормальных соединений и атак, взятых в соотношении, бликом к 1:1.

Результаты тестирования РНС для некоторых служб приведены в таблице 2. Мера аномальности подбиралась по результатам экспериментов таким образом, чтобы максимизировать отношение числа обнаруженных атак к числу ложных срабатываний.

Подключение второй нейронной сети – для распознавания атак – дало следующие результаты: на наборе данных KDD, состоящем из 494021 записи верно обнаруживается 395984 (99,81%) атак, из них 374149 (94,49%) верно распознаются, при всего 398 (0,41%) ложных срабатываниях (атака считается обнаруженной, если атаку обнаруживают обе сети). Статистика обнаружения и распознавания по основным службам, для которых обучались отдельные нейронные сети показана в таблице 3.

Набор данных KDD содержит 22 типа атак, которые относятся к 4 классам нарушений информационной безопасности [9]:

- DOS – «denial-of-service» - отказ в обслуживании. Например, Syn-лавина.
- U2R – неавторизованное получение привилегий root на данной системе. Например, различные атаки «переполнения буфера».
- R2L – неавторизованный доступ с удалённой системы. Например, подбор пароля.
- Probe – наблюдение и другое зондирование, разведка. Например, сканирование портов.

Как видно из результатов, применяемая методика обнаружения атак хорошо подходит для обнаружения атак классов DOS и PROBE, и недостаточно хорошо – для атак классов U2R и R2L.

5. ЗАКЛЮЧЕНИЕ

В данной статье мы обратились к некоторым аспектам применения нейронных сетей для обнаружения вторжений. Используя две различные нейронных сети, а именно РНС и MLP, мы можем идентифицировать и распознавать атаки на компьютерные сети. По сравнению с другими подходами нейронные сети позволяют проектировать системы обнаружения вторжения, которые имеют способность к обучению и работе в реальном времени. Эксперименты показали эффективность применения нейросетевой технологии.

Авторы благодарят за поддержку исследований Белорусский республиканский фонд фундаментальных исследований при НАН Беларуси.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. M. Bishop, S. Cheung, C. Wee, J. Frank, J. Hoagland and S. Samorodin. The treat from the Net. IEEE Spectrum, 34(8), pp. 56-53, 1993.
2. D. Anderson, T. Frivold & A. Valdes. Next-generation Intrusion Detection Expert Systems (NIDES): A Summary. SRI International Technical Report SRI-CSL-95-07, 1995.

3. E. Spafford and D. Zamboni. Data collection mechanisms for intrusion detection systems. CERIAS Technical Report 2000-08, CERIAS, Pardue University, 1315 Recitation Building, West Lafayette, IN, 2000.
4. H. Debar, M. Becke & D.Simboni. A Neural Network Component for an Intrusion Detection System. In proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, (1992).
5. C. Jirapummin and N. Wattanapongsakorn. Visual Intrusion Detection using Self-Organizing Maps, Proc. of Electrical and Electronic Conference (EECON-24), Thailand, Vol. 2, pp. 1343-1349, 2001.
6. S.C. Lee and D.V. Heinbuch. Training a Neural Network Based Intrusion Detector to Recognize Novel Attacks. Information Assistance and Security, pp. 40-46, 2000.
7. S. Hawkins, H. He, G. Williams, R. Baxter. Outlier Detection Using Replicator Neural Networks. Proceedings of the 4th International Conference on Data Warehousing and Knowledge Discovery (DaWaK02) Lecture Notes in computer Science, Vol. 2454, Springer, Pages 170-180, ISBN 3-540-44123-9, 2002
8. V. Golovko, O. Ignatiuk, Yu. Savitsky, T. Laopoulos, A. Sachenko, L. Grandinetti. Unsupervised learning for dimensionality reduction. Proc. of Second Int. ICSC Symposium on Engineering of Intelligent Systems EIS'2000, University of Paisley, Scotland, June 2000. Canada / Switzerland: ICSS Academic Press, pp. 140 – 144, 2000.
9. 1999 KDD Cup Competition. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

УДК 004.383

Дунец А.П.

НЕЙРОННЫЕ СЕТИ ПРЯМОГО РАСПРОСТРАНЕНИЯ С ДОПОЛНИТЕЛЬНЫМИ СВЯЗЯМИ

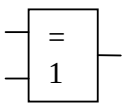
1. Введение

На данный момент в области нейросетевого моделирования разработано и исследовано значительное количество моделей искусственных нейронных сетей. Эти НС успешно применяются для решения разнообразных практических задач [1]. Одними из самых популярных нейросетевых моделей являются НС прямого распространения. Их популярность обусловлена простой и регулярной структурой. Для данных НС разработано большое число алгоритмов обучения. Предлагаются разные функции активации нейронных элементов (НЭ) [1]. Получено множество теоретических результатов. В то же время сообщество исследователей не оставляет попыток улучшить эту, уже ставшую классической, НС.

В данной работе предлагается вариант модернизации нейронной сети прямого распространения. Модернизация основана на введении дополнительных связей между слоями. Модифицированная таким образом модель обучалась на данных задачи "Исключающее «ИЛИ»" и показала свою большую эффективность в сравнении с НС классической архитектуры.

2. Задача "Исключающее «ИЛИ»"

Задача "Исключающее «ИЛИ»" (рис. 1) – один из интересных теоретических вопросов, которые рассматриваются в нейросетевом моделировании. Эта задача возникает, если попытаться заменить элементы булевой логики нейросетевыми структурами. В работе [1] показано, что для элементов «И», «ИЛИ» это можно сделать, используя персептрон Розеблатта. В то же время элемент "Исключающее «ИЛИ»" построить на персептроне Розеблатта нельзя из-за того, что в основе персептрона лежит линейное преобразование информации, а задача "Исключающее «ИЛИ»" - нелинейная.



X_1	X_2	Y
0	0	0
1	0	1
0	1	1
1	1	0

Рис. 1. Элемент "Исключающее «ИЛИ»" с таблицей истинности

В [1] для решения данной задачи используется многослойная нейронная сеть прямого распространения информации. Сеть содержит 3 слоя: распределительный слой и 2 обрабатывающих слоя. Обрабатывающие слои состоят из НЭ с пороговой функцией активации. Следует отметить, что пороговая функция в этом случае несколько неудобна для теоретического анализа. Это делает НС на ее основе сложными для применения к ним градиентных алгоритмов обучения. Целесообразно использовать сигмоидную функцию активации. При небольших допущениях она эквивалентна пороговой функции и при этом легче поддается анализу аналитическими методами:

$$y = \frac{1}{1+e^{-s}}, \qquad (1)$$

где

$$S = \sum_{i=1}^{n} \omega_i x_i - T. \qquad (2)$$

В этом выражении x_i - значение, которое подано на i-ый вход нейронного элемента, ω_i - значение весового коэффициента для i-го входа, T - значение порога НЭ.

В результате обучения НС получен результат, который приведен на рис. 2.

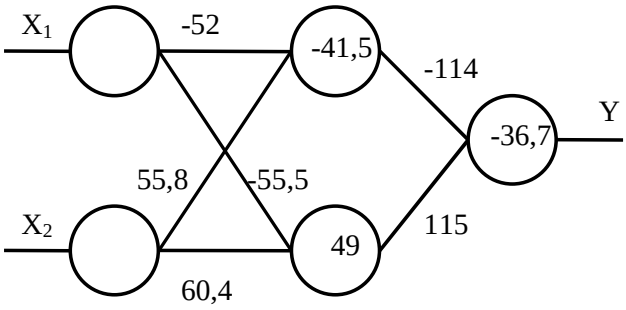


Рис. 2. Обученная НС классической архитектуры

Полученная в результате НС содержит 3 обрабатывающих НЭ и всего 9 настраиваемых коэффициентов: 4 веса и 2 порога в скрытом слое и 2 веса и 1 порог в выходном слое.

Дунец Андрей Петрович, *ст. преподаватель каф. интеллектуальных информационных технологий Брестского государственного технического университета.*
Беларусь, БГТУ, 224017, г. Брест, ул. Московская, 267.