2. B. Byfield. OpenOffice.org Writer vs. Microsoft Word // NewsForge: the online newspaper for Linux and Open Source. 12.06.2005.
http://software.newsforge.com/article.pl?sid=05/06/14/2137222&from=rss
3. WYSIWYM. The WYSIWYM paradigm in software engineering. 21.06.2006.
http://en.wikipedia.org/wiki/WYSIWYM
4. M. Müller-Prove. The Interface of Kai Krause's Software. ASI Software-Ergonomie Lehre Seminare. University of Hamburg. 1999. http://www.mprove.de/script/99/kai/index.html

УДК 519.876.5+004.514.6:657.1
Войцехович Л. Ю.
Научный руководитель: д.т.н., профессор Головко В. А.

НЕЙРОСЕТЕВЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ АТАК НА КОМПЬЮТЕРНЫЕ СЕТИ

1. ВВЕДЕНИЕ

Одной из форм глобализации мирового пространства является информационная глобализация, которая связана с широким распространением сети Интернет. Информационная глобализация увеличивает степень уязвимости компьютерных систем, что уменьшает их безопасность. *Атакой на компьютерные сети* называется совокупность определенных действий, приводящих к подрыву безопасности системы. В результате атаки злоумышленник может получить доступ к конфиденциальной информации или нарушить нормальное функционирование системы. Это приводит к большим материальным и социальным издержкам.

Важным этапом обеспечения безопасности компьютерных систем является проектирование *систем обнаружения атак* (Intrusion Detection System – IDS). Такие системы способны на основе анализа сетевого трафика автоматически обнаруживать атаки TCP/IP, что позволяет предпринять необходимые меры для нейтрализации угрозы.

В данной работе рассматриваются нейросетевые подходы для построения систем обнаружения атак. В качестве базы данных для тестирования системы используется KDD-99 [1], которая содержит почти 5 миллионов записей соединений и 41 параметр сетевого трафика. При этом атаки делятся на четыре основных класса: DoS, U2R, R2L и Probe.

Атака DoS – отказ в обслуживании, характеризуется генерацией большого объема трафика, что приводит к перегрузке и блокированию сервера.

Атака U2R предполагает получение зарегистрированным пользователем привилегий локального суперпользователя (администратора).

Атака R2L характеризуется получением доступа незарегистрированного пользователя к компьютеру со стороны удаленной машины.

Атака Probe заключается в сканировании портов с целью получения конфиденциальной информации.

В работе предлагаются различные варианты построения систем обнаружения атак, которые базируются на использовании рециркуляционных и многослойных нейронных сетей. Результаты экспериментов обсуждаются.

2. ГЕНЕРИРОВАНИЕ АРХИТЕКТУРНЫХ РЕШЕНИЙ

Рассмотрим различные архитектурные решения для построения систем обнаружения атак. В качестве входных данных используется 41-размерный вектор, который характеризует параметры соединения сети. Задачей IDS является обнаружение и распознавание атак. Поэтому в качестве выходных данных используется m-мерный вектор, где m равняется количеству атак плюс нормальное состояние.

На рис 1 приведена система обнаружения атак, которая состоит из рециркуляционной нейронной сети (RNN) и многослойного персептрона (MLP)

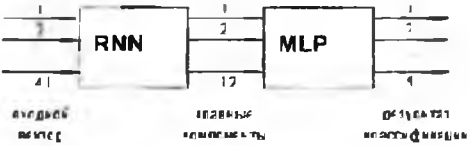

Рис. 1. Первый вариант IDS

Задачей RNN является сжатие входного пространства образов с целью получения главных компонент [2]. Главные компоненты являются некоррелированными и содержат наиболее информативные признаки исходного пространства образов. Многослойный персептрон осуществляет обработку сжатого пространства входных образов (главных компонент) с целью распознавания класса атаки.

На рис. 2 приведена вторая схема системы обнаружения атак. Она характеризуется тем, что главные компоненты с выходов RNN одновременно поступают на 4 отдельных многослойных персептрона, каждый из которых соответствует определенному классу атаки: DoS, U2R, R2L и Probe. С выходов MLP данные поступают на арбитр, который и принимает окончательное решение о состоянии системы. В качестве арбитра может использоваться линейный или многослойный персептрон. Тогда обучение его будет производиться после обучения RNN и MLP. Такая схема может осуществлять иерархическую классификацию атак. В этом случае арбитр определяет один из 5 классов атаки, а соответствующий многослойный персептрон – тип атаки.

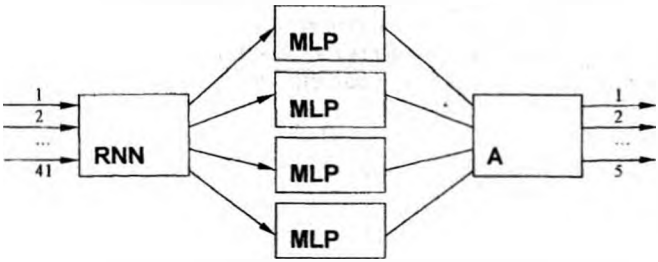

Рис. 2. Второй вариант IDS

На рис. 3 изображен третий вариант IDS. Он характеризуется тем, что исходный 41 размерный вектор данных разбивается на части (подвекторы), содержащие однородные данные. При этом для каждого подвектора ставится в соответствие своя RNN, которая вычисляет соответствующие главные компоненты. С выходов RNN данные поступают на многослойные персептроны, которые определяют тип атаки. Арбитр принимает окончательное решение. Его структура определяется, как и в предыдущем варианте.

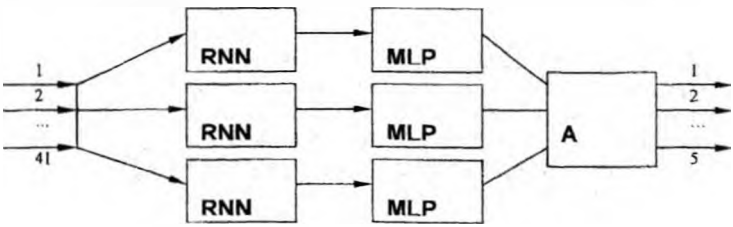

Рис. 3. Третий вариант IDS

Кроме того, возможен вариант представленный на рис 4, который является модификацией варианта 3 Отличительной особенностью этой нейросетевой структуры является общий для всех RNN модуль MLP Он и производит основные вычисления, связанные с распознаванием входного вектора, одновременно используя всю информацию предоставленную рециркуляционными нейронными сетями

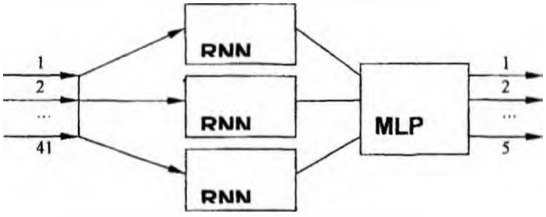

Рис 4. Четвертый вариант IDS

Рассмотренные в данном разделе архитектурные решения систем обнаружения атак базируются на различной компиляции рециркуляционных и многослойных нейронных сетей

3. ПРОЕКТИРОВАНИЕ НЕЙРОННЫХ СЕТЕЙ

Рассмотрим линейную рециркуляционную нейронную сеть. Она осуществляет сжатие 41-размерного входного вектора в 12-размерный выходной вектор Количество главных компонент определялось экспериментальным путем исходя из достижения приемлемой точности без существенной потери информативности Эксперименты показали, что существует некоторое оптимальное число главных компонент, дальнейшее увеличение которых не приводит к повышению качества распознавания

Обучение RNN производилось в соответствии с правилом Ойя [3]:

$$w'_{ji}(t+1) = w'_{ji}(t) + \alpha\ y_j \cdot (x_i - \bar{x}_i),$$

где w'_{ji} - весовой коэффициент между *j*-ым нейроном скрытого слоя и *i*-ым нейроном выходного слоя,

x_i - значение *i*-го параметра входного вектора,

y_j - значение *j*-го элемента скрытого слоя,

$\bar{x}_i$ восстановленное значение *i* го элемента входного вектора

Перед подачей данных на вход RNN проводилась их предварительная обработка:

$$x^t = x^t - \mu(x_i),$$

где $\mu(x_i) = \frac{1}{L}\sum_{k=1}^{L} x^k$

Здесь L – размерность обучающей выборки

Для обучения RNN использовались данные из базы KDD-99 Желаемая суммарная среднеквадратичная ошибка – 0,01. После обучения сети она может преобразовывать входное пространство образов в главные компоненты

Рассмотрим отображение входного пространства образов для нормального состояния и атаки (тип атаки Neptune) на плоскость двух первых главных компонент (рис 5)

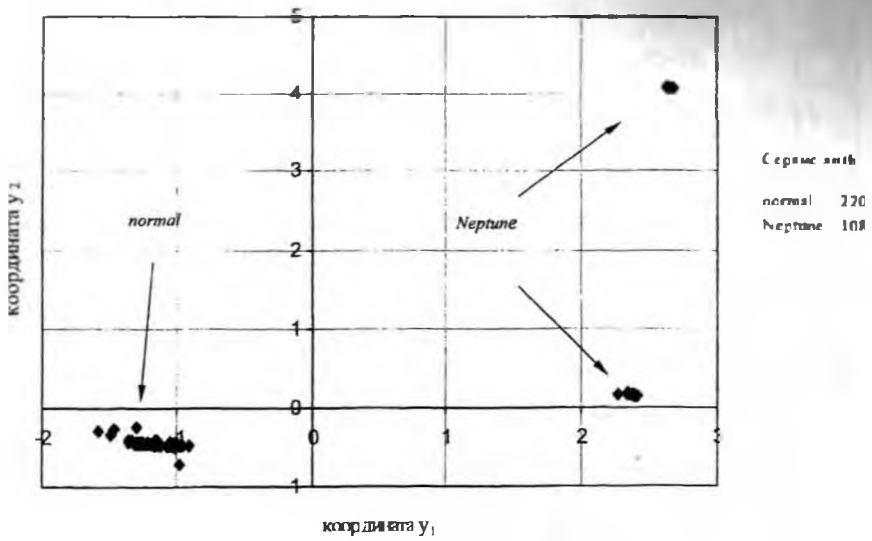

Рис. 5 Данные после обработки RNN на примере сервиса auth

Из рисунка видно, что данные, соответствующие одному типу атаки могут концентрироваться в нескольких областях. Это затрудняет классификацию атак при использовании RNN. Для устранения этого недостатка можно применить нелинейную RNN, что будет рассмотрено в дальнейших работах.

Как уже отмечалось, многослойный персептрон предназначен для классификации атак на основе главных компонент. Поэтому структура сети следующая: количество нейронов в распределительном слое – 12; в скрытом слое - 10, а в выходном слое варьируется в зависимости от определения класса или типа атаки. Для обучения использовался алгоритм обратного распространения ошибки. Сеть обучалась до суммарной квадратичной ошибки равной 0,01.

После обучения рассмотренных выше нейронных сетей они объединялись в единую систему обнаружения атак.

4. ЭКСПЕРИМЕНТЫ

В процессе обучения и тестирования системы использовалась 10% выборка данных из базы KDD 99. Эксперименты проводились для каждой службы отдельно. Обучающие выборки содержали около 20% записей по каждой службе. После обучения на сеть подавался весь набор имеющихся записей, и собиралась статистика обнаружения и распознавания атак.

Рассмотрим функционирование системы на примере модели 1 (см. раздел 2). Результаты тестирования в режиме распознавания класса атаки для некоторых служб приведены в табл. 1, а сводные данные по почти 30 службам – в табл. 2.

Таблица 1. Результаты тестирования в режиме классификации атак

служба	normal		DoS			U2R		
	кол.	распознано	кол.	обнаружено	распознано	кол.	обнаружено	распознано
auth	220	220(100%)	108	108(100%)	108(100%)	—	—	—
domain	3	3(100%)	112	112(100%)	112(100%)	—	—	—
eco_i	389	387(99,5%)	—	—	—	—	—	—
ecr_i	345	327(94,8%)	281049	281031 (100%)	281031 (100%)	—	—	—
finger	468	456(97,4%)	197	189(95,9%)	85(45,0%)	—	—	—
ftp	373	359(96,2%)	104	104(100%)	104(100%)	3	3(100%)	3(100%)
ftp_data	3798	3752(98,8%)	170	168(98,8%)	26(15,5%)	12	12(100%)	11 (91,7%)
http	61885	61787(99,8%)	—	—	—	—	—	—
IRC	42	41(97,6%)	—	—	—	—	—	—
pop_3	79	79(100%)	118	118(100%)	118(100%)	34	26(76,5%)	26(100%)
smtp	9598	9472(98,7%)	120	120(100%)	120(100%)	—	—	—
telnet	219	204(93,2%)	198	198(100%)	198(100%)	34	26(76,5%)	26(100%)

служба	R2L			Probe		
	кол.	обнаружено	распознано	кол.	обнаружено	распознано
auth	—	—	—	—	—	—
domain	—	—	—	1	1(100%)	1(100%)
eco_i	—	—	—	1253	1251(99,8%)	1251(100%)
ecr_i	—	—	—	6	0(0,0%)	0(0,0%)
finger	—	—	—	5	5(100%)	4(80,0%)
ftp	313	245(78,3%)	144(46%)	5	5(100%)	5(100%)
ftp_data	733	683(93,2%)	595(81,1%)	8	8(100%)	7(87,5%)
http	4	4(100%)	4(100%)	8	8(100%)	8(100%)
IRC	—	—	—	1	1(100%)	1(100%)
pop_3	—	—	—	5	5(100%)	5(100%)
smtp	—	—	—	5	5(100%)	3(60,0%)
telnet	57	56(98,2%)	53(94,6%)	5	5(100%)	5(100%)

Таблица 2. Статистика тестирования в режиме классификации атак (около 30 сервисов)

класс	всего	обнаружено	распознано
DoS	286369	286334(99,9%)	286087(99,9%)
U2R	49	41(83,7%)	40(97,6%)
R2L	1119	1000(89,4%)	906(90,6%)
Probe	1320	1312(99,4%)	1308(99,7%)
нормальное состояние			
Normal	83281	---	82943(99,6%)

Табл. 2 позволяет оценить эффективность предложенного алгоритма при решении задач классификации атак. Наилучший результат был достигнут для атак класса DoS и Probe (почти однозначная распознаваемость). Несколько хуже определяются U2R и R2L, соответственно 83,7% и 89,4%. Кроме того, существует процент ложных срабатываний системы.

Далее приведен результат тестирования в режиме распознавания типа атаки (табл. 3). В этом случае количество нейронных элементов в выходном слое MLP равняется 23 (все типы атак + нормальное состояние).

Таблица 3 Результаты тестирования в режиме определения типа атак

служба	определенные атаки	ложное срабатывание	распознанные атаки
auth	108(100%)	0	108(100%)
domain	113(100%)	0	113(100%)
ecr_i	1252(99,9%)	0	1239(99,0%)
ecr_i	281034(99,9%)	13(3,77%)	281034(100%)
finger	186(92,1%)	10(2,14%)	185(99,5%)
ftp	418(98,3%)	26(6,97%)	418(100%)
ftp_data	856(92,7%)	31(0,82%)	636(74,3%)
http	2400(99,7%)	96(0,16%)	2400(100%)
IRC	1(100%)	1(2,38%)	1(100%)
pop_3	123(100%)	0	123(100%)
smtp	122(97,6%)	35(0,36%)	119(97,5%)
telnet	284(96,6%)	15(6,85%)	272(95,7%)

5. ЗАКЛЮЧЕНИЕ

В работе рассмотрены различные варианты построения систем обнаружения атак, которые базируются на нейросетевых технологиях. Путем комбинирования двух различных нейронных сетей, а именно RNN и MLP, можно идентифицировать и распознавать атаки на компьютерные сети с достаточно высокой степенью точности. В качестве базы данных для тестирования предложенных методов использовалась база KDD-99. Основными преимуществами использования подходов, основанных на нейронных сетях, является способность адаптироваться к динамическим условиям и быстрота функционирования, что особенно важно при работе системы в режиме реального времени.

ЛИТЕРАТУРА:

1 1999 KDD Cup Competition http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

2 Головко В.А. Нейронные сети: обучение, организация и применение Кн 4 Учеб пособие для вузов / Общая ред. А И Галушкина. – М.: ИПРЖР, 2001 – 256 с.

3 Hyvaerinen A., Oja E. Independent component analysis: algorithms and applications // Neural Networks, №13, 2000, - P 411-430.