УДК 004

ВИШНЯКОВ ВЛАДИМИР АНАТОЛЬЕВИЧ

доктор техн. наук, профессор кафедры информационных технологий, МИУ, Беларусь, г. Минск

СЛАБКО ПАВЕЛ ГЕННАДЬЕВИЧ

магистрант кафедры информационных технологий, МИУ, Беларусь, г. Минск

СИСТЕМА ИНТЕЛЛЕКТУАЛЬНОЙ БЕЗОПАСНОСТИ НА БАЗЕ ПЕРЦЕПТРОНА РУМЕЛЬХАРТА

Аннотация: в данной работе проведён анализ системы безопасности на базе нейронной сети.

Ключевые слова: безопасность, нейронная сеть, перцептрон.

VISHNIAKOV VLADIMIR ANATOLEVICH

Minsk Innovation University, Ph.D., Associate Professor, Department of Information Technologies, Minsk

SLABKO PAVEL GENNADEVICH

Student of Minsk Innovation University, Minsk

SYSTEM INTELLECTUAL SECURITY BASED ON RUMELHARD PERCEPTRON

Annotation: In this paper, we provide an analysis of security system based on artificial neural network.

Keywords: security, artificial neural network, perceptron.

Одним из решений для обеспечения безопасности веб-приложений является файервол. Большинство файерволов действуют по принципу фильтрации пользовательских входящих обращений в соответствии с заранее выставленными паттернами и инструкциями. Паттерны как правило основываются на регулярных выражениях, — наиболее популярные файерволы: ModSecurity, NAXSI. Тем не менее в связи с быстрым развитием веб-приложений количество угроз стремительно растет и таким образом подход с использованием регулярных выражений не способен обеспечить требуемую функциональность файервола за допустимое время. Имеет смысл выработать новый подход для обеспечения безопасности веб-приложений. Во-первых, он должен быть масштабируемым, т. е. новый подход обязан нормально функционировать с ростом количества правил. Во-вторых, он должен легко обновляться. В-третьих, новый подход должен быть способен взаимодействовать с динамической природой атак на веб-приложения, включая сложные паттерны. И в-четвертых, время фильтрации входящих клиентских запросов не должно сильно влиять на производительность самого веб-приложения.

В работе реализована схема многослойного перцептрона Румельхарта. На примере которой есть возможность сравнения результатов работы различных активационных функций и возможность варьировать количеством скрытых слоёв.

Для построения нейронной сети имеет смысл определить размерность Вапкина-Червоненкиса (VC-размерность или комбинаторная размерность) для выбранной топологии нейронной сети, как численную характеристику сети.

$$2\left[\frac{K}{2}\right]N \le VC\dim \le 2N_w\left(1+\lg N_n\right) \quad (1)$$

где N – размерность входных данных

K – количество нейронов скрытого слоя

N_w – количество всех весов сети

N_n – количество всех нейронов сети

Размерность обучающей выборки должна быть меньше либо равной размерности скрытого слоя для того чтобы не было переобучения нейронной сети.

Для проектирования нейронной сети использовался модуль “Tensorflow”.

Наборы данных для обучения искусственной нейронной сети получаем из базы данных, состоящую из наборов данных о реальных сетевых соединениях и вторжениях. Наборы данных взяты с ”http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html”.

При выборе архитектуры сети рассматриваются как существенные девять характеристик, Таблица 1, которые обеспечивают описание информации, переданной в пакете. Архитектура искусственной нейронной сети изображена на Рисунке 1.

Таблица 1. Параметры соединения

Параметр	**Описание**
duration	Длительность соединения (секунда)
protocol_type	Тип протокола
service	Сетевая служба получателя
flag	Состояние соединения
src_bytes	Число байтов переданных от источника получателю
dst_bytes	Число байтов переданных от получателя источнику
land	1 – для случаев соединения по идентичным портам 0 – в других случаях
wrong_fragment	Количество “неверных” пакетов
urgent	Количество пакетов с флагом “URG”

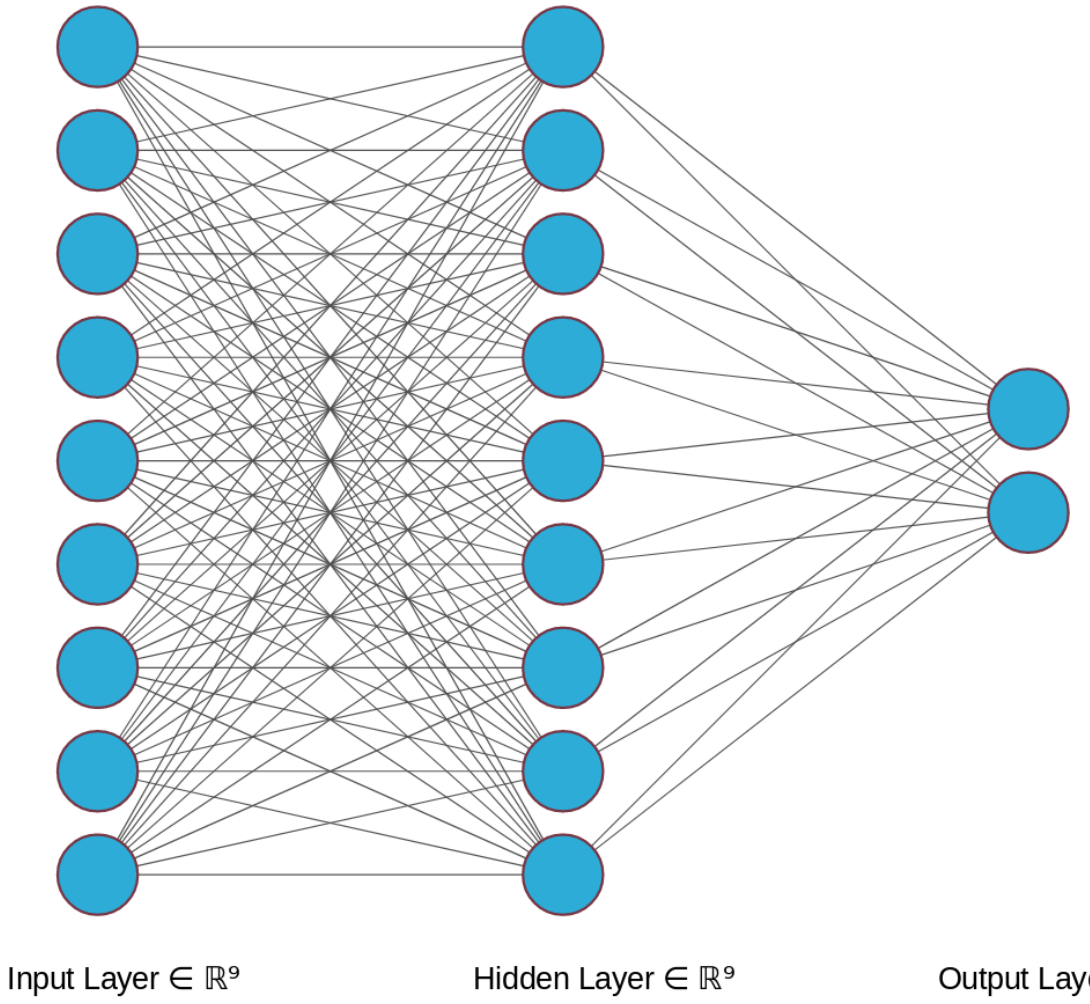

Рисунок 1 – Архитектура нейронной сети

Набор данных был разделён на три категории:

- обучающая (TrainData)
- тестируемая (TestData)
- подбор оптимального состояния (FutureData).

Данные категории TrainKDD применяются для тренировочного процесса и состоят из соединений имитирующих следующие типы вторжений:

1. back – DoS
2. buffer_overflow – U2R
3. ftp_write – R2L
4. guess_passwd – R2L
5. imap – R2L
6. ipsweep – Probe
7. land – DoS
8. loadmodule – U2R
9. multihop – R2L
10. neptune – DoS
11. nmap – Probe
12. perl – U2R
13. phf – R2L
14. pod – DoS
15. portsweep – Probe
16. rootkit – U2R
17. satan – Probe
18. smurf – DoS
19. spy – R2L
20. teardrop – DoS
21. warezclient – R2L
22. warezmaster – R2L

Наборы данных представлены различным количеством соединений. Преобладающее число соединений в наборах – это DoS вторжения. Это

обусловлено концепцией главной идеи данной категории вторжений, которая использует огромное количество IP-пакетов с целью перегрузить сетевые службы.

Данные категории FutureData применяются для обучения новым неизвестным ранее свойствам соединений. Эти свойства отсутствуют в тренировочном наборе данных TrainData. Таким образом на по результатам проверки на наборе FutureData можно будет сделать вывод о способности системы обучаться распознаванию новых типов вторжений.

Для обучения искусственной нейронной сети применялся алгоритм обратного распространения ошибки. В нем вычисляется ошибка, как выходного слоя, так и каждого нейрона обучаемой сети, а также производится коррекция весов в соответствии с их текущими значениями. На первом шаге алгоритма все веса межнейронных связей заполняются произвольными значениями в диапазоне от нуля до одного.

После определения весов в процессе обучения нейронной сети выполняются следующие шаги:

- прямое распространение сигнала;
- вычисление ошибки нейронов последнего слоя;
- обратное распространение ошибки.

Итоги обучения и тестирования искусственной нейронной сети показывают применимость ее для решения задачи выявления сетевых компьютерных вторжений. Искусственная нейронная сеть правильно классифицирует соединения в сети в 88% случаев распознавая действия злоумышленника.

Список литературы:

1. OWASP Top 10 2017 [Электронный ресурс] // The Ten Most Critical Web Application Security Risks. – Режим доступа: https://www.owasp.org/index.php/Top_10-2017_Top_10. – Дата доступа: 28.11.2018.

2. Кашев Т. Р. – Алгоритмы активного аудита информационной системы на основе технологий искусственных иммунных систем. [Электронный ресурс] // – Режим доступа:

http://www.ugatu.ac.ru/assets/files/documents/nich/dissov/d7/18.09.08/kashaev_avtoreferat.pdf. — Дата доступа: 15.11.2018.

3. Баскин И. И. – МОДЕЛИРОВАНИЕ СВОЙСТВ ХИМИЧЕСКИХ СОЕДИНЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ И ФРАГМЕНТНЫХ ДЕСКРИПТОРОВ.