ISSN 2079-3316 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ №4(35), 2017, с. 197–207

УДК 004.89

Н. С. Абрамов, В. П. Фраленко

Нейросетевая система защиты информации вычислительных комплексов

Аннотация. Работа посвящена нейросетевой системе защиты вычислительных комплексов от сетевых атак. Предложены методика защиты информации с использованием нейросетевого подхода, алгоритм анализа сетевого трафика. Представлены результаты тестирования программного обеспечения системы защиты вычислительных комплексов от сетевых атак.

Ключевые слова и фразы: информация, анализ, система, безопасность, защита, искусственная нейронная сеть.

Введение

Вычислительные системы, как правило, имеют сложную топологию и, как следствие, нуждаются в точной системе информационной безопасности, оперативно реагирующей на угрозы [1]. Современные средства защиты от несанкционированного доступа основываются на мониторинге сетевого трафика, позволяют выделять аномалии трафика за счет накопления и дальнейшего использования статистики обращений к серверам и предоставляемым ими сервисам. На сегодняшний день не существует универсальных способов защиты, поэтому есть необходимость создания новых средств, обладающих функциями обеспечения полноценной информационной защиты.

1. Методика защиты информации на базе нейросетевого подхода

Методы защиты данных можно разделить на следующие группы по функциональности:

- препятствие (защита информационных систем от физического проникновения посторонних персон);

Работа выполнена при финансовой поддержке РФФИ (проект № 16–07–00078–А).

DOI: 10.25209/2079-3316-2017-8-4-197-207

- маскировка (преобразование или шифрование исходных данных в данные, невозможные для восприятия посторонними персонами);
- регламентация (комплекс мер, правил и предписаний для персонала, посредством которых должны осуществляться любые действия с охраняемыми данными);
- управление (комплекс наперед установленных правил, которыми осуществляется управление всеми частями системы).

Для построения системы защиты информации, сочетающей в себе перечисленную выше функциональность, предлагается следующий подход:

- оценка имеющихся информационных ресурсов, в том числе их основных компонентов, взаимозависимостей и уязвимостей;
- выдвижение предположений о количестве и типе уязвимостей на основе анализа данных о сети;
- эмуляция атаки на найденные уязвимые ресурсы;
- установка многоступенчатой защиты, включая программы обнаружения вторжений, корпоративные системы управления и сканеры вредоносных кодов;
- разработка средств своевременного предупреждения и информирования о нападениях;
- разработка решений, способствующих прогнозированию активности угроз;
- разработка средств восстановления и обеспечения непрерывной работы сети.

Для построения системы защиты от сетевых угроз предлагается использовать искусственные нейронные сети (ИНС), поскольку они имеют способность к самообучению на нормальном и анормальном сетевом трафике. ИНС могут участвовать в составлении профилей (осуществляя кластеризацию многомерных данных), анализировать весь сетевой трафик, контролировать последовательности вводимых пользователем команд, переходы состояний и пр. На сегодняшний день существует большое количество разработок в этой области. Так, например, в работе [2] описаны результаты исследований разработанной нейросетевой системы обнаружения атак на основе самоорганизующихся карт Кохонена, показано, что нейросетевой подход к решению проблемы защиты информационных сетей достаточно уверенно обнаруживает атаки и при этом имеет низкий показатель ложных срабатываний.

В работе [3] приведен обзор методов и алгоритмов информационной безопасности на основе искусственных нейронных сетей. В работе [4] рассмотрены методы построения модели для ИНС на основе системы обнаружения вторжений «Snort», авторы рассмотрели несколько типов обобщенно-регрессионных сетей и сетей адаптивного резонанса. В работе [5] приведены результаты исследования по оценке и планированию испытаний программных средств системы защиты. Авторами показано, что с поставленной задачей успешно справляются ИНС прямого распространения с четырьмя слоями и искусственные нейронные сети с дополнительными обходными связями. Для защиты информации также широко используются биометрические технологии, в частности, распознавание почерка [6, 7].

На основе выполненного анализа выделим ряд необходимых подсистем перспективной системы защиты:

- подсистема управления доступом — выполняет функции идентификации и проверки подлинности субъектов доступа вычислительной системы; обеспечивает контроль и управление доступом к защищаемым данным в соответствии с заданным уровнем конфиденциальности и правами доступа;
- подсистема регистрации и учета — выполняет функции регистрации, создания, изменения и удаления учетных записей субъектов доступа; регистрации и учета конфиденциальной информации; регистрации изменения полномочий субъектов доступа и общего уровня секретности;
- криптографическая система — осуществляет функции шифрования трафика в сети и конфиденциальной информации на носителях;
- подсистема обеспечения целостности — осуществляет контроль целостности файлов и основных модулей информационной системы.

2. Программное обеспечение анализа сетевого трафика, выявления аномалий и защиты данных

Чтобы решить задачу защиты вычислительных комплексов от сетевых атак методами анализа сетевой активности с применением технологий ИНС, воспользуемся системой «Snort» [8]. Предлагается следующий алгоритм:

- перехваченный средствами «Snort» очередной пакет передается модулям определения отклонений в работе сети передачи данных (СПД);

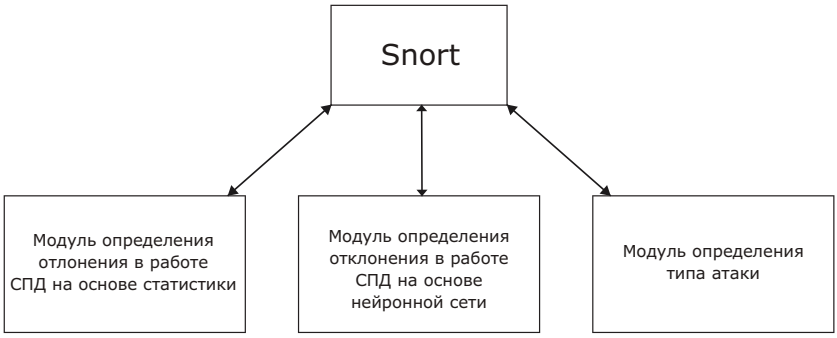


Рис. 1. Структура встраиваемой в «Snort» системы обнаружения и классификации сетевых атак

- модули определения отклонений в работе СПД проверяют наличие сетевой атаки;
- при наличии атаки пакет передается модулю определения класса атаки;
- модуль идентификации типа атаки передает в «Snort» информацию о пакете: «нормальный» / «аномальный»; если модули определения отклонений в работе СПД обнаруживают отклонения, а модуль идентификации типа атаки не может установить причину (класс атаки), то решение о классификации пакета как «нормальный» / «аномальный» будет зависеть от настроечных параметров системы (возможна блокировка всего подозрительного трафика или блокировка только распознанных атак).

Структура системы мониторинга сетевых атак показана на рис. 1.

Для определения типа пакета система использует систему правил. Каждое правило содержит набор параметров, по которым можно определить текущую ситуацию. Важной особенностью предлагаемого решения задачи является то, что модули определения отклонений в работе СПД не расходуют больших ресурсов и поэтому работают быстро. В случае возникновения подозрения на атаку, задействуется модуль определения типа атаки.

3. Нейросетевая система защиты информации вычислительных комплексов от сетевых атак

Для анализа сетевого трафика, выявления аномалий в потоках данных и защиты сетей и вычислительных комплексов от атак разработан экспериментальный образец системы защиты информации, который построен по модульному принципу с поддержкой высокопроизводительных вычислений.

Система выполняет и автоматизирует следующие процессы:

- первичный анализ пакетов, передаваемых по сети, извлечение из них информативных признаков;
- запись новых признаков в базу данных и настроек системы;
- анализ сетевых признаков и предобработка информации;
- классификация пакета в два класса: нормальный / аномальный (или вредоносный);
- в случае подозрения на вредоносный пакет — принятие окончательного решения на основе комитета классификаторов;
- оповещение пользователя и выработка защитных действий.

Предложенная система основана на следующих методах и подходах: распознающие автоматы, методы на основе опорных векторов, байесовский математический аппарат, искусственные нейронные сети различных типов (прямого распространения; вероятностная ИНС; сеть Кохонена с модифицированной метрикой Евклида–Махаланобиса).

Программное обеспечение системы состоит из трех модулей:

- модуль статистического обнаружения сетевых атак;
- модуль нейросетевого обнаружения атак;
- модуль определения типа атак.

4. Модуль статистического обнаружения сетевых атак

Для задач выявления аномалий среди сетевого потока данных необходимо определить некоторую меру аномальности данного потока. Статистический критерий дает числовую меру различия между двумя наборами выборок. Сетевой поток данных характеризуется набором некоторых параметров: загруженность сетевых каналов, сетевые адреса и порты текущих соединений, процентные соотношения используемых протоколов. Для каждой отдельной характеристики

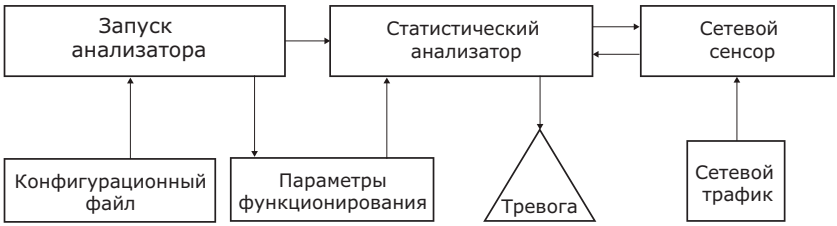


Рис. 2. Архитектура модуля статистического анализа сетевого трафика

текущий набор значений параметров можно представлять как случайную выборку $(x_1, \ldots, x_n)$. Данной выборке соответствует некоторая эмпирическая функция распределения F_X. Далее предполагается, что «нормальный» сетевой поток данных имеет четкое распределение F, которое мы умеем описывать. Если набор величин, характеризующий поток сетевых данных, имеет другое распределение $\{F_X \neq F\}$, то считаем, что в сети происходит подозрительная активность. Если же верно, что $\{F_X = F\}$, то считаем, что набор параметров $(x_1, \ldots, x_n)$ является «нормальным».

На рис. 2 приведена архитектура модуля статистического анализа характеристик трафика.

5. Модуль нейросетевого обнаружения сетевых атак

Для решения задачи обнаружения сетевых атак создан модуль нейросетевого анализа характеристик трафика, который предназначен для обеспечения безопасности функционирования информационной системы путем мониторинга и анализа на аномальность ключевых характеристик сетевого трафика. Реализованы функции, которые позволяют на основе методов машинного обучения производить обучение модуля нейросетевого анализа характеристик трафика в три этапа:

- сбор информации, характеризующей поведение системных приложений в штатном режиме функционирования сети;
- формирование обучающего множества для нейронной сети и ее обучение на этом множестве;
- непосредственно обучение нейронной сети.

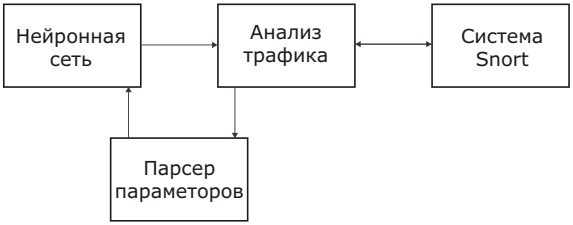


Рис. 3. Архитектура модуля определения типа сетевых атак

6. Модуль определения типа сетевых атак

Модуль определения сетевых атак производит регистрацию атак с использованием нейронной сети в системе «Snort». Архитектура модуля определения сетевых атак показана на рис. 3.

Приведем алгоритм обнаружения и классификации атак:

- перехват сетевого пакета системой «Snort»;
- анализ полученного пакета и вызов модуля определения сетевых атак для определения характера пришедшего пакета;
- модуль определения сетевых атак анализирует полученный пакет и выделяет информативные признаки, которые подаются на распознавание ИНС;
- ИНС анализирует полученные данные и возвращает в модуль определения сетевых атак класс принадлежности пакета;
- модуль определения типа сетевых атак возвращает в систему «Snort» значение характеризующее пакет как «аномальный» / «не аномальный», после чего «Snort» либо отсеивает пакет, либо передает по назначению как безопасный.

7. Результаты тестирования нейросетевой системы защиты информации вычислительных комплексов

Подготовка обучающей и тестовой выборок производится с использованием разработанной подсистемы сохранения сетевых признаков, подключаемой в качестве модуля к системе «Snort», и организации типовых атак с наперед заданных и известных сетевых узлов. Для имитации сетевых атак различных классов были использованы несколько специализированных утилит. Так, пакеты класса Nmap генерирует программное обеспечение «Zenmap»; для генерации сетевых пакетов класса DoS была использована утилита «TCP/IP DoS Attacker».

В ходе тестирования системы распознавания сетевых атак были получены следующие результаты (приведены средние значения по серии запусков):

- полнота классификации класса Nmap — 98.7%;
- точность классификации класса Nmap — 99.2%;
- полнота классификации класса DoS — 99.3%;
- точность классификации класса DoS — 99.1%.

Для решения поставленных задач применялась программно-аппаратная среда, ориентированная на организацию конвейерно-параллельных вычислений [9] со следующими характеристиками:

- материнская плата: MSI X99A SLI PLUS;
- процессор: Intel Socket 2011V3 Core i76850K;
- видеокарты: 2 x Geforce GTX 1060 6 ГБ GDDR5;
- ОЗУ: 4 x Corsair CMK8GX4M1A2666C16R (32 ГБ).

Заключение

Принятый вариант технического решения по созданию нейросетевой программной системы продемонстрировал высокую точность и полноту решения задач анализа и защиты информации вычислительных комплексов. Эффективность принятой архитектуры системы обуславливается модульной моделью с возможностью модификации отдельных компонент, возможностью конвейерно-параллельной обработки данных, возможностью использования высокопроизводительных платформ и использованием аппарата ИНС, который зарекомендовал себя как высокоточный и быстрый инструмент для решения задачи классификации.

Список литературы

[1] Ю. Г. Емельянова, В. П. Фраленко. «Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления», *Программные системы: теория и приложения*, 2011, №4, с. 17–31, URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf ↑ 197

[2] А. Ю. Балахонцев, Д. В. Сидорик, А. Н. Сидоревич, М. В. Якутович. «Нейросетевая система для обнаружения атак в локальных вычислительных сетях», *Сборник работ 62-й научной конференции студентов и аспирантов Белгосуниверситета*, в 3 ч.. Т. 2 (17 –20 мая 2005 г., г. Минск), ред. А. Г. Захаров и др., БГУ, Минск, 2005, с. 119–122. ↑ 198

[3] Г. А. Марков. «Использование технологий нейронных сетей при решении задач информационной безопасности», *Молодежный научно-технический вестник*, 2014, №3, 11 с., URL: http://sntbul.bmstu.ru/file/out/717971 ↑ 199

[4] А. В. Гришин. «Нейросетевые технологии в задачах обнаружения компьютерных атак», *Информационные технологии и вычислительные системы*, 2011, №1, с. 53–64, URL: http://www.isa.ru/jitcs/images/documents/2011-01/53_64.pdf ↑ 199

[5] Г. А. Марков. «Планирование испытаний программ с открытым кодом с помощью нейросетевых технологий», *Труды Международного симпозиума «Надежность и качество»*. Т. 1 (26 мая–1 июня 2014, г. Пенза), 2014, с. 383–385. ↑ 199

[6] В. И. Волчихин, А. И. Иванов. «Естественное использование искусственных нейронных сетей в биометрии», *Системы безопасности*, 2002, №3(45), с. 46–47. ↑ 199

[7] В. А. Галкин, С. Н. Чернуха. «Исследование быстродействия нейросетевого распознавателя почерка», *Наука и образование: электронное научно-техническое издание*, 2011, №12, 16 с., URL: http://technomag.bmstu.ru/file/out/505021 ↑ 199

[8] *Snort — Network Intrusion Detection & Prevention System* (english), URL: http://www.snort.org ↑ 199

[9] А. А. Талалаев. «Организация конвейерно-параллельных вычислений для обработки потоков данных», *Информационные технологии и вычислительные системы*, 2011, №1, с. 8–13, URL: http://www.isa.ru/jitcs/images/documents/2011-01/8_13.pdf ↑ 204

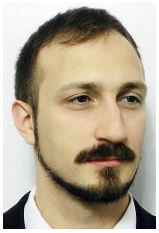
Рекомендовал к публикации *д.т.н., проф. В. М. Хачумов*

Пример ссылки на эту публикацию:

Н. С. Абрамов, В. П. Фраленко. «Нейросетевая система защиты информации вычислительных комплексов», *Программные системы: теория и приложения*, 2017, **8**:4(35), с. 197–207.

URL: http://psta.psiras.ru/read/psta2017_4_197-207.pdf

Об авторах:



Николай Сергеевич Абрамов

К.т.н., старший научный сотрудник ИЦМС ИПС им. А.К. Айламазяна РАН. Область научных интересов: математические методы синтеза, обработки и анализа изображений и сигналов, искусственный интеллект и принятие решений, интеллектуальный анализ данных и распознавание образов, геометрия.

e-mail: n-say@nsa.pereslavl.ru

Виталий Петрович Фраленко

К.т.н., старший научный сотрудник ИЦМС ИПС им. А.К. Айламазяна РАН, автор более 80 публикаций. Область научных интересов: интеллектуальный анализ данных и распознавание образов, искусственный интеллект и принятие решений, параллельные алгоритмы, сетевая безопасность, диагностика сложных технических систем.

e-mail: alarmod@pereslavl.ru

Nikolai Abramov, Vitaly Fralenko. *Neural network data protection system for computer systems.*

Abstract. The work is devoted to the neural network protection against network attacks for computer systems. The methods of information protection using the neural network approach, the algorithm of the analysis of network traffic are offered. The results of software testing are presented. (*In Russian*).

Key words and phrases: information, analysis, system, security, protection, artificial neural network.

References

[1] Yu. G. Yemel'yanova, V. P. Fralenko. "Problems and prospects analysis for cloud computing network attacks detection and prevention intelligent system creation", *Program Systems: Theory and Applications*, 2011, no.4, pp. 17–31 (in Russian), URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf

DOI: 10.25209/2079-3316-2017-8-4-197-207

[2] A. Yu. Balakhontsev, D. V. Sidorik, A. N. Sidorevich, M. V. Yakutovich. “Neural network system for detecting attacks in local area networks”, *Sbornik rabot 62-y nauchnoy konfrentsii studentov i aspirantov Belgosuniversiteta*, v 3 ch.. V. 2 (17 –20 maya 2005 g., g. Minsk), eds. A. G. Zakharov i dr., BGU, Minsk, 2005, pp. 119–122 (in Russian).

[3] G. A. Markov. “Use of neural network technologies in solving information security problems”, *Youth Scientific and Technical Bulletin*, 2014, no.3 (in Russian), 11 p., URL: http://sntbul.bmstu.ru/file/out/717971

[4] A. V. Grishin. “Neural network technologies in the tasks of detecting computer attacks”, *Information Technologies and Computer Systems*, 2011, no.1, pp. 53–64 (in Russian), URL: http://www.isa.ru/jitcs/images/documents/2011-01/53_64.pdf

[5] G. A. Markov. “Planning testing of open source programs using neural network technologies”, *Proc. of International Symposium “Reliability and Quality”*. V. 1 (26 maya–1 iyunya 2014, g. Penza), 2014, pp. 383–385 (in Russian).

[6] V. I. Volchikhin, A. I. Ivanov. “The natural use of artificial neural networks in biometrics”, *Security Systems*, 2002, no.3(45), pp. 46–47 (in Russian).

[7] V. A. Galkin, S. N. Chernukha. “Research of speed of the neural network handwriting recognizer”, *Science & Education: Scientific Edition of Bauman MSTU*, 2011, no.12 (in Russian), 16 p., URL: http://technomag.bmstu.ru/file/out/505021

[8] *Snort — Network Intrusion Detection & Prevention System* (english), URL: http://www.snort.org

[9] A. A. Talalayev. “Organization of parallel-pipeline computing for data flow processing”, *Information Technologies and Computer Systems*, 2011, no.1, pp. 8–13 (in Russian), URL: http://www.isa.ru/jitcs/images/documents/2011-01/8_13.pdf

Sample citation of this publication:

Nikolai Abramov, Vitaly Fralenko. “Neural network data protection system for computer systems”, *Program systems: Theory and applications*, 2017, **8**:4(35), pp. 197–207. (*In Russian*).

URL: http://psta.psiras.ru/read/psta2017_4_197-207.pdf