РАЗДЕЛ XVII. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Абрамов Н.С., Фраленко В.П.

Нейросетевая система защиты вычислительных комплексов от сетевых атак

*Федеральное государственное бюджетное учреждение науки Институт программных систем им. А.К. Айламазяна Российской академии наук
(Россия, Переславль-Залесский)*

doi:10.18411/lj-09-2018-86

idsp: 000001:lj-09-2018-86

Аннотация

В работе описана нейросетевая система защиты вычислительных комплексов от сетевых атак. Предложен метод анализа сетевого трафика. Представлены результаты тестирования программного обеспечения системы защиты вычислительных комплексов от сетевых атак.

Ключевые слова: информация, сетевая атака, анализ, защита, безопасность, искусственная нейронная сеть

На сегодняшний день не существует универсальных способов защиты вычислительных комплексов от сетевых атак в силу высокой сложности и разнообразия топологий сетей и постоянно развивающихся и меняющихся сетевых угроз [1]. Современные средства защиты от несанкционированного доступа основываются на контроле сетевого трафика, выделении аномалий в анализируемых данных, накоплении базы знаний, статистических и интеллектуальных методах, в том числе, с применением технологий искусственных нейронных сетей (ИНС) [2-5]. Обеспечение информационной безопасности на данный момент является одной из приоритетных задач в области развития коммуникаций в связи с распространенностью глобальной сети и применения сетевых технологий в разных сферах деятельности.

Для решения задач защиты вычислительных комплексов применяют специализированные экспертные системы, содержащие в себе набор правил, на основе которых производится анализ и классификация текущей сетевой активности. Правила формируются в виде сигнатуры, в качестве которой может выступать либо шаблон действий, либо последовательность символов, и другие признаки, в совокупности характеризующие аномальную деятельность [6].

Средства защиты должны с высокой точностью диагностировать наличие атаки, уметь определять неизвестные типы атак, обладать высокой скоростью работы и иметь возможность адаптации к новым условиям и типам атак. В настоящей работе описаны результаты тестирования разработанной системы защиты вычислительных комплексов от сетевых атак на основе нейросетевого подхода [7].

Для анализа сетевого трафика и выявления аномалий в сети передачи данных (СПД) разработан экспериментальный образец нейросетевой системы защиты вычислительных комплексов от сетевых атак («НС Бастион»), основывающийся на системе «Snort» [8]. Система «НС Бастион» построена по модульному принципу и поддерживает высокопроизводительные вычисления. Схема работы представлена на рис.1.

Рисунок 1 – Структура системы обнаружения и классификации сетевых атак

Система выполняет следующие функции:

- первичный анализ сетевых пакетов, извлечение из них информативных признаков;
- запись новых признаков в базу данных и настроек системы;
- классификация пакета в два класса: нормальный / аномальный на основе комитета классификаторов;
- оповещение пользователя и выработка защитных действий в случае обнаружения аномального трафика.

Разработанная система основана на следующих методах и подходах: распознающие автоматы, методы на основе опорных и релевантных векторов, искусственные нейронные сети различных типов (прямого распространения; вероятностная ИНС; сеть Кохонена; комбинированные сети) и др. Программное обеспечение системы состоит из трех модулей: модуль статистического обнаружения сетевых атак, модуль нейросетевого обнаружения атак и модуль определения типа атак.

Подготовка обучающей и тестовой выборки 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 проведения испытаний выбраны следующие типы вредоносного воздействия: DoS, Nmap, HTTP-exploit и SNScan.

В ходе доработки и тестирования системы распознавания сетевых атак, были получены новые результаты, представленные в сравнении с подобными системами в табл.1 (приведены средние значения точности и полноты классификаторов по серии запусков).

Таблица 1.

Результаты тестирования системы защиты от сетевых атак

	Норма		Dos		Nmap		HTTP-exploit		SNScan	
	точность, % полнота, %									
IDSSnort	100	99.8	100	0.002	100	0.08	100	5	100	85.9
IDSBro	100	99.9	100	40.7	100	0.01	94.9	100	100	0.05
НС Бастион	100	100	100	100	100	99.9	100	100	100	99.6

Общий алгоритм работы комплекса осуществляется согласно схеме, отображенной на рис.2.

Рисунок 2 – Схема работы программного комплекса

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

- материнская плата: MSI X99A SLI PLUS;
- процессор: Intel Core i7-6850K 3.6 @ 4.0 ГГц;
- ОЗУ: 4 x Corsair CMK8GX4M1A2666C16R (32 ГБ).

Принятый вариант технического решения по созданию нейросетевой программной системы продемонстрировал высокую точность и полноту решения задач анализа и защиты информации вычислительных комплексов. Преимуществом принятого подхода

является гибкость настройки алгоритмов работы и возможность дообучения нейросетевых классификаторов, в том числе, на модифицированных известных и новых типах сетевых атак. Результаты экспериментов с разработанной системой защиты вычислительных комплексов от сетевых атак в очередной раз показали эффективность использования аппарата ИНС, который зарекомендовал себя как высокоточный и быстрый инструмент для решения задач классификации в разных областях.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 16-07-00078-а «Разработка и исследование нейросетевых методов обеспечения безопасности и защиты информации вычислительных комплексов»).

1. Емельянова Ю.Г., Фраленко В.П. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления. – Программные системы: теория и приложения, №4, 2011, с.17-31.
2. Марков Г.А. Использование технологий нейронных сетей при решении задач информационной безопасности. – Молодежный научно-технический вестник, №03, 2014. URL: <http://sntbul.bmstu.ru/file/717971.html> (дата обращения: 26.09.2018).
3. Гришин А.В. Нейросетевые технологии в задачах обнаружения компьютерных атак. – Информационные технологии и вычислительные системы, №1, 2011, с.53-64.
4. Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М. Разработка нейросетевого модуля для мониторинга аномальной сетевой активности. – Нейрокомпьютеры: разработка, применение, №7, 2011, с.32-38.
5. Кондратьев А.А., Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М. Методологическое обеспечение интеллектуальных систем защиты от сетевых атак. – Современные проблемы науки и образования, №2, 2014. URL: <https://www.science-education.ru/pdf/2014/2/610.pdf> (дата обращения: 26.09.2018).
6. Лукацкий А.В. Системы обнаружения атак. Взгляд изнутри. – Центр информационной безопасности. URL: <http://www.bezpeka.com/ru/lib/sec/ids.html> (дата обращения: 26.09.2018).
7. Абрамов Н.С., Фраленко В.П. Нейросетевая система защиты информации вычислительных комплексов. – Программные системы: теория и приложения, №4, 2017, с.197-207.
8. Snort – Network Intrusion Detection & Prevention System. URL: <https://www.snort.org/> (дата обращения: 26.09.2018).
9. Талалаев А.А., Фраленко В.П. Отказоустойчивая система организации высокопроизводительных вычислений для решения задач обработки потоков данных. – Программные системы: теория и приложения, №1, 2018, с.85-108.

Ерохин В.В.

Проектирование систем электронного документооборота вуза

*ФГАОУ ВО Московский государственный институт международных отношений
(университет) Министерства иностранных дел Российской Федерации
(Россия, Москва)*

doi:10.18411/lj-09-2018-87

idsp: 000001:lj-09-2018-87

Аннотация

В статье приводятся основные аспекты внедрения систем электронного документооборота в вузах. Рассмотрены модели и инструментальные средства на базе современных IT-технологий (в виде XML- и smart-технологий) для управления электронного документооборота вуза. Представлены тенденции по синтезу объединенной информационной системы для поддержки учебной, финансовой и управленческой деятельности вуза.

Ключевые слова: обучение, электронный документооборот, информационная система, оптимизация, программное обеспечение, моделирование.