DOI: 10.12737/article_5940f01ab85752.95859922

Буханов Д.Г., аспирант, инженер,
Поляков В.М., канд. техн. наук, доц.,
Смакаев А.В., аспирант
Белгородский государственный технологический университет им. В.Г. Шухова

ОПРЕДЕЛЕНИЕ СОСТОЯНИЯ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ НЕЙРОННЫХ СЕТЕЙ АРТ

db.old.stray@gmail.com.

Предлагается подход к созданию системы обнаружения вторжений, работающей на основе анализа параметров сетевого трафика с применением нейронной сети на базе адаптивно-резонансной теории. Проведен эксперимент по обнаружению и распознаванию классов сетевых атак на тестовой выборке. Результаты эксперимента показывают целесообразность использования нейронных сетей адаптивно-резонансной теории для анализа сетевого трафика в системе обнаружения вторжений.

Ключевые слова: *нейронная сеть АРТ-2, система обнаружения вторжений, информационная безопасность.*

Введение. Согласно анализу кибер-атак 2015–2016 годов, выполненному компанией Positive Technologies, “нарушители все реже прибегают к атакам с эксплуатацией уязвимостей нулевого дня, переходя на более простые методы проникновения” [1]. Лишь в 20 % случаев использовались так называемые уязвимости нулевого дня, при этом среднее время присутствия атакующих в системе увеличилось до 3 лет [2]. Это показывает, что несмотря на важность обеспечения защиты компьютерных сетей, эта задача до сих пор не имеет доступного и качественного метода решения.

Среди существующего множества средств обеспечения информационной безопасности особо выделяются системы обнаружения вторжений (СОВ) [3]. Их особенностью является комплексный подход к сбору и анализу данных, что позволяет охватить наибольший спектр угроз, в числе которых несанкционированный доступ к ресурсам сети, атаки отказа в обслуживании (DDoS) и т.д. Любая СОВ включает в себя две обязательные подсистемы - сенсорную и аналитическую. Вне зависимости от устройства сенсорной подсистемы, аналитическая является ядром СОВ и от ее эффективности зависит работа всей системы.

Для анализа сетевого трафика в СОВ используют различные подходы. В [4] авторы предлагают использовать для анализа методы, основанные на нечеткой логике, но использование таких подходов предполагает выполнение дополнительных действий, таких как: создание лингвистических переменных, составление базы правил и, как правило, требует наличие эксперта в данной предметной области.

В настоящее время, наиболее интенсивно развивающимся разделом интеллектуальных методов анализа данных являются искусственные нейронные сети [5]. Их применение в данной области считается наиболее перспективным.

В [6] предлагается использовать двухэтапную обработку входящей информации – на первом этапе происходит уменьшение размерности вектора входных данных при помощи нелинейной рециркуляционной нейронной сети, а на втором этапе – обнаружение атак с использованием многослойного перцептрона, который осуществляет обработку сжатого пространства входных образов с целью распознавания класса атаки. Такой подход требует предварительный анализ параметров сети для создания нелинейной рециркуляционной нейронной сети.

Авторы статьи [7] предлагают свести задачу обучения нейросетевой системы к поиску и извлечению информативных признаков, их сжатию с помощью метода главных компонент, дальнейшей обработки с помощью рециркуляционной нейронной сети и применение двухслойного перцептрона или сети Кохонена на базе выделенных информационных векторов признаков. Существенным недостатком в этом случае является существенное увеличение временной сложности при обучении сети распознаванию новых видов сетевых атак.

В данной работе предлагается структура СОВ и использование искусственной нейронной сети на основе адаптивно-резонансной теории (АРТ) для решения задачи анализа трафика.

1. Описание общей системы обнаружения сетевых атак

На рис. 1 изображена общая схема системы обнаружений и противодействия сетевым атакам в локальных вычислительных сетях.

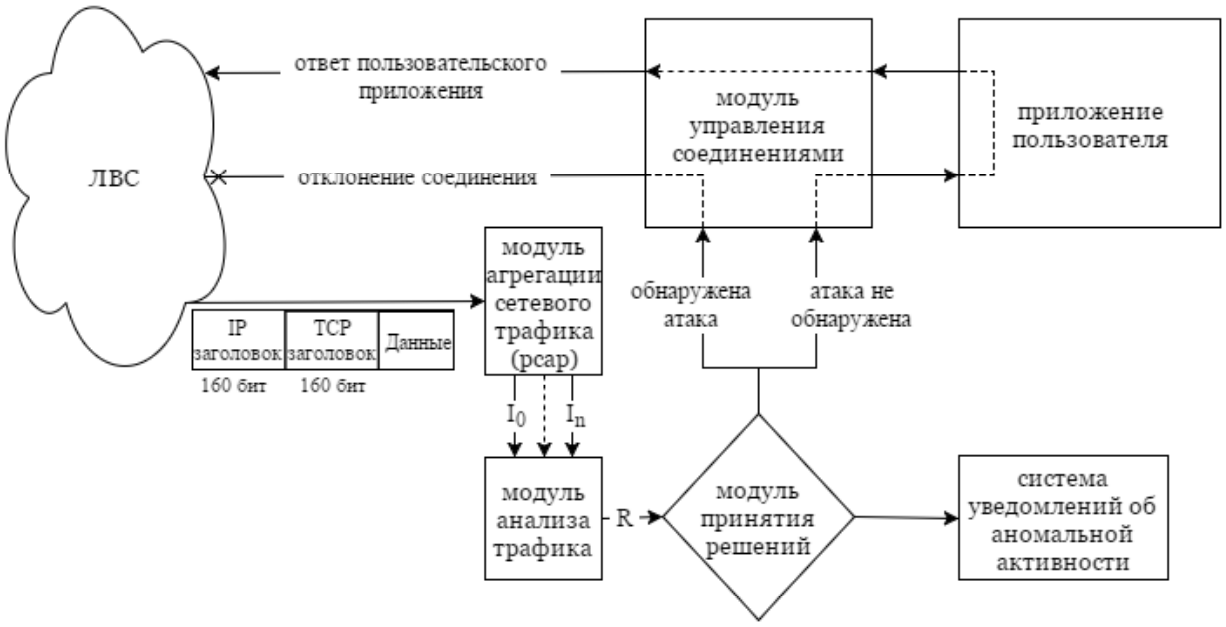

Рис. 1. Общая схема системы обнаружения сетевых атак

Модуль агрегации сетевого трафика используется для перехвата сетевых пакетов и их анализа на принадлежность конкретному соединению. После выполнения этих действий происходит обновление анализируемых параметров соответствующего соединения.

Модуль анализа трафика включает в себя нейронную сеть на основе адаптивно-резонансной теории. Для данной системы была выбрана сеть АРТ-2, позволяющая работать с входными векторами, состоящими из вещественных чисел. Сеть осуществляет определение принадлежности соединения к группе сетевых соединений, характерных для нормального или аномального состояния сети. Под аномальным состоянием сети понимается состояние, при котором выполняется противоправные действия, т.е. совершается одна из сетевых атак, рассмотренных в выборке KDD'99.

Результат работы модуля анализа передается в модуль принятия решений. На основе результата анализа он либо отклоняет соединение и уведомляет администратора об атаке, либо позволяет модулю управления соединениями передать пакет приложению пользователя для дальнейшей обработки. Модули принятия решений образуют распределенную систему, предназначенную для согласования действий и дообучения нейронных сетей.

2. Анализ сетевого трафика на основе АРТ-2

Для сбора сетевого трафика используется библиотека PCap (Packet Capture) [9]. Применение библиотеки PCap позволяет значительно снизить время получения и регистрации трафика. В работе [10] приведен пример использования драйвера PCap и его модификации WinPCap.

Для дальнейшего анализа в работе предлагается выделять 41 параметр трафика, согласно описанию, составленному на конференции International Knowledge Discovery and Data Mining Tools Competition [8].

Общие положения АРТ-2 выдвинуты С. Гроссбергом и подробно изложены в его работах [11–13]. Дальнейшее применение сетей АРТ изложено в работах [14, 15]. Основная идея заключается в том, что распознавание векторов данных, описывающих различные образы, является результатом частичного или полного соответствия состояния весов одного из обученных распознающих нейронов входному нормализованному вектору, т.е. вхождения в резонанс сенсорного и распознающего слоев сети. Возникший резонанс оценивается управляющими нейронами. Если он достаточен, т.е. превышает заранее определенный порог, то считается, что соответствие между вектором входных данных и образом из памяти сети установлено. Иначе управляющий слой замораживает резонировавший нейрон распознающего слоя и процедура распознавания повторяется. Если в конце все нейроны распознающего слоя оказываются заморожены, то в этот слой добавляется новый нейрон и его веса обучаются таким образом, чтобы он с достаточной степенью соответствовал вектору входных данных, т.е. происходит дообучение сети.

На рис. 2 изображена схема нейронной сети АРТ-2. Данная сеть принимает на вход вектора вещественных чисел.

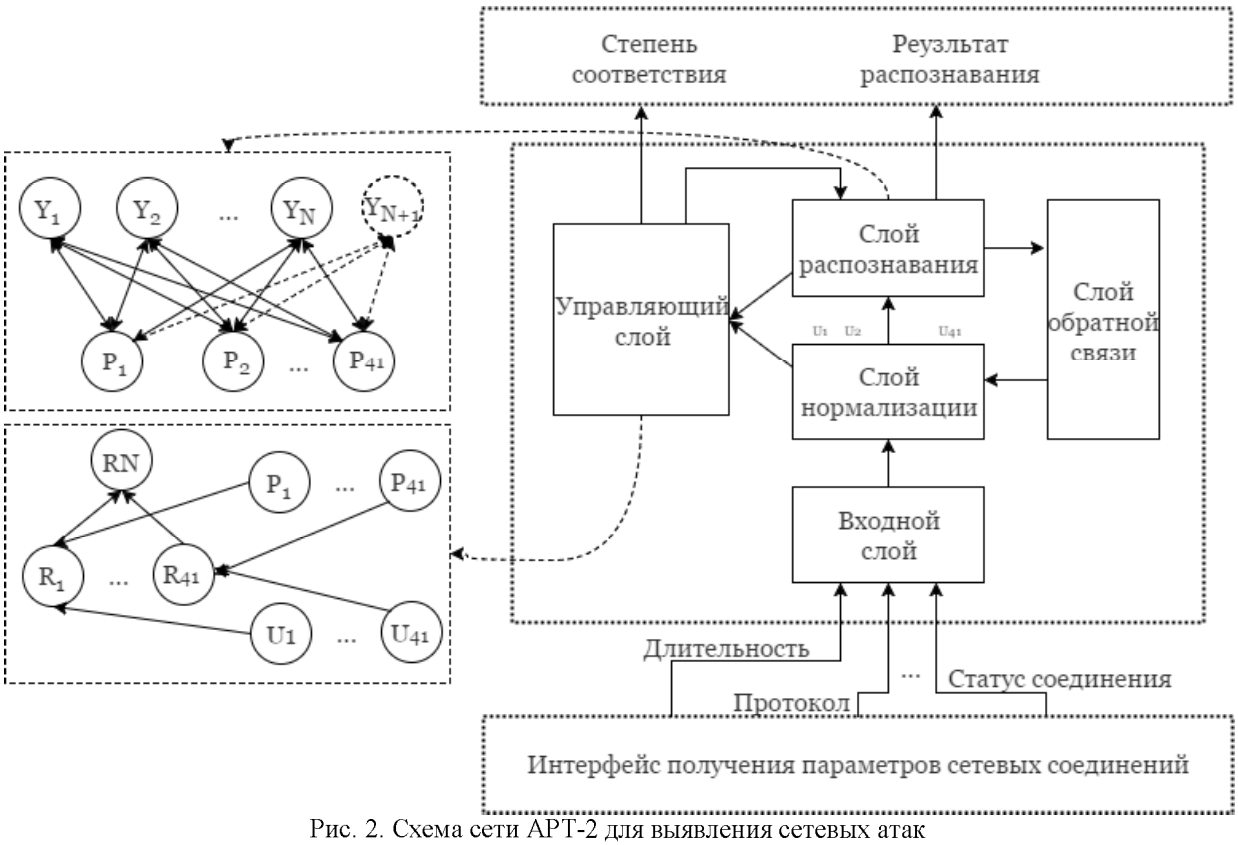

Рис. 2. Схема сети АРТ-2 для выявления сетевых атак

Каждый входной вектор содержит 41 сетевой параметр, выделенный из сетевого трафика. Далее в блоке нормализации происходит нормировка входных данных. Полученный вектор объединяется с информацией из обратной связи с распознающим слоем.

После нормализации данные попадают в группу нейронов *P* распознающего слоя. Далее вычисляется значения нейронов слоя *Y* на основании соответствующих весов связей от *P* к *Y*.

$$Y_j = P_i \times z_{ij} \quad (1)$$

где z_{ij} – вес связи от P_i к Y_j; $j = (1..N)$, $i = (1..41)$; *N* – количество нейронов слоя *Y*.

Среди нейронов слоя *Y* определяется наибольшее значение. Затем корректируются нейроны *P* слоя с использованием весов связей от выбранного максимального нейрона *Y* слоя.

$$m = \max(Y) \quad (2)$$

$$P_i = U_i + d \times z_{mi} \quad (3)$$

где *max()* – функция, возвращающая индекс максимального нейрона из слоя *Y*; $i = (1..41)$; U_i – выходной нейрон слоя нормализации, *d* – константа, принятая 0,9.

Полученный результат оценивается посредством вычисления выходных значений группы нейронов R_i управляющего слоя из значений выходных векторов нормализующего и распознающего слоев.

$$R_i = U_i + c \times P_i \quad (4)$$

где $i = (1..41)$, $c = 0,1$.

Далее вычисляется норма *RN* вектора *R* и определяется ее соответствие пороговому значению. Если *R* не удовлетворяет пороговому значению, то выбранный нейрон *Y* слоя замораживается, и процедура распознавания повторяется еще раз без его участия, пока не будут заморожены все нейроны или пока не будет найден такой результат распознавания, который удовлетворял бы пороговому значению.

$$RN = \|R\| \quad (5)$$

$$\frac{vagilance}{eps+RN} < 1 \quad (6)$$

где *vagilance* – пороговое значение, *eps* – малое число, для предотвращения деления на ноль.

Если в результате повторного выполнения процедуры распознавания все нейроны *Y* распознающего слоя оказываются заморожены, то к нейронам *Y* слоя добавляется новый нейрон и происходит обучение весов его связей с нейронами слоя *P*.

Для решения задачи анализа трафика и обнаружения сетевых атак сети АРТ-2 обладают следующими ключевыми особенностями:

– возможность создания нового класса распознаваемых векторов в случае несоответствия входного вектора ни одному из существующих классов;

– отсутствие необходимости полного переобучения сети для добавления новой информации;

– в весах каждого нейрона распознающего слоя хранится только одно изображение, полученное в результате выделения общих свойств

изображений обучающей выборки.

3. Результаты применения АРТ-2 сети для решения задачи обнаружения сетевых атак

Нейронная сеть на базе АРТ была обучена на выборке, состоящей из 489 296 векторов данных. Эксперимент проводился на тестовой выборке размером в 2 351 447 векторов. В таблице 1 представлены общие результаты распознавания классов атак. В случае, если система обнаруживала атаку, но не верно указывала группу, к которой она принадлежит, то считалось, что атака обнаружена неверно.

Таблица 1

Результаты эксперимента по распознаванию состояния сети

Класс <группы>	Точность
normal < normal >	0.96
dos <back, land, neptune, pod, smurf, teardrop>	0,913
u2r < buffer_overflow, loadmodule, perl, rootkit>	0,48
r2l < ftp_write, guess_password, imap, multihop, phf, warezmaster>	0
probe < ipsweep, nmap, portsweep, satan>	0,805

На рис. 3 показаны результаты эксперимента по распознаванию состояния сети, где по оси абсцисс расположены названия групп атак, а по оси ординат - точность определения конкретного состояния сети. Из результатов видно, что не все классы атак были распознаны достаточно хорошо. Следует отметить, что такие атаки как warezmaster и ipsweep составляют в сумме около 0.003 % выборки, соответствующим образом они были представлены и в обучающей выборке. Таким образом, для обучения сети распознаванию атак этого типа было недостаточно образцов, однако, вследствие их редкости можно пренебречь ошибкой в их распознавании.

Основной группой атак в тестовой выборке были dos-атаки. Атаки этой группы были обнаружены и правильно классифицированы с ошибкой всего в 0.15 %. Следующей по величине группой состояний сети является нормальное состояние - ошибка при его распознавании составила 3.6 %.

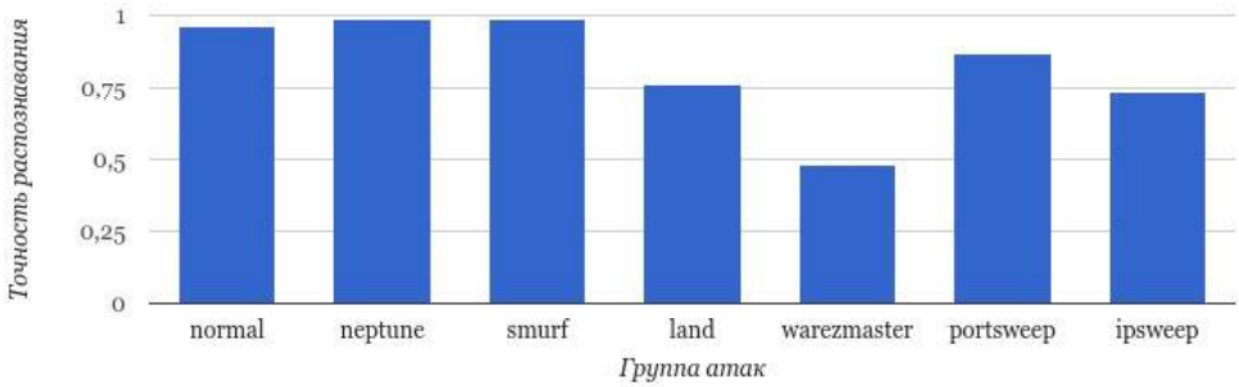

Рис. 3. Подробные результаты эксперимента по распознаванию состояния сети

В [6] производился эксперимент с сетями Кохоннена и двухслойным перцептроном на такой же тестовой выборке KDD'99. Авторы статьи производили обучение сети на полной тестовой выборке, о чем свидетельствуют показатели полноты в результатах их экспериментов. В большинстве случаев полнота обучающей выборки в работе [6] была на порядок выше, чем в эксперименте, проведенном в данной работе. При этом точность определения наиболее распространенных классов атак сетью АРТ-2 оказывается не хуже, чем сетями Кохоннена и двухслойным перцептроном. Низкие показатели для атак группы teardrop, nmap и back объясняются малым количеством этих атак как в обучающей, так и в полных выборках.

Заключение.

В ходе исследования был предложен подход к разработке СОВ, отличительной особенностью которого является использование сетей адаптивно-резонансной теории для анализа параметров сетевых соединений. Сетевое соединение представляет собой кортеж из 41 параметра. Данные параметры являются, как частями принятых пакетов (флаги пакетов), так и статистически накапливаемыми характеристиками сетевых соединений(например, время соединения). В качестве технологии распознавания состояния сети использовалась искусственная нейронная сеть АРТ-2, основным преимуществом которой

является возможность классификации новых образов без переобучения ранее запомненных.

Были проведены эксперименты с применением тестовый выборки KDD'99. Общие результаты эксперимента, а также их сравнительный анализ с результатами аналогичных экспериментов показывают возможность применения АРТ-2 для обнаружения и классификации сетевых атак в модуле анализа сетевых данных в составе системы обнаружения вторжений.

В ходе работы было выявлено два недостатка нейронной сети на базе АРТ-2: сложность организации параллельных вычислений и долгий поиск активного нейрона из слоя Y. Целесообразно разработать модификацию АРТ-2 с целью изменения структуры памяти сети для эффективного решения описанных проблем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ключевые тенденции кибератак 2015 года по версии Positive Technologies [электронный ресурс] – открытый доступ, URL: http://www.securitylab.ru/news/476333.php (дата обращения: 30.04.2017)

2. КИБЕРБЕЗОПАСНОСТЬ 2016-2017: ОТ ИТОГОВ К ПРОГНОЗАМ [электронный ресурс] – открытый доступ, URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf (дата обращения: 30.04.2017)

3. Мельников Д. Информационная безопасность открытых систем. М.: Изд. Litres, 2015, 448 с.

4. Марьенков А.Н., Ажмухамедов И.М. Обеспечение информационной безопасности компьютерных сетей на основе анализа сетевого трафика //Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2011. №. 1. С. 141–148.

5. Марков Р.А. Исследование нейросетевых технологий для выявления инцидентов информационной безопасности //Молодой ученый, 2015. №23. С. 55–60.

6. Головко В.А., Безобразов С.В. Проектирование интеллектуальных систем обнаружения аномалий //Труды международной научно-технической конференции" Открытые семантические технологии проектирования интеллектуальных систем", OSTIS. 2011. С. 185–196.

7. Емельянова Ю. Г., Талалаев А. А., Тищенко И. П., Фраленко В. П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: теория и приложения. 2011. Т.2. №3. С. 3–15.

8. KDD-99 International Conference on Knowledge Discovery and Data Mining [электронный ресурс] – открытый доступ, URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (дата обращения: 1.05.2017)

9. Risso F., Degioanni L. An architecture for high performance network analysis //Computers and Communications, 2001. Proceedings. Sixth IEEE Symposium on. – IEEE. 2001. P. 686–693.

10.Буханов Д. Г., Поляков В. М., Усков Д. А., Даееф Ф. Обнаружение SYN Flood атаки с использованием драйвера WinPCap //ISJ Theoretical & Applied Science. 2015. Т.1. №. 21. С. 139–144.

11.Carpenter G. A., Grossberg S. Category learning and adaptive pattern recognition: A neural network model // Proceedings, Third Army Conference on Applied Mathematics and Computing, ARO Report. 1985. P. 86–101.

12.Carpenter G. A., Grossberg S. ART 2: Self-organization of stable category recognition codes for analog input patterns //Applied optics. 1987. Т. 26. №23. С. 4919–4930.

13.Carpenter G. A., Grossberg S., Rosen D. B. ART 2: An adaptive resonance algorithm for rapid category learning and recognition //Neural networks. 1991. Т. 4. №4. P. 493–504.

14.Дмитриенко В.Д., Терёхина В.М., Заковоротный А.Ю. Вычислительное устройство для распознавания режимов функционирования динамических объектов // Вестник Национального технического университета Харьковский политехнический институт. Серия: Информатика и моделирование. 2004. №34. С.70-81.

15.Дмитриенко В.Д., Леонов С.Ю. Разработка К-значных нейронных сетей АРТ с несколькими полями обрабатывающих нейронов //Наука і техніка Повітряних Сил Збройних Сил України. 2015. №1. С. 166–170.

Bukhanov D.G., Polaykov V.M., Smakaev A.V.

DETERMINATION OF COMPUTER NETWORK STATUS BASED ON ART NEURAL NETWORKS

Proposed an approach to create an intrusion detection system that based on analysis of network traffic parameters using a neural network of the adaptive resonance theory. An experiment was made to detect and recognize classes of network attacks on a test sample. The results of the experiment show the feasibility of using neural networks of adaptive resonance theory to analyze network traffic in an intrusion detection system.

***Key words**: neural network ART-2, intrusion detection system, information Security.*

Буханов Дмитрий Геннадьевич, аспирант кафедры программного обеспечения вычислительной техники и автоматизированных систем.
Белгородский государственный технологический университет им. В.Г. Шухова.
Россия, 308012, Белгород, ул. Костюкова, д. 46.
E-mail: db.old.stray@gmail.com.

Поляков Владимир Михайлович, кандидат технических наук, зав. кафедры программного обеспечения вычислительной техники и автоматизированных систем.
Белгородский государственный технологический университет им. В.Г. Шухова.
Россия, 308012, Белгород, ул. Костюкова, д. 46.

Смакаев Анатолий Витальевич, аспирант кафедры программного обеспечения вычислительной техники и автоматизированных систем.
Белгородский государственный технологический университет им. В.Г. Шухова.
Россия, 308012, Белгород, ул. Костюкова, д. 46.