УДК 004.896

ПРИМЕНЕНИЕ ИНСТРУМЕНТАРИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Корнев П.А.[1], Пылькин А.Н.[1], Свиридов А.Ю.[1]

[1]ГОУ ВПО «Рязанский Государственный радиотехнический университет», Рязань, Россия (390005, Рязань, Гагарина,59,1), e-mail: svaur@mail.ru

Проведен анализ возможности применения инструментария искусственного интеллекта в системах обнаружения вторжений, рассмотрены наиболее значимые работы в области применения искусственных нейронных сетей, генетических алгоритмов, иммунных и нечетких систем в системах обнаружения вторжения на вычислительные сети. По результатам анализа было выявлено, что все работы основаны на уже устаревшей базе данных атак KDD CUP 99[13], при этом отсутствуют какие-либо подходы к обнаружению атак более высокого уровня (exploit pack's). Разработан прототип модуля для программы Snort: snort with simple artificial neural network (SANNSNORT), который в перспективе сможет с высокой вероятностью находить новые виды атак на вычислительные сети при помощи механизма обнаружения «отстуков» зараженных вредоносным программным обеспечением хостов.

Ключевые слова: искусственный интеллект, системы обнаружения вторжений, IDS, нейронные сети, генетические алгоритмы, нечеткие системы, SANNSNORT.

USING ARTIFICIAL INTELLIGENCE IN INTRUSION DETECTION SYSTEMS

Kornev P.A.[1], Pylkin A.N.[1], Sviridov A.U.[1]

[1]GOU VPO "Ryazan State Radio Engineering University", Ryazan, Russia (390005, Ryazan, Gagarina 59,1), e-mail: svaur@mail.ru

An analysis of application possibility of artificial intelligence tools in intrusion detection systems, are considered the most important work in the field of application of neural networks, genetic algorithms, immune and fuzzy systems in intrusion detection systems for computer networks. It was found on the analysis base, that all works are based on outdated database attacks KDD CUP 99[13], thus there are no approaches to detection of higher level attacks (exploit pack's). The module prototype for the program Snort: snort with simple artificial neural network (SANNSNORT), which should be able to find with a high probability new kinds of attacks to computer networks using a detection mechanism of "feedbacks" hosts, infected by malware, is developed.

Keywords: artificial intelligence, intrusion detection systems, IDS, neural networks, genetic algorithms, fuzzy systems, SANNSNORT.

Количество инцидентов в области информационной безопасности постоянно увеличивается. Атаки на вычислительные сети уже давно перестали быть делом избранных специалистов. В настоящее время средства для взлома может найти любой человек, не обладающий глубокими познаниями в области информационной безопасности для их эффективного использования. Поэтому атаки на корпоративные сети и ПК обычных пользователей становятся все более обыденным делом, а развитый рынок продажи уязвимостей и эксплойтов [14] помогает совершенствовать методы и средства их проведения. Поэтому важной задачей становится разработка и совершенствование средств защиты.

1. Обзор наиболее значимых работ, основанных на применении технологий искусственного интеллекта в системах обнаружения вторжений

В настоящее время существует много программных продуктов, направленных на решение такой актуальной задачи, как обнаружение вторжений. Практически во всех этих

средствах используются методы искусственного интеллекта (ИИ), так как о наличии атаки можно судить лишь приблизительно, оценивая параметры системы [1].

Задачи обнаружения вторжений в вычислительные сети обычно решаются с применением:

- экспертных систем;
- искусственных нейронных сетей (ИНС);
- искусственных иммунных систем;
- нечетких систем;
- генетических алгоритмов.

Рассмотрим подробнее инструментарий искусственного интеллекта, применяемый для обнаружения вторжений.

1.1. Экспертные системы

Наиболее часто в системах обнаружения вторжений применяются экспертные системы. Данный факт объясним тем, что сигнатурный метод анализа сетевого трафика является наиболее быстрым и не требующим больших вычислительных мощностей. Самыми известными представителями систем обнаружения вторжений на основе экспертных систем являются: Snort, Tripwire, IBM ISS, McAfee.

Самым крупным недостатком экспертной системы в качестве системы обнаружения вторжений является неспособность в принципе обнаруживать новые виды атак. Кроме того, известно множество технологий обхода систем обнаружения вторжений на основе экспертных систем, например, polymorphic shell code, insertion, exclusion и т.п.

Подход к обнаружению вторжений, основанный на применении экспертных систем, широко применяется в практических приложениях, поэтому в дальнейшем подробно не рассматривается и считается классическим.

1.2. Искусственные нейронные сети

Искусственная нейронная сеть – это математическая модель, а также её программная или аппаратная реализация, построенная по принципу организации и функционирования биологических нейронных сетей (сетей нервных клеток живого организма)[1]. Ограниченность применения нейронных сетей в системах обнаружения вторжений обусловлена требованием больших вычислительных мощностей и невозможности оперативного анализа больших объемов данных в условиях работы в качестве NIDS (сетевая система обнаружения вторжений) большой корпоративной сети. В качестве примера разработок в области применения нейронных сетей в NIDS рассмотрим ниже несколько наиболее известных отечественных и зарубежных исследований.

1.2.1. Исследования простого двухслойного персептрона

Жигулин П.В. и Подворчан Д.Э. использовали для детектирования атак двухслойной персептрон с одним скрытым слоем по схеме 38 входных, 38 скрытых, 10 выходных нейронов [2]. В их экспериментах 38 входных векторов представляли собой числовые эквиваленты наиболее значимых признаков набора данных KDD CUP 99. В скрытом слое функционировали 38 решающих нейронов. В выходном слое было использовано 10 выходов, являющихся идентификаторами различных типов атак. Точность определения типа атаки достигла 98%. Однако недостатком разработки является то, что нейронная сеть тестировалась всего на 20% тестового набора, обучение и калибровка сети происходила на остальных 80%, то есть сеть «знала» практически все о тестовом наборе.

1.2.2. Исследования нескольких многослойных персептронов

Исследователи Моради М. и Зелкернин М. из университета Queen использовали несколько схем реализации нейросети и получили следующие результаты [12]:

1) схема: 35 входных, 35 скрытых нейронов первого уровня, 35 скрытых нейронов второго уровня, 3 выходных нейрона показала 91% верных решений на тестовых примерах;
2) схема: 35 входных, 45 скрытых, 3 выходных нейронов показала 87% верных решений на тестовых примерах;
3) схема: 41 входных, 40 скрытых нейронов первого уровня, 40 скрытых нейронов второго уровня, 1 выходной нейрон показала 99% верных решений на тестовых примерах.

В первых двух схемах в качестве выходных векторов использовались схемы:

1) [1,0,0] – нормальное состояние;
2) [0,1,0] – отказ в обслуживании;
3) [0,0,1] – сканирование.

Третья схема с большой вероятностью определяет наличие атаки, но не ее тип.

Как видно из полученных результатов[12], увеличение числа скрытых слоев не приводит к значительному улучшению качества работы сети (всего 4%) при экспоненциально возросшей сложности схемы и, как следствие, времени анализа.

1.2.3. Однослойный классификатор для детектирования стандартного состояния

Исследователи Клионский Д.М., Большев А.К. и Геппенер В.В. разработали систему на основе HNIDS (Heuristic Network Intrusion Detection Systems), которая использует однослойный классификатор на базе искусственных нейронных сетей (ИНС) [6].

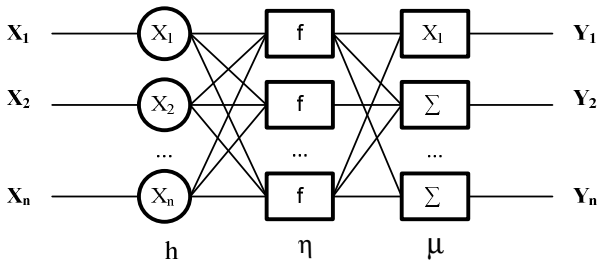

Рис. 1. Нейронная сеть, представляющая собой однослойный классификатор

На рисунке 1 представлена ИНС, реализующая работу однослойного классификатора. В качестве функции активации используется сигмоидальная функция активации где:

– h – количество нейронов скрытого слоя;

– η – коэфициент скорости обучения;

– μ – коэффициент инерционности.

Главным отличием такого типа систем от других является то, что система обучается на «нормальном» трафике целевой сети и в случае обнаружения отклонений сообщает об атаке или аномалии. Система работает на сетевом (транспортном) уровнях модели открытых систем и анализирует завершенные TCP-сессии между хостами.

При тестировании прототипа исследователями в тестовой выборке использовали 17 вторжений сетевого уровня. С помощью варьирования параметров ИНС проводились минимизации по критериям ложной тревоги (FP) и пропуска сигналов (FN). При минимизации по критерию FP, прототип обнаружил 12 атак при 2 ложных срабатываниях. При минимизации по критерию FN, прототип обнаружил 16 атак при 1878 ложных срабатываниях.

1.2.4. Построение гибридных нейронных сетей для обнаружения сетевых атак

В своих исследованиях Жульков Е.В. предложил разбить трафик на векторы и при помощи системы обнаружения вторжений (СОВ), построенной по модульному принципу, анализировать трафик как векторы [3].

Алгоритм поиска вторжений сводится к последовательности следующих действий.

1. Подготовка базы данных атак.
2. На основании части базы DARPA[13] не содержащей вторжений, генерация базы для генератора шума (система, выдающая векторы нормального трафика, используется для обучения нейросети).
3. Выделение параметров межсетевого взаимодействия (основные параметры трафика, используемые в векторах).

4. Создание и обучение нейронной сети первого уровня.
5. Обучение второго уровня нейронной сети выходными данными первого уровня.
6. Тестирование.
7. Работа СОВ.

Вероятность обнаружения известных атак составила 91%, вероятность обнаружения неизвестных атак составила 86%.

Хафизов А.Ф. предложил использовать гибридную нейронную сеть для анализа пифограмм атак [10]. На первом этапе работы гибридной искусственной нейросети, на множестве входных векторов обучается слой Кохонена. В результате нейроны этого слоя самоорганизуются таким образом, что векторы их весов наилучшим образом отображают распределение данных обучающих векторов. Далее веса фиксируются и на вход подается обучающая выборка, затем происходит финальная корректировка весов нейронов. На втором этапе обучается персептронная сеть. Обучение происходит с учителем. Для данной сети обучающие сигналы формируются из выходных сигналов слоя Кохонена и вектора ожидаемых значений.

Результатом работы такой нейронной сети является отнесение входных данных к классу атак или к классу нормальных взаимодействий. Эффективность системы заключается в том, что разработанная методика обнаружения сетевых вторжений превосходит существующие решения на 15%.

1.3. Нечеткие системы

Нечеткие системы как научное направление в 2015 году будут отмечать свое пятидесятилетие, за это время были получены выдающиеся результаты применения нечетких систем в различных областях человеческой деятельности. Нечеткие системы так же нашли свое применение в качестве компонента системы обнаружения вторжений, так как они оперируют «нечеткими» и «размытыми» данными [2], которыми и являются векторы атак на вычислительные сети. В качестве примера применения нечетких систем в IDS, рассмотрим несколько работ отечественных и иностранных ученых.

1.3.1. Применение нечеткой логики для обнаружения сетевых атак

Исследователи из Индии Шанмагавадива Р.и Нагаражан Н. создали систему обнаружения вторжений на основе нечеткой логики. Схема работы сети представлена на рисунке 2.

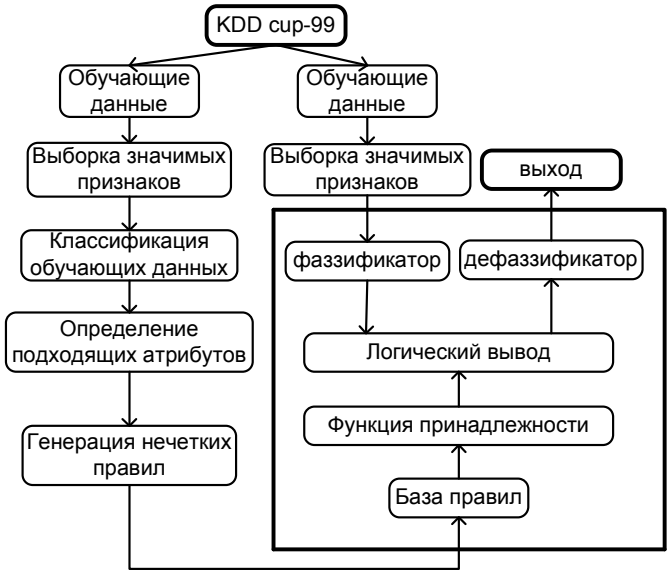

Рис. 2. Схема работы СОВ на основе нечеткой логики

Авторам [15] удалось достичь более 90% срабатываний, причем лишь 10% набора использовалось для создания базы нечетких правил.

1.3.2. Применение нечеткой нейронной сети для обнаружения сетевых атак

Исследователи Слеповичев И.И., Ирматов П.В., Комарова М.С. и Бежин А.А.[9] разработали систему обнаружения SYN Flood атак на основе нечеткой нейронной сети. Метод обучения ИНС - метод обратного распространения ошибки.

На основании разработанной модели исследователями была разработана программа, которая, используя математический аппарат нечеткой логики и нейронных сетей, определяет степень уверенности в наличии атаки.

1.3.3. Применение искусственных иммунных систем для обнаружения сетевых атак

При синтезе алгоритмов активного аудита информационной системы Кашаевым Т.Р. была разработана система обнаружения вторжений на основе искусственных иммунных систем [5].

Разработанная система использует нечеткие сети Петри. Система в общем случае работает следующим образом:

1. Определяются нормальные шаблоны активности системы (множество *S*) в виде строк равной длины *l*, составленных из букв конечного алфавита.

2. Генерируется набор детекторов *R*, каждый из которых не совпадает ни с одной из строк из нормального шаблона активности. При этом кандидат в детекторы считается совпадающим с нормальным шаблоном в том и только в том случае, когда совпадают символы в *r* одинаковых позициях. Величина *r* подбирается в соответствии с решаемой задачей.

3. данные контролируются путем сопоставления детекторов с поведением системы. Любое совпадение на данном шаге означает изменение в работе системы (аномалию).

На основании разработанной модели был реализован прототип. Тестирование показало, что система обнаруживает до 85% атак.

1.3.4. Применение нечетких когнитивных карт для обнаружения сетевых атак

Свечников Л.А.[8] в рамках создания интеллектуальной системы обнаружения атак на основе имитационного моделирования показал эффективность использования нечетких когнитивных карт в области обнаружения атак [7].

Данный подход основан на выделении совокупности основных факторов (концептов), обозначающих различные понятия моделируемой предметной области и построении на их основе ориентированного графа, отображающего взаимосвязи между концептами. Каждому i-му концепту нечеткой когнитивной карты ставится в соответствие переменная состояния Xi и вес wij, характеризующий влияние i-го концепта на j-й концепт. Величина веса wij лежит в пределах отрезка [0;1] и характеризует степень значимости (влияния) соответствующего концепта.

На основании разработанного алгоритма был создан исследовательский прототип системы обнаружения атак на основе нечетких когнитивных карт, реализующий предложенные алгоритмы обнаружения атак по результатам моделирования рисков ИС в режиме реального времени. В проведенных экспериментах разработанный прототип системы обнаружения атак позволяет распознать и блокировать до 97% атак на защищаемые компоненты информационной системы.

1.4. Генетические алгоритмы

Хотя основной областью применения генетических алгоритмов является оптимизация запросов базы данных [1], генетические алгоритмы так же могут быть частью системы обнаружения вторжений. Рассмотрим работу, которая позволяет говорить о перспективности этого направления.

Ученые Ануп Гоял и Четан Камар из Northwestern University создали систему обнаружения вторжений GA-NIDS, основанную на генетическом алгоритме [11]. Схема работы системы представлена на рисунке 3.

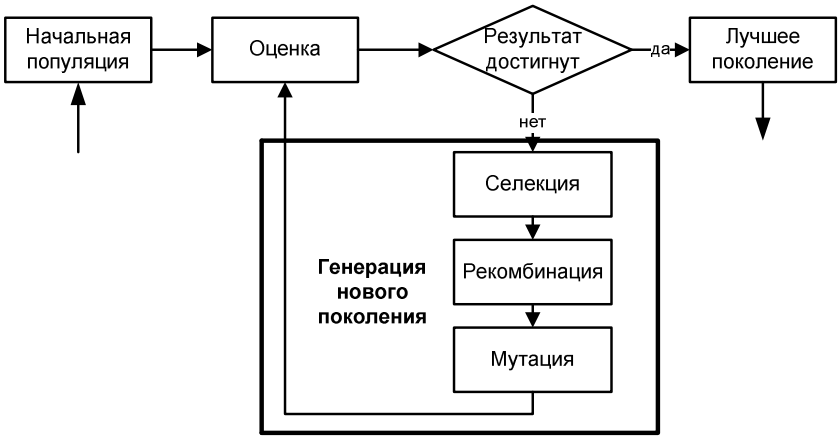

Рис. 3. Схема работы GA-NIDS

Для генерации правил использовалось 10% набора KDD CUP 99. Сгенерированные правила показали более 95% правильных решений на тестовых примерах.

2. Разработка собственного модуля (SANNSNORT)

Проведенный анализ известных и доступных работ позволил провести исследования, в ходе которых был разработан модуль для программы анализа сетевого трафика IDS Snort. Общая схема работы модуля представлена на рисунке 4

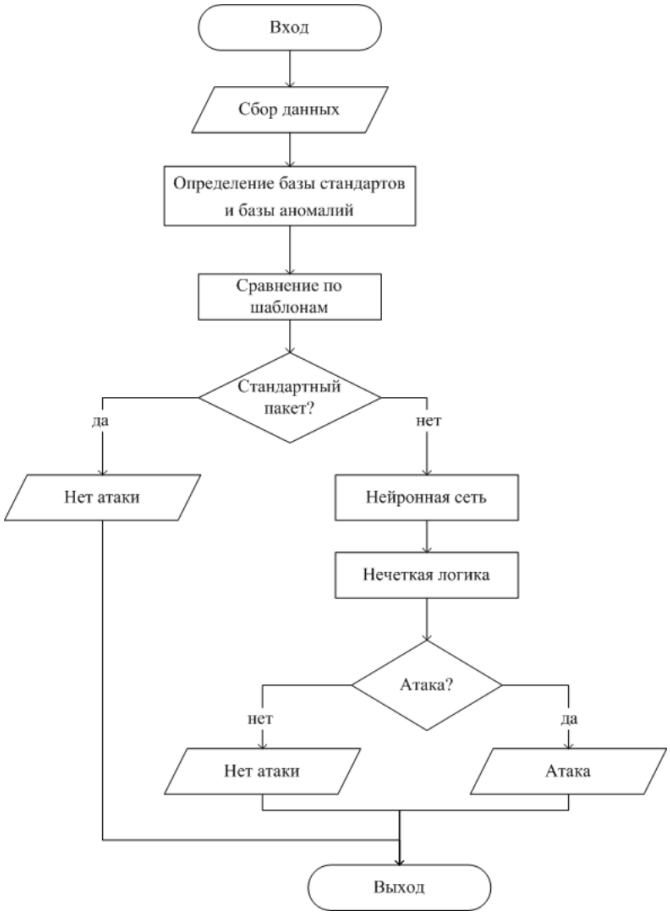

Рис. 4. Обобщенная схема функционирования модуля SANNSNORT

Система при помощи нейронной сети анализирует векторы атак(шаблоны), полученные из сетевого трафика

В ходе тестирования разработанный модуль проверял 15000000 запросов, в которых содержалось 400 признаков заражения вычислительной сети. Было отмечено 320 «подозрительных» признаков, из которых 12 – ошибка первого рода. Основная часть модуля находится на стадии усовершенствования, однако прототип показал хорошие результаты, которые указывают на необходимость продолжения разработки.

Заключение

Рассмотренные в статье исследователи изучали применение различных методов искусственного интеллекта в системах обнаружения вторжений. При этом сравнительно мало внимания было уделено исследованию современных сложных технических атак, таких как ZeuS, SpyEye, а так же многочисленных наборов эксплоитов(Exploit pack), которые на сегодняшний день являются основным источником угроз в крупных предприятиях. Подобные выводы создают платформу для дальнейшего изучения и проектирования альтернативных методов анализа сетевых аномалий и поиска сетевых вторжений.

Список литературы

1. Демидова Л.А., Пылькин А.Н. Методы и алгоритмы принятия решений в задачах многокритериального анализа. М.: Горячая линия-Телеком, 2007. 232 с.
2. Демидова Л.А., Кираковский В.В., Пылькин А.Н. Принятие решений в условиях неопределенности. М.: Горячая линия-Телеком, 2012. 288 с.
3. Жигулин П.В., Подворчан Д.Э. Статья в информационном портале университета ТУСУР [Электронный ресурс]. – Томск: www.tusur.ru. – «Анализ сетевого трафика с помощью нейронных сетей». Режим доступа http://storage.tusur.ru/files/425/КИБЭВС-1005_Жигулин_П.В.__Подворчан_Д.Э.pdf.
4. Жульков Е. В. Диссертация в электронной библиотеке РГБ [Электронный ресурс]. – Москва: http://dlib.rsl.ru. – «Построение модульных нейронных сетей для обнаружения классов сетевых атак». Режим доступа: http://dlib.rsl.ru/01003177093.
5. Кашаев Т. Р. Диссертация в электронной библиотеке РГБ [Электронный ресурс]. – Москва: http://dlib.rsl.ru. – «Алгоритмы активного аудита информационной системы на основе технологий искусственных иммунных систем». Режим доступа: http://dlib.rsl.ru/01003447155.
6. Клионский Д.М., Большев А.К., Геппенер В.В. Статья в Национальном исследовательском ядерном университете «МИФИ» [Электронный ресурс]. – Москва:

http://library.mephi.ru. – «Применение искусственных нейронных сетей в сетевых технологиях и интеллектуальном анализе данных». Режим доступа: http://library.mephi.ru/data/scientific-sessions/2011/neiroinform/ch3/2-1-6.doc;

7. Крошилин А.В., Крошилина С.В. Обзор способов формирования когнитивных карт в системах поддержки принятия решений //Программные информационные системы. Рязань: РГРТУ. 2011. С.20-24.

8. Свечников Л. А. Диссертация в электронной библиотеке РГБ [Электронный ресурс]. – Москва: http://dlib.rsl.ru. – «Система обнаружения атак на информационную систему с использованием динамических моделей на основе нечетких когнитивных карт». Режим доступа: http://dlib.rsl.ru/01004730956.

9. Слеповичев И. И., Ирматов П. В., Комарова М. С., Бежин А. А. Обнаружение DDoS атак нечеткой нейронной сетью // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2009. № 9:3. С. 84-89.

10. Хафизов А. Ф. Диссертация в электронной библиотеке РГБ [Электронный ресурс]. – Москва: http://dlib.rsl.ru. – «Нейросетевая система обнаружения атак на WWW-Сервер». Режим доступа: http://dlib.rsl.ru/01002663345;

11. Ануп Гоял, Четан Кумар. Статья в информационном портале университета Northwestern University [Электронный ресурс]. – Иллинойс: http://www.cs.northwestern.edu. – «GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System». Режим доступа: http://www.cs.northwestern.edu/~ago210/ganids/GANIDS.pdf 01.12.2013.

12. Моради М., Зелкернин М. Статья в информационном портале университета Queen’s University [Электронный ресурс]. – Кингстон: http://queensu.ca. – «A Neural Network Based System for Intrusion Detection and Classification of Attacks».Режим доступа: http://research.cs.queensu.ca/~moradi/148-04-MM-MZ.pdf+ 01.12.2013.

13. Набор данных KDD Cup 1999 Data, [Электронный ресурс]. – http://kdd.ics.uci.edu «KDD Cup 1999 Data». Режим доступа: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

14. Пьерлуиджи Паганини. Статья в информационном портале института INFOSEC. [Электронный ресурс]. – Elmwood Park: http:// infosecinstitute.com. – «A World of Vulnerabilities».Режим доступа: http://resources.infosecinstitute.com/a-world-of-vulnerabilities.

15. Шанмагавадива Р., Нагаражан Н. INDIAN JOURNAL OF COMPUTER SCIENCE AND ENGINEERING [Электронный ресурс]. – Тамил Наду, Индия: www.ijcse.com, 2011. – «network intrusion detection system using fuzzy logic». Режим доступа: http://www.ijcse.com/docs/IJCSE11-02-01-034.pdf+01.12.2013.

Рецензенты:

Еремеев В.В., д.т.н., директор НИИ обработки аэрокосмических изображений, профессор РГРТУ, г. Рязань;

Костров Б.В., д.т.н., заведующий кафедрой ЭВМ, профессор РГРТУ, г. Рязань.