УДК 004.056.5
DOI: 10.25559/SITITO.16.202003.533-542

Оригинальная статья

Исследование алгоритмов адаптивных нейро-нечетких сетей ANFIS для решения задачи идентификации сетевых атак

Д. И. Парфёнов*, И. П. Болодурина, Л. С. Забродина, А. Ю. Жигалов
ФГБОУ ВО «Оренбургский государственный университет», г. Оренбург, Российская Федерация
460018, Российская Федерация, г. Оренбург, пр. Победы, д. 13
* parfenovdi@mail.ru

Аннотация

В настоящий момент темпы изменения характера инцидентов кибербезопасности обуславливают необходимость модификации существующих алгоритмов идентификации атак систем обнаружения вторжений таким образом, чтобы осуществлялось быстрое реагирование на новые типы атак. Современные алгоритмы интеллектуального анализа данных позволяют строить решения подобных задач, однако результат, как правило, зависит как от используемых инструментов и алгоритмов обучения, так и от качества данных, на которых строится модель. Для повышения качества данных из-за объективной неопределенности существует комплекс методов и алгоритмов обработки и фильтрации, при этом влияние субъективности экспертов является сложнейшей задачей, эффективность в решении которой показали системы нейро-нечеткого вывода. В связи с этим, данная работа направлена на исследование алгоритмов адаптивных нейро-нечетких сетей ANFIS на базе различных представлений нечетких правил, позволяющих выполнять классификацию входящего трафика сети для идентификации различных инцидентов кибербезопасности. Полученные результаты общей оценки эффективности идентификации сетевых атак с помощью различных мер точности показали, что наиболее оптимальным нейро-нечетким классификатором является сеть ANFIS с использованием нечеткого вывода Такаги-Сугено-Канга. При этом наименее эффективные результаты идентификации различных типов сетевых атак показало применение нечеткого вывода Ванга-Менделя. Разработанные модули могут использоваться для обработки данных, полученных с датчиков системы управления информацией и событиями безопасности.

Ключевые слова: нечеткая нейронная сеть, сетевые атаки, базы знаний, нечеткие правила, ANFIS, алгоритм обратного распространения ошибки.

Финансирование: исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 20-07-01065 «Разработка интеллектуальных методов адаптивного управления безопасностью и верификации работы виртуальной сетевой инфраструктуры мультиоблачной платформы для обработки больших данных», а также гранта Президента Российской Федерации на государственную поддержку ведущих научных школ Российской Федерации (НШ-2502.2020.9) и гранта Президента Российской Федерации для государственной поддержки молодых российских ученых - кандидатов наук (МК-860.2019.9). Авторы заявляют об отсутствии конфликта интересов.

Авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Парфёнов, Д. И. Исследование алгоритмов адаптивных нейро-нечетких сетей ANFIS для решения задачи идентификации сетевых атак / Д. И. Парфёнов, И. П. Болодурина, Л. С. Забродина, А. Ю. Жигалов. – DOI 10.25559/SITITO.16.202003.533-542 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 3. – С. 533-542.

Original article

Research of Adaptive Neuro-Fuzzy Network Algorithms ANFIS for Solving the Problem of Network Attack Identification

D. I. Parfenov*, I. P. Bolodurina, L. S. Zabrodina, A. Yu. Zhigalov
Orenburg State University, Orenburg, Russian Federation
13 Pobeda Ave., Orenburg 460018, Russian Federation
* parfenovdi@mail.ru

Abstract

At the moment, the pace of change in the nature of cybersecurity incidents necessitates the modification of existing algorithms for identifying attacks in intrusion detection systems in such a way that a quick response to new types of attacks is carried out. Modern algorithms for data mining allow building solutions to such problems, however, the result, as a rule, depends both on the tools and learning algorithms used, and on the quality of the data on which the model is built. To improve the quality of data due to objective uncertainty, there is a complex of methods and algorithms for processing and filtering, while the influence of the subjectivity of experts is the most difficult task, the effectiveness of which was shown by the systems of neuro-fuzzy inference. In this regard, this work is aimed at studying the algorithms of adaptive neuro-fuzzy networks ANFIS based on various representations of fuzzy rules that allow the classification of incoming network traffic to identify various cybersecurity incidents. The obtained results of a general assessment of the effectiveness of identifying network attacks using various measures of accuracy showed that the most optimal neuro-fuzzy classifier is the ANFIS network using fuzzy Takagi-Sugeno-Kanga inference. At the same time, the least effective results of identifying various types of network attacks were shown by the use of Wang-Mendel's fuzzy inference. The developed modules can be used to process data received from sensors of the security information and event management system.

Keywords: Fuzzy neural network, network attacks, knowledge bases, fuzzy rules, ANFIS, error back propagation algorithm.

Funding: The research was carried out with the financial support of the Russian Foundation for Basic Research within the framework of scientific project No. 20-07-01065 "Development of Intelligent Methods for Adaptive Security Management and Verification of the Operation of the Virtual Network Infrastructure of a Multi-Cloud Platform for Processing Big Data", as well as a grant from the President of the Russian Federation for state support of the leading scientific schools of the Russian Federation (НШ-2502.2020.9) and a grant of the President of the Russian Federation for state support of young Russian scientists — candidates of science (МК-860.2019.9).

The authors declare no conflict of interest.

For citation: Parfenov D.I., Bolodurina I.P., Zabrodina L.S., Zhigalov A.Yu. Research of Adaptive Neuro-Fuzzy Network Algorithms ANFIS for Solving the Problem of Network Attack Identification. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2020; 16(3):533-542. DOI: https://doi.org/10.25559/SITITO.16.202003.533-542

Введение

В настоящее время вопросы обеспечения необходимого уровня сетевой безопасности и защиты от кибератак активно изучаются различными исследователями в области машинного обучения и анализа данных. Связано это с тем, что существующие интеллектуальные алгоритмы анализа позволяют решать задачи поиска аномалий и выявления всевозможных взаимосвязей внутри данных и т.д [1-3]. Однако, в любой из представленных систем формирования интеллектуальных решений, результат, как правило, зависит как от используемых инструментов и алгоритмов обучения, так и от качества данных, на которых строится некоторая модель.

Снижение качества данных происходит как под действием объективной неопределенности, проявляющейся в шумах, аномалиях, выбросах и т.п., так и под действием лингвистической неопределенности, проявляющейся из-за субъективности оценки экспертов [4]. На данный момент для повышения качества данных из-за объективной неопределенности разработан комплекс методов и алгоритмов обработки и фильтрации, при этом влияние субъективности экспертов является сложнейшей задачей, эффективность в решении которой показали системы нейро-нечеткого вывода.

Цель исследования

Проблема формирования базы нечетких правил заключается в разработке оптимальных функций принадлежности и создании терм-множеств, позволяющих создать систему нечеткого вывода, не зависящей от субъективных оценок специалистов в той или иной области. Одним из методов, призванных решить данную проблему, является построение нейро-нечеткой сети ANFIS. В связи с этим, цель исследования заключается в разработке и исследовании алгоритмов адаптивных нейро-нечетких сетей ANFIS на базе различных представлений нечетких правил [5-7], позволяющих выполнять классификацию входящего трафика сети для идентификации различных инцидентов кибербезопасности.

Технологии обеспечения безопасности в сети посредством создания систем нечеткого вывода

Существует довольно большое количество технологий обеспечения безопасности в сетях, в том числе основанных на нечетком выводе. Рассмотрим основные технологии, использующиеся на данный момент для идентификации сетевых атак.

Исследование бинарной классификации сетевых атак с использованием методов нечеткой логики провели авторы в рамках работы [8], где описали процесс нечеткого вывода Такаги-Сугено на ограниченном наборе признаков сетевого трафика. Результаты разработанного подхода показали высокую точность определения подозрительной сетевой активности. Наиболее сложная система обнаружения сетевых атак была предложена в работе [9] и основывалась на комплексировании нейронных и нейронечетких классификаторов. Предложенный подход использован для обработки данных, полученных от сенсоров системы управления информацией и событиями безопасности, и показал высокую эффективность выявления новых типов атак при минимальном количестве ложных срабатываний.

В связи с высокой эффективность, которую продемонстрировали методы на основе искусственных нейронных сетей совместно с алгоритмами нечеткого вывода, в исследовании [10] авторы представили метод нечеткой кластеризации для генерации различных обучающих подмножеств, а для агрегирования полученных результатов предложили мета-обучающий модуль. Данный подход позволил уменьшить ложные срабатывания и получить более стабильные результаты при идентификации атак.

Впервые идентификацию сетевых атак на примере различных шаблонов DDoS, рассмотрели как динамический процесс подбора наиболее эффективного алгоритма классификации с помощью нечеткой логики в работе [11]. Результаты экспериментов показали, что построенная система нечеткой логики эффективно выбирать алгоритм классификации на основе статуса трафика и позволяет выстраивать определенный компромисс между точностью и задержками алгоритмов идентификации.

Повышение точности обнаружения сетевых атак с помощью нечеткой логики рассмотрено в исследовании [12] и основано на сетевом мониторинге характеристик, таких как время отклика, размеры входящих и исходящих пакетов, пропускная способность и т.д. В рамках данной статьи построен интегральный показатель наличия некоторого типа угрозы, с использованием базы нечетких правил соответствия характеристик типам угроз. Применение инструментов нечеткой логики для обнаружения вторжений в сети продемонстрировано также в статье [13], в которой описано проведение лавинной атаки с синхронизацией по протоколу управления передачей. Предложенный подход показал сравнимые по производительности результаты с методом деревьев решений, который является наиболее распространенным методом машинного обучения.

Исследование [14] посвящено обнаружению вредоносных узлов в мобильной adhoc-сети MANET при проведении различных типов атак. Предлагаемая система нечеткого вывода позволяет также предотвращать подобные атаки с помощью эффективного метода блокировки узлов и обеспечивать необходимый уровень безопасности. Модифицированную гибридную систему обнаружения сетевых атак в беспроводных сенсорных сетях на основе нечеткой логики представили коллеги из Технического университета Гуджрала Пенджаба в работе [15]. Результаты экспериментов показали, что построенная система обнаружения вторжений имеет высокую точность и низкую частоту ложных срабатываний, а также подтверждает эффективность применения данной системы по анализу пропускной способности и количеству потерянных пакетов.

Таким образом, обзор существующих методов, алгоритмов и систем нечетного вывода для анализа сетевого трафика в условиях неопределенности показал, что современные системы не позволяют учитывать все актуальные типы атак, а также оставляют место для модификации и улучшения точности результатов идентификации, так как зависят от экспертной оценки и алгоритмов оптимизации. В связи с этим, данная работа направлена на исследование алгоритмов адаптивных нейро-нечетких сетей ANFIS на базе различных представле-

ний нечетких правил, позволяющих выполнять классификацию входящего трафика сети для идентификации различных инцидентов кибербезопасности.

Формальная постановка задачи идентификации сетевых атак

Рассмотрим задачу построения системы нейро-нечеткой классификации сетевых атак с точки зрения прогнозного моделирования, решение которой можно получить методами машинного обучения с учителем. В связи с тем, что множество идентифицируемых атак ограничено только с практической точки зрения и представлено наиболее распространенными типами атак, то данная задача является многоклассовой классификацией. Заметим, что нейро-нечеткая система позволяет преобразовывать в терм-множества как непрерывные, так и категориальные данные, что значительно расширяем множество возможных для использования переменных характеристик.

Опишем формальную математическую постановку задачи классификации сетевых атак. Предположим, что информация о происходящих событиях в сети фиксируется с некоторым достаточно малым интервалом времени. При этом, помимо данных о самом устройстве и его технических характеристиках, также фиксируется информация о действиях совершаемых конечными пользователями через рассматриваемые устройства. Пусть множество X содержит информацию о состояниях всех объектов сети $x_i \in X, i = 1,..,m$, с которыми сопоставляются некоторые записи журнала событий, т.е. $x_i = \{x_{i1}, x_{i2}, ..., x_{ik}\}$. Задача многоклассовой классификации сетевых атак состоит в том, чтобы объектам сети сопоставить множество типов атак $Y = \{1, ..., K\}$.

Таким образом, задача идентификации сетевых атак состоит в том, что необходимо построить отображение $f_c(X): X \to Y$, позволяющее описать зависимость между фиксирующимися характеристиками сетевого трафика и сопоставить поведение объектов сети с характеристиками и выбрать наиболее вероятное при отсутствии атак и при конкретном типе атаки.

В рамках данного исследования проводится анализ классификации сетевых атак на наборе данных UNSW-NB15[1] [16], который содержит сведения о трафике с пяти различными типами сетевых атак и множество Y имеет вид *{Normal, Fuzzers, Generic, Reconnaissance, Exploits, DoS}*. Заметим, что представленные данные о сетевом трафике собраны более чем по 40 характеристикам и имеют более 2,5 млн. записей. Кроме того, данным сопоставлены сбалансированные наборы для обучения и для тестирования при анализе точности полученных моделей классификации.

Подходы к построению систем нейро-нечеткой классификации

Нейро-нечеткие сети позволяют входным сигналам посредством нечетких преобразований (алгоритмов Сугено-Такаги, Такаги-Сугено-Канга и Ванга-Менделя) и аппроксимации сопоставить выходной сигнал. Заметим, что данные методы позволяют аппроксимировать произвольные непрерывные функции, зависимые от многих переменных, суммой функций, зависимых от одной переменной, с заданной точностью. Рассмотрим основные идеи построения нейро-нечетких сетей ANFIS с применением данных алгоритмов, а также представим подходы к формированию нейро-нечеткого вывода.

Алгоритм Сугено-Такаги

Алгоритм Сугено-Такаги использует следующую модель нечеткого правила:

R_i :ЕСЛИ x_i это A_{i1} И ...И x_n это A_{in} ТО $y = f(X)$

Отметим, что для каждого нечеткого правила Сугено-Такаги подбирается уровень отсечения, при котором рассчитываются выводы правил. В рамках данного исследования в качестве выходной функции использован полином первого порядка [17-18].

Нейро-нечеткая сеть ANFIS, соответствующая модели вывода Сугено-Такаги, представлена на рис. 1 и имеет следующую структуру:

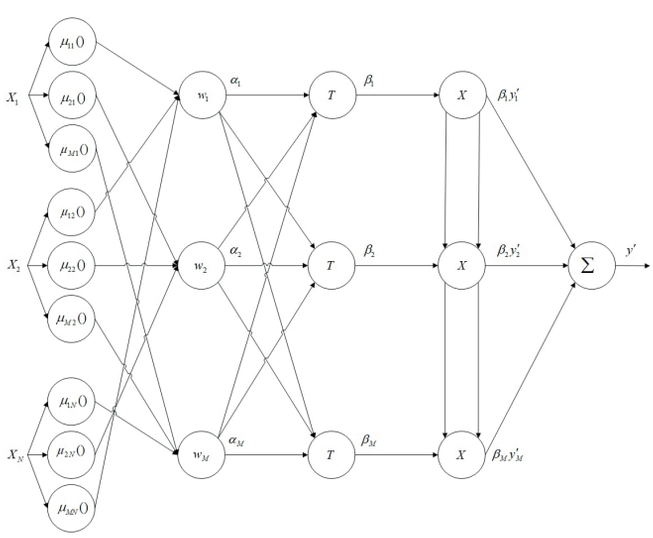
Слой 1. Отвечает за сопоставление непрерывным значениям входного сигнала конкретного терм-множества (фаззификация).

Слой 2. Определяет посылки нечетких правил с учетом входных значений терм-множеств и интерпретируется как степень выполнения некоторого правила.

Слой 3. Вычисляет относительную частоту выполнения нечеткого правила (нормализация).

Слой 4. Вычисляет степень важности каждого нечеткого правила и определяет его вклад в результат.

Слой 5. Агрегирует результаты нечетких правил с учетом выявленной степени важности.



Р и с. 1. Нейро-нечеткая сеть ANFIS с использованием вывода Сугено-Такаги

F i g. 1. Neuro-fuzzy network ANFIS using Sugeno-Takagi inference

[1] *Nour M.* The UNSW-NB15 dataset. UNSW.dataset [Электронный ресурс] // Research Data Australia. 2015. DOI: https://doi.org/10.26190/5d7ac5b1e8485 (дата обращения: 01.11.2020).

Алгоритм Такаги-Сугено-Канга

Алгоритм Такаги-Сугено-Канга использует следующую модель нечеткого правила:

P_i :ЕСЛИ x_i это A_{i1} И ... И x_j это A_{ij} И ...И x_m это A_{im} ТО $y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j, j = 1,..,n.$

Отметим, что для каждого нечеткого правила Такаги-Сугено-Канга функцией принадлежности является функция Гаусса и все входные сигналы являются четкими. В рамках данного исследования в качестве метода дефаззификации выбран метод центроида [19-20].

Нейро-нечеткая сеть ANFIS, соответствующая модели вывода Такаги-Сугено-Канга, представлена на рис. 2 и имеет следующую структуру:

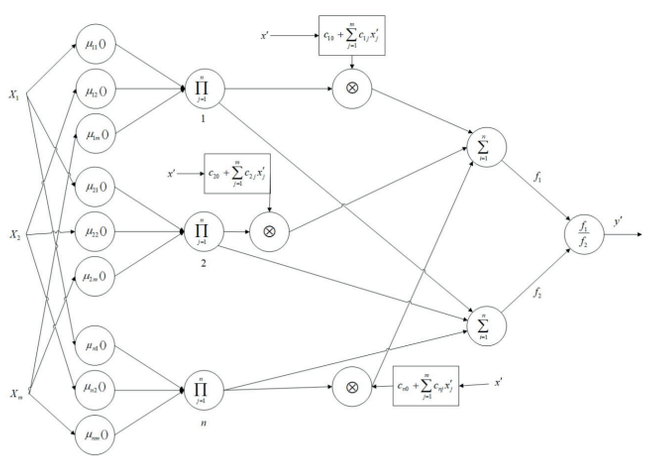
Слой 1. Отвечает за сопоставление четким значениям входного сигнала (фаззификация) и вычисление значений гауссовых функций принадлежности.

Слой 2. Выполняем нечеткое произведение посылок нечетких правил.

Слой 3. Формирует значения функций выходного сигнала с учетом весовых коэффициентов полученных на предыдущем слое.

Слой 4. Агрегирует заключения правил предыдущего слоя и формирует предварительные вычисления для дефаззификации.

Слой 5. Нормализует значения и проводит дефаззификацию результата.



Р и с. 2. Нейро-нечеткая сеть ANFIS с использованием вывода Такаги-Сугено-Канга

F i g. 2. Neuro-fuzzy network ANFIS using Takagi-Sugeno-Kanga inference

Алгоритм Ванга-Менделя

Алгоритм Ванга-Менделя использует следующую модель нечеткого правила:

D_i :ЕСЛИ x_i это A_{i1} И ... И x_j это A_{ij} И ...И x_m это A_{im} ТО $y = B_{i/}, j = 1,..,n.$

Отметим, что для каждого нечеткого правила Ванга-Менделя функцией принадлежности является функция Гаусса и все входные сигналы являются четкими. В рамках данного исследования в качестве метода дефаззификации выбран средний центр [21-22].

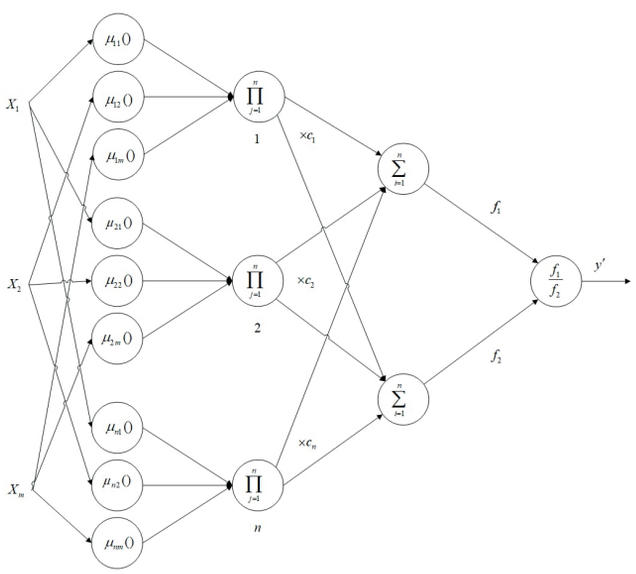
Нейро-нечеткая сеть ANFIS, соответствующая модели вывода Ванга-Менделя, представлена на рис. 3 и имеет следующую структуру:

Слой 1. Отвечает за сопоставление четким значениям входного сигнала (фаззификация) и вычисление значений гауссовых функций принадлежности.

Слой 2. Выполняет агрегирование степеней принадлежностей посылок нечетких правил.

Слой 3. Формирует заключение правил на основе степеней принадлежности посылок, полученных на предыдущем слое, и формирует предварительные вычисления для дефаззификации.

Слой 4. Проводит дефаззификацию результата.



Р и с. 3. Нейро-нечеткая сеть ANFIS с использованием вывода Ванга-Менделя

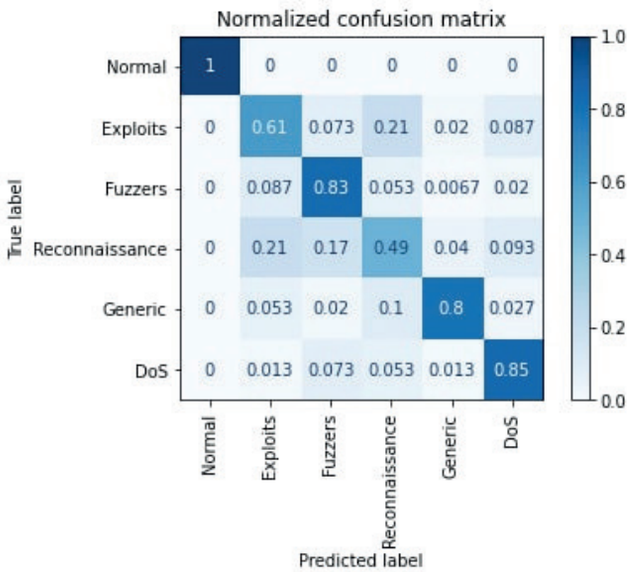
F i g. 3. Neuro-fuzzy network ANFIS using Wang-Mendel inference

Проведенные исследования в области нейро-нечеткой классификации [23-25] показали, что применение различных систем нечеткого вывода для идентификации сетевых атак различного типа подтверждает эффективность рассмотрения всех рассмотренных типов нейро-нечетких сетей и более подробного изучения их достоинств и недостатков при классификации инцидентов кибербезопасности на реальном сетевом трафике.

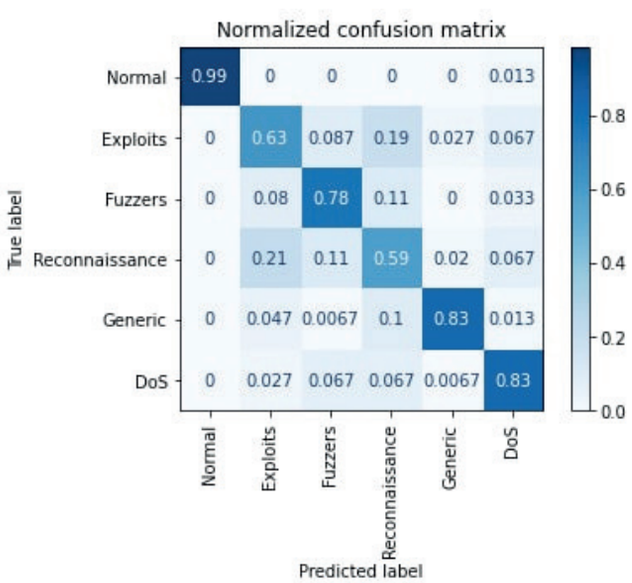
Результаты экспериментального исследования

Для проведения вычислительного эксперимента по идентификации атакующих воздействий, представленные алгоритмы нейро-нечеткой классификации ANFIS были реализованы в виде самостоятельных модулей на языке Python. Эффективность построенных систем нечеткого вывода для определения класса атакующих воздействий была оценена на основе анализа сетевого трафика на наборе данных UNSW-NB15 (более

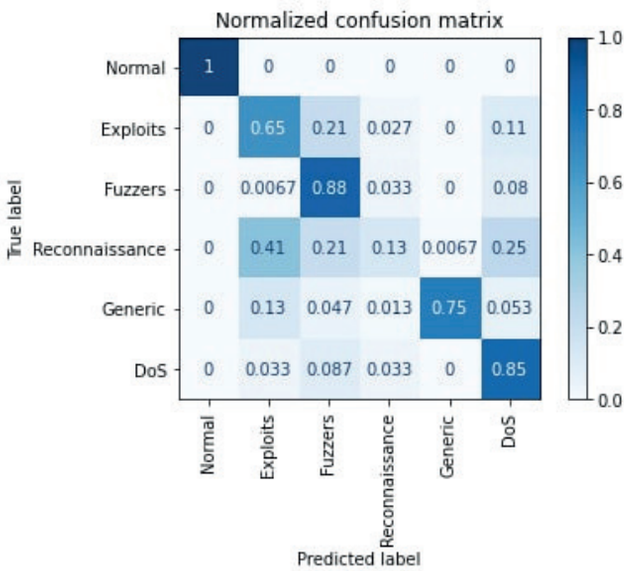
82 тыс. уникальных записей), а результаты классификации представлены в виде матриц ошибок для алгоритма нечеткого вывода Сугено-Такаги (рис. 4), алгоритма Такаги-Сугено-Канга (рис. 5) и алгоритма Ванга-Менделя (рис. 6).



Р и с. 4. Матрица ошибок ANFIS с использованием Сугено-Такаги
F i g. 4. ANFIS error matrix using Sugeno-Takagi



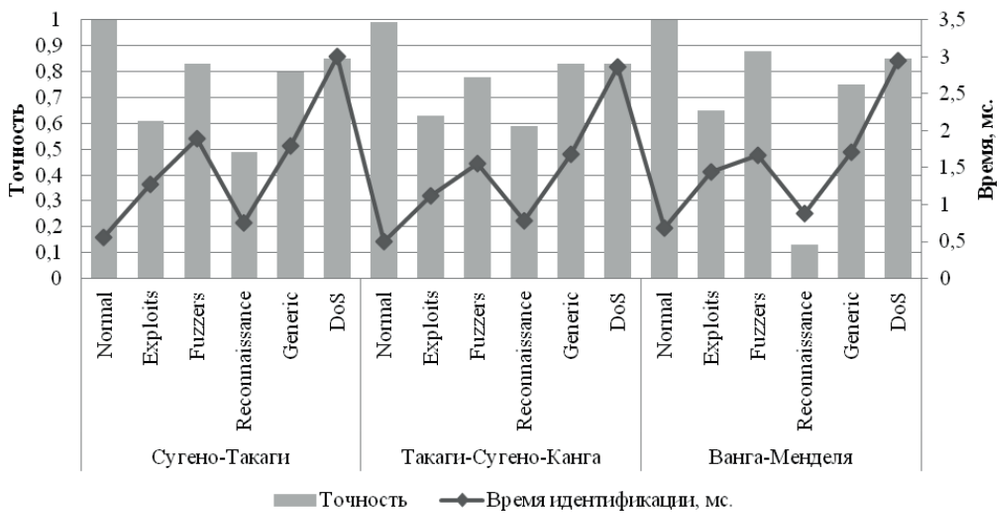
Р и с. 5. Матрица ошибок ANFIS с использованием Такаги-Сугено-Канга
F i g. 5. ANFIS error matrix using Takagi-Sugeno-Kanga



Р и с. 6. Матрица ошибок ANFIS с использованием Ванга-Менделя
F i g. 6. ANFIS error matrix using Wang-Mendel

Полученные результаты также представлены общей оценкой эффективности идентификации сетевых атак с помощью мер точности, полноты, F-меры и количеством истинно положительных результатов классификации (рис. 7), согласно которой наиболее оптимальным нейро-нечетким классификатором с точки зрения различных мер точности является сеть ANFIS с использованием нечеткого вывода Такаги-Сугено-Канга (STK). При этом, наименее эффективные результаты идентификации различных типов сетевых атак показала нейро-нечеткая сеть ANFIS с использованием нечеткого вывода Ванга-Менделя (VM).

Р и с. 7. Оценка точности результатов классификации атак различными алгоритмами
F i g. 7. Assessment of the accuracy of the results of classification of attacks by various algorithms



Р и с. 8. Производительность и точность алгоритмов нейро-нечекой классификации сетевых атак
F i g. 8. Performance and accuracy of algorithms for neural-neural classification of network attacks

Для того, чтобы оценить эффективность применения исследуемых нейро-нечетких подходов к идентификации сетевых атак не только с точки зрения точности получаемых результатов обученных моделей, проведем оценку производительности предложенного решения в относительно времени, затрачиваемого на идентификацию в сетевом трафике каждого из рассмотренных типов атак (рис. 8). Для каждого алгоритма нечеткого вывода дополнительно представим на графике значение полученной точности модели классификации.

Проведенный вычислительный эксперимент, направленный на анализ производительности точности алгоритмов нейро-нечекой классификации трафика показал, что на каждом из представленных типов атак все методы идентификации требовали незначительных вычислительных ресурсов и показывали в среднем сравнимые по точности результаты. Однако, подход основанный на нечетком выводе Такаги-Сугено-Канга в большинстве случаев показал лучшую точность.

Заключение

В рамках данной работы проведено исследование алгоритмов адаптивных нейро-нечетких сетей ANFIS на базе различных представлений нечетких правил, позволяющих выполнять классификацию входящего трафика сети для идентификации различных инцидентов кибербезопасности. Результаты анализа скоростей атак и точности алгоритмов нейро-нечекой классификации показали, что на каждом из представленных типов атак все методы идентификации требовали незначительных вычислительных ресурсов. Полученные результаты общей оценки эффективности идентификации сетевых атак с помощью различных мер точности показали, что наиболее оптимальным нейро-нечетким классификатором является сеть ANFIS с использованием нечеткого вывода Такаги-Сугено-Канга. При этом наименее эффективные результаты идентификации различных типов сетевых атак показало применение нечеткого вывода Ванга-Менделя. Разработанные модули могут использоваться для обработки данных, полученных с датчиков системы управления информацией и событиями безопасности.

Список использованных источников

[1] Кусакина, Н. М. Методы анализа сетевого трафика как основа проектирования системы обнаружения сетевых атак // International Scientific Review of the Problems and Prospects of Modern Science and Education: XLI International Scientific and Practical Conference (Boston. USA — 30 January, 2018). — 2018. — № 1(43). — С. 28-31. — URL: https://elibrary. ru/item. asp? id=32639163 (дата обращения: 01.11.2020). — Рез. англ.

[2] Чистякова, М. А. Методы идентификации атак на WI-FI сеть на основе интеллектуального анализа данных / М. А. Чистякова, М. В. Ильин. — DOI 10.25791/asu.07.2019.749 // Промышленные АСУ и контроллеры. — 2019. — № 7. — С. 41-51. — URL: https://elibrary. ru/item. asp? id=39179401 (дата обращения: 01.11.2020). — Рез. англ.

[3] Никонов, В. В. Разработка автоматизированной системы выявления нештатной сетевой активности и обнаружения угроз / В. В. Никонов, В. П. Лось, Г. В. Росс // Проблемы информационной безопасности. Компьютерные системы. — 2016. — № 2. — С. 60-69. — URL: https://elibrary. ru/item. asp? id=28783777 (дата обращения: 01.11.2020). — Рез. англ.

[4] Jin, S. Intrusion Detection System Enhanced by Hierarchical Bidirectional Fuzzy Rule Interpolation / S. Jin, Y. Jiang, J. Peng. — DOI 10.1109/SMC.2018.00010 // 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC). — Miyazaki, Japan, 2018. — Pp. 6-10. — URL: https://ieeexplore. ieee. org/document/8616005 (дата обращения: 01.11.2020).

[5] Pradeepthi, K. V. Detection of Botnet traffic by using Neuro-fuzzy based Intrusion Detection / K. V. Pradeepthi, A. Kannan. — DOI 10.1109/ICoAC44903.2018.8939109 // 2018 Tenth International Conference on Advanced Computing (ICoAC). — Chennai, India, 2018. — Pp. 118-123. — URL: https://ieeexplore. ieee. org/document/8939109 (дата обращения: 01.11.2020).

[6] Mangrulkar, N. S. Network Attacks and Their Detection Mechanisms: A Review / N. S. Mangrulkar, A. R. Bhagat Patil, A. S. Pande. — DOI 10.5120/15606-3154 // International Journal of Computer Applications. — 2014. — Vol. 90, no. 9. — Pp. 37-39. — URL: https://www. ijcaonline. org/archives/volume90/number9/15606-3154 (дата обращения: 01.11.2020).

[7] Munz, G. Real-time Analysis of Flow Data for Network Attack Detection / G. Munz, G. Carle. — DOI 10.1109/INM.2007.374774 // 2007 10th IFIP/IEEE International Symposium on Integrated Network Management. — Munich, Germany, 2007. — Pp. 100-108. — URL: https://ieeexplore. ieee. org/abstract/document/4258526 (дата обращения: 01.11.2020).

[8] Груздев, С. П. Бинарная классификация компьютерных атак на информационные ресурсы при помощи нечёткой логики / С. П. Груздев, О. И. Шелухин // Телекоммуникации и информационные технологии. — 2019. — Т. 6, № 2. — С. 115-122. — URL: https://elibrary. ru/item. asp? id=42206780 (дата обращения: 01.11.2020). — Рез. англ.

[9] Браницкий, А. А. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов / А. А. Браницкий, И. В. Котенко. — DOI 10.15217/issn1684-8853.2015.4.69 // Информационно-управляющие системы. — 2015. — № 4. — С. 69-77. — URL: https://elibrary. ru/item. asp? id=24113108 (дата обращения: 01.11.2020). — Рез. англ.

[10] Wang, G. A New Approach to Intrusion Detection Using Artificial Neural Networks and Fuzzy Clustering / G. Wang, J. Hao, J. Ma, L. Huang. — DOI 10.1016/j. eswa.2010.02.102 // Expert Systems with Applications. — 2010. — Vol. 37, issue 9. — Pp. 6225-6232. — URL: https://www. sciencedirect. com/science/article/pii/S0957417410001417 (дата обращения: 01.11.2020).

[11] Alsirhani, A. DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark / A. Alsirhani, S. Sampalli, P. Bodorik. — DOI 10.1109/TNSM.2019.2929425 // IEEE Transactions on Network and Service Management. — 2019. — Vol. 16, no. 3. — Pp. 936-949. — URL: https://ieeexplore. ieee. org/document/8765599 (дата обращения: 01.11.2020).

[12] Levonevskiy, D. K. Network attacks detection using fuzzy logic / D. K. Levonevskiy, R. R. Fatkieva, S. R. Ryzhkov. — DOI 10.1109/SCM.2015.7190470 // 2015 XVIII International Conference on Soft Computing and Measurements (SCM). — St. Petersburg, Russia, 2015. — Pp. 243-244. — URL: https://ieeexplore. ieee. org/document/7190470 (дата обращения: 01.11.2020).

[13] A Fuzzy Logic Based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack / N. N. P. Mkuzangwe, F. V. Nelwamondo. — DOI 10.1007/978-3-319-54430-4_2 // Intelligent Information and Database Systems. ACIIDS 2017. Lecture Notes in Computer Science; N. Nguyen, S. Tojo, L. Nguyen, B. Trawiński (ed.). Springer, Cham. — 2017. — Vol. 10192. — Pp. 14-22. — URL: https://link. springer. com/chapter/10.1007/978-3-319-54430-4_2 (дата обращения: 01.11.2020).

[14] Balan, E. V. Fuzzy Based Intrusion Detection Systems in MANET / E. V. Balan, M. K. Priyan, C. Gokulnath, G. U. Devi. — DOI 10.1016/j. procs.2015.04.071 // Procedia Computer Science. — 2015. — Vol. 50. — Pp. 109-114. — URL: https://www. sciencedirect. com/science/article/pii/S1877050915005724 (дата обращения: 01.11.2020).

[15] Singh, R Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks / R. Singh, J. Singh, R. Singh. — DOI 10.1155/2017/3548607 // Wireless Communications and Mobile Computing. — 2017. — Vol. 2017. — Article 3548607. — URL: https://www. hindawi. com/journals/wcmc/2017/3548607 (дата обращения: 01.11.2020).

[16] Moustafa, N. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) / N. Moustafa, J. Slay. — DOI 10.1109/MilCIS.2015.7348942 // 2015 Military Communications and Information Systems Conference (MilCIS). — Canberra, ACT, Australia, 2015. — Pp. 1-6. — URL: https://ieeexplore. ieee. org/document/7348942 (дата обращения: 01.11.2020).

[17] Талагаев, Ю. В. Анализ и синтез сверхустойчивых нечетких систем Такаги-Сугено / Ю. В. Талагаев // Проблемы управления. — 2016. — № 6. — С. 2-11. — URL: https://elibrary. ru/item. asp? id=27346259 (дата обращения: 01.11.2020). — Рез. англ.

[18] Chiang, T.-S. Learning convergence analysis for Takagi-Sugeno Fuzzy Neural Networks / T.-S. Chiang, P. Liu, C-E. Yang. — DOI 10.1109/FUZZ-IEEE.2012.6251318 // 2012 IEEE International Conference on Fuzzy Systems. — Brisbane, QLD, Australia, 2012. — P. 1-6. — URL: https://ieeexplore. ieee. org/document/6251318 (дата обращения: 01.11.2020).

[19] Солдатова, О. П. Алгоритм минимизации базы правил нечеткой нейронной сети Такаги-Сугено-Канга / О. П. Солдатова, Ю. М. Шепелев // EUROPEAN RESEARCH. Сборник статей победителей X Международной научно-практической конференции. — Пенза: Наука и Просвещение, 2017. — Часть 3. — С. 46-49. — URL: https://www. elibrary. ru/item. asp? id=29224790 (дата обращения: 01.11.2020). — Рез. англ.

[20] Субботин, С. А. Метод синтеза нейро-нечетких моделей количественных зависимостей для решения задач диагностики и прогнозирования / С. А. Субботин. — DOI 10.15588/1607-3274-2010-1-22 // Радиоэлектроника, информатика, управление. — 2010. — № 1. — С. 121-127. — URL: http://ric. zntu. edu. ua/article/view/14719 (дата обращения: 01.11.2020). — Рез. англ.

[21] Ketata, R. Fuzzy Approach for 802.11 Wireless Intrusion Detection. i-manager's / R. Ketata, H. Bellaaj. — DOI 10.26634/jse.2.2.567 // Journal on Software Engineering. — 2007. — Vol. 2, issue 2. — Pp. 49-55. — URL: https://imanagerpublications. com/article/567/3 (дата обращения: 01.11.2020).

[22] de Campos Souza, P. V. Detection of Anomalies in Large-Scale Cyberattacks Using Fuzzy Neural Networks / P. V. de Campos Souza, A. J. Guimarães, T. S. Rezende, V. J. Silva Araujo, V. S. Araujo. — DOI 10.3390/ai1010005 // AI. — 2020. — Vol. 1, issue 1. — Pp. 92-116. — URL: https://www. mdpi. com/2673-2688/1/1/5 (дата обращения: 01.11.2020).

[23] ViswaBharathy, A. M. Fixed Neuro Fuzzy Classification Technique For Intrusion Detection Systems / A. M. ViswaBharathy, R. Bhavani // International Journal of Scientific & Technology Research. — 2019. — Vol. 8, issue 10. — Pp. 450-455. — URL: http://www. ijstr. org/final-print/oct2019/Fixed-Neuro-Fuzzy-Classification-Technique-For-Intrusion-Detection-Systems. pdf (дата обращения: 01.11.2020).

[24] Belej, Ol. Development of a Network Attack Detection System Based on Hybrid Neuro-Fuzzy Algorithms / Ol. Belej, L. Halkiv // CEUR Workshop Proceedings. Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020). Zaporizhzhia, Ukraine, April 27-May 1, 2020. — 2020. — Vol. 2608. — Pp. 926-938. — URL: http://ceur-ws. org/Vol-2608/paper69. pdf (дата обращения: 01.11.2020).

[25] Upasani, N. A modified neuro-fuzzy classifier and its parallel implementation on modern GPUs for real time intrusion detection / N. Upasani, H. Om. — DOI 10.1016/j. asoc.2019.105595 // Applied Soft Computing. — 2019. — Vol. 82. — Article 105595. — URL: https://www. sciencedirect. com/science/article/pii/S1568494619303758 (дата обращения: 01.11.2020).

Поступила 01.11.2020; одобрена после рецензирования 18.11.2020; принята к публикации 26.11.2020.

Об авторах:

Парфёнов Денис Игоревич, заведующий сектором программно-технической поддержки дистанционного обучения, ФГБОУ ВО «Оренбургский государственный университет» (460018, Российская Федерация, г. Оренбург, пр. Победы, д. 13), кандидат технических наук, ORCID: http://orcid.org/0000-0002-1146-1270, parfenovdi@mail.ru

Болодурина Ирина Павловна, заведующий кафедрой прикладной математики, ФГБОУ ВО «Оренбургский государственный университет» (460018, Российская Федерация, г. Оренбург, пр. Победы, д. 13), доктор технических наук, профессор, ORCID: http://orcid.org/0000-0003-0096-2587, prmat@mail.osu.ru

Забродина Любовь Сергеевна, ассистент кафедры прикладной математики, ФГБОУ ВО «Оренбургский государственный университет» (460018, Российская Федерация, г. Оренбург, пр. Победы, д. 13), ORCID: http://orcid.org/0000-0003-2752-7198, zabrodina97@inbox.ru

Жигалов Артур Юрьевич, ведущий программист сектора автоматизированной поддержки организации учебного процесса, ФГБОУ ВО «Оренбургский государственный университет» (460018, Российская Федерация, г. Оренбург, пр. Победы, д. 13), ORCID: http://orcid.org/0000-0003-3208-1629, leroy137.artur@gmail.com

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

[1] Kusakina N.M. Methods of the Network Traffic Analysis as a Basis for Designing the Intrusion Detection System. In: *International Scientific Review of the Problems and Prospects of Modern Science and Education: XLI International Scientific and Practical Conference (Boston. USA - 30 January, 2018)*. 2018; (1):28-31. Available at: https://elibrary.ru/item.asp?id=32639163 (accessed 01.11.2020). (In Russ., abstract in Eng.)

[2] Chistyakova M.A., Ilyin M.V. Methods for Identifying Attacks on a WI-FI Network Based on Data Mining. *Industrial Automatic Control Systems and Controllers*. 2019; (7):41-51. (In Russ., abstract in Eng.) DOI: https://doi.org/10.25791/asu.07.2019.749

[3] Nikonov V.V., Loss V.P., Ross G.V. Development of Automated System for Identifying Abnormal Network Activity and Detect Threats. *Problems of Information Security. Computer Systems*. 2016; (2):60-69. Available at: https://elibrary.ru/item.asp?id=28783777 (accessed 01.11.2020). (In Russ., abstract in Eng.)

[4] Jin, S., Jiang, Y., Peng, J. Intrusion Detection System Enhanced by Hierarchical Bidirectional Fuzzy Rule Interpolation. In: *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. Miyazaki, Japan; 2018. p. 6-10. (In Eng.) DOI: https://doi.org/10.1109/SMC.2018.00010

[5] Pradeepthi K.V., Kannan A. Detection of Botnet traffic by using Neuro-fuzzy based Intrusion Detection. In: *2018 Tenth International Conference on Advanced Computing (ICoAC)*. Chennai, India; 2018. p. 118-123. (In Eng.) DOI: https://doi.org/10.1109/ICoAC44903.2018.8939109

[6] Mangrulkar N.S., Bhagat Patil A.R., Pande A.S. Network Attacks and Their Detection Mechanisms: A Review. *International Journal of Computer Applications*. 2014; 90(9):37-39. (In Eng.) DOI: https://doi.org/10.5120/15606-3154

[7] Munz G., Carle G. Real-time Analysis of Flow Data for Network Attack Detection. In: *2007 10th IFIP/IEEE International Symposium on Integrated Network Management*. Munich, Germany; 2007. p. 100-108. (In Eng.) DOI: https://doi.org/10.1109/INM.2007.374774

[8] Gruzdev S.P., Sheluhin O.I. Binary Classification of Computer Attacks to Information Resources Using Fuzzy logic. *Telekommunikacii i informacionnye tehnologii* = Telecommunications and information technologies. 2019; 6(2):115-122. Available at: https://elibrary.ru/item.asp?id=42206780 (accessed 01.11.2020). (In Russ., abstract in Eng.)

[9] Branitskiy A., Kotenko I. Network Attack Detection Based on Combination of Neural, Immune and Neuro-fuzzy Classifiers. *Information and Control Systems*. 2015; (4):69-77. (In Russ., abstract in Eng.) DOI: https://doi.org/10.15217/issn1684-8853.2015.4.69

[10] Wang G., Hao J., Ma J., Huang L. A New Approach to Intrusion Detection Using Artificial Neural Networks and Fuzzy Clustering. *Expert Systems with Applications*. 2010; 37(9):6225-6232. (In Eng.) DOI: https://doi.org/10.1016/j.eswa.2010.02.102

[11] Alsirhani A., Sampalli S., Bodorik P. DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy

Logic System in Apache Spark. *IEEE Transactions on Network and Service Management*. 2019; 16(3):936-949. (In Eng.) DOI: https://doi.org/10.1109/TNSM.2019.2929425

[12] Levonevskiy D.K., Fatkieva R.R., Ryzhkov S.R. Network attacks detection using fuzzy logic. In: *2015 XVIII International Conference on Soft Computing and Measurements (SCM)*. St. Petersburg, Russia; 2015. Pp. 243-244. (In Eng.) DOI: https://doi.org/10.1109/SCM.2015.7190470

[13] Mkuzangwe N.N.P., Nelwamondo F.V. A Fuzzy Logic Based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack. In: Nguyen N., Tojo S., Nguyen L., Trawiński B. (ed.) Intelligent Information and Database Systems. ACIIDS 2017. *Lecture Notes in Computer Science*. 2017; 10192:14-22. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-319-54430-4_2

[14] Balan E.V., Priyan M.K., Gokulnath C., Devi G.U. Fuzzy Based Intrusion Detection Systems in MANET. *Procedia Computer Science*. 2015; 50:109-114. (In Eng.) DOI: https://doi.org/10.1016/j.procs.2015.04.071

[15] Singh R., Singh J., Singh R. Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks. *Wireless Communications and Mobile Computing*. 2017; 2017:3548607. (In Eng.) DOI: https://doi.org/10.1155/2017/3548607

[16] Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: *2015 Military Communications and Information Systems Conference (MilCIS).* Canberra, ACT, Australia; 2015. p. 1-6. (In Eng.) DOI: https://doi.org/10.1109/MilCIS.2015.7348942

[17] Talagaev Yu.V. Analysis and synthesis of superstable Takagi - Sugeno fuzzy systems. *Problemy Upravleniya* = Control Sciences. 2016; (6):2-11. Available at: https://elibrary.ru/item.asp?id=27346259 (accessed 01.11.2020). (In Russ., abstract in Eng.)

[18] Chiang T.-S., Liu P., Yang C-E. Learning convergence analysis for Takagi-Sugeno Fuzzy Neural Networks. In: *2012 IEEE International Conference on Fuzzy Systems*. Brisbane, QLD, Australia; 2012. p. 1-6. (In Eng.) DOI: https://doi.org/10.1109/FUZZ-IEEE.2012.6251318

[19] Soldatova O.P., Shepelev Yu.M. An Algorithm of Rule Base Minimization for Takagi-Sugeno-Kang Fuzzy Neural Network. In: *EUROPEAN RESEARCH. Proceedings of the X International scientific-practical conference*. Nauka i Prosveshhenie, Penza; 2017. Part 3. p. 46-49. Available at: https://www.elibrary.ru/item.asp?id=29224790 (accessed 01.11.2020). (In Russ., abstract in Eng.)

[20] Subbotin S.A. Method of Neuro-fuzzy Model Synthesis of Quantative Dependences for Diagnostics and Prediction Problems Solving. *Radio Electronics, Computer Science, Control*. 2010; (1):121-127. (In Eng.) DOI: https://doi.org/10.15588/1607-3274-2010-1-22

[21] Ketata R., Bellaaj H. Fuzzy Approach for 802.11 Wireless Intrusion Detection. i-manager's. *Journal on Software Engineering*. 2007; 2(2):49-55. (In Eng.) DOI: https://doi.org/10.26634/jse.2.2.567

[22] de Campos Souza P.V., Guimarães A.J., Rezende T.S., Silva Araujo V.J., Araujo V.S. Detection of Anomalies in Large-Scale Cyberattacks Using Fuzzy Neural Networks. *AI*. 2020; 1(1):92-116. (In Eng.) DOI: https://doi.org/10.3390/ai1010005

[23] ViswaBharathy A.M., Bhavani R. Fixed Neuro Fuzzy Classification Technique For Intrusion Detection Systems. *International Journal of Scientific & Technology Research*. 2019; 8(10):450-455. Available at: http://www.ijstr.org/final-print/oct2019/Fixed-Neuro-Fuzzy-Classification-Technique-For-Intrusion-Detection-Systems.pdf (accessed 01.11.2020). (In Eng.)

[24] Belej Ol., Halkiv L. Development of a Network Attack Detection System Based on Hybrid Neuro-Fuzzy Algorithms. *CEUR Workshop Proceedings. Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020). Zaporizhzhia, Ukraine, April 27-May 1, 2020*. 2020; 2608:926-938. Available at: http://ceur-ws.org/Vol-2608/paper69.pdf (accessed 01.11.2020). (In Eng.)

[25] Upasani N., Om H. A modified neuro-fuzzy classifier and its parallel implementation on modern GPUs for real time intrusion detection. *Applied Soft Computing*. 2019; 82:105595. (In Eng.) DOI: https://doi.org/10.1016/j.asoc.2019.105595

Submitted 01.11.2020; approved after reviewing 18.11.2020; accepted for publication 26.11.2020.

About the authors:

Denis I. Parfenov, Head of the Department Software and Technical Support of Distance Learning, Orenburg State University (13 Pobeda Ave., Orenburg 460018, Russian Federation), Ph.D. (Engineering), ORCID: http://orcid.org/0000-0002-1146-1270, parfenovdi@mail.ru

Irina P. Bolodurina, Head of the Department of Applied Mathematics, Orenburg State University (13 Pobeda Ave., Orenburg 460018, Russian Federation), Dr.Sci. (Engineering), Professor, ORCID: http://orcid.org/0000-0003-0096-2587, prmat@mail.osu.ru

Lyubov S. Zabrodina, Assistant of Department Applied Mathematics, Orenburg State University (13 Pobeda Ave., Orenburg 460018, Russian Federation), ORCID: http://orcid.org/0000-0003-2752-7198, zabrodina97@inbox.ru

Artur Yu. Zhigalov, Senior Software Developer of the Sector of Automated Support for the Organization of the Educational Process, Orenburg State University (13 Pobeda Ave., Orenburg 460018, Russian Federation), ORCID: http://orcid.org/0000-0003-3208-1629, leroy137.artur@gmail.com

All authors have read and approved the final manuscript.