ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
2025. Т. 7, № 1 (20). С. 105–112 http://siit.ugatu.su
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Научная статья

УДК 004.056 DOI 10.54708/2658-5014-SIIT-2025-no1-p105 EDN GVIQLO

НЕЙРОСЕТЕВАЯ СИСТЕМА ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Э. Р. Хайруллин • А. М. Вульфин • В. И. Васильев • С. А. Мандовен

Аннотация. Актуальность исследования обусловлена высокой трудоемкостью обеспечения безопасности компьютерных систем и сетей, связанной с масштабными эпидемиями сетевых червей, DDoS атаками с бот-сетей, применением автоматизированных средств поиска уязвимостей в сетях. Целью работы является повышение эффективности обнаружения сетевых атак с помощью моделей машинного обучения. Новизна предлагаемого решения основана на применении нейросетевых моделей и алгоритмов предобработки данных в задаче классификации сетевого трафика на основе статистических признаков сетевых потоков. Отличие от существующих решений заключается в оптимизации гиперпараметров нейросетевых моделей с помощью алгоритма Байесовской оптимизации и построении итогового комитета моделей классификации. Такой подход позволяет повысить эффективность обнаружения сетевых атак как по типам (многоклассовая классификация), так и в случае бинарной классификации.

Ключевые слова: система обнаружения атак; сетевые атаки; машинное обучение; многослойный персептрон; оптимизация гиперпараметров.

ВВЕДЕНИЕ

Обнаружение сетевых атак представляет собой актуальную задачу обеспечения безопасности компьютерных сетей. Среди наиболее распространённых угроз в настоящее время можно выделить эпидемии компьютерных вирусов, а также DDoS-атаки с применением бот-сетей.

Одним из направлений в решении данной проблемы является использование систем обнаружения атак (СОА). Основная цель СОА – обнаружение и распознавание сетевых атак в режиме реального времени. Существующие подходы к обнаружению атак включают сигнатурный метод, использование экспертных систем, встроенных сенсоров и др. Такие системы анализируют весь сетевой трафик (или трафик определенного участка сети) и при обнаружении каких-либо отклонений в нем сигнализируют об этом. В своей работе они используют сигнатурные правила [1].

К сожалению, использование таких систем уже недостаточно для надежной защиты сети. По данным DDoS-Guard, экспертов в сфере защиты от DDoS-атак, злоумышленники не перестают разрабатывать новые механизмы и методы реализации своих атак. Согласно отчету компании Stormwall, в 2023 году рост количества многовекторных атак составил 108 %.

Физически невозможно обновлять базы данных сигнатур формальных СОА в достаточно короткие промежутки времени. Кроме того, увеличение количества сигнатур отрицательно сказывается на производительности систем анализа. Таким образом, актуальной является задача оперативного анализа сетевого трафика с целью обнаружения сетевых атак в режиме реального времени. Как показывают исследования, это реализуемо путем создания перспективных СОА с использованием нейросетевых технологий и методов машинного обучения. Применение интеллектуального анализа позволяет выделить нелинейные зависимости между признаками, извлекаемыми из сетевого трафика, и спроектировать систему обнаружения атак, которая работает в режиме реального времени и способна определять не только существующие, но и неизвестные ранее атаки (модификации существующих атак) [2, 3].

Рекомендовано к публикации программным комитетом X Международной научной конференции ITIDS’2024 «Информационные технологии интеллектуальной поддержки принятия решений», Уфа, 12–14 ноября 2024 г.

Целью работы является повышение эффективности обнаружения сетевых атак с помощью нейронных сетей и моделей машинного обучения.

1. Анализ известных методов обнаружения сетевых атак на основе интеллектуального анализа

В настоящее время технологии обнаружения компьютерных атак активно развиваются производителями различного программного обеспечения. Множество исследований посвящены применению нейронных сетей и методов машинного обучения в задачах обнаружения сетевых атак.

В работе [4] проведен сравнительный анализ методов обнаружения веб-атак. Выявлено, что применение нейронных сетей в системах обнаружения вторжений является перспективным направлением, поскольку работа таких сетей обладает большей гибкостью в сравнении с заранее запрограммированными алгоритмами обнаружения вторжений. Преимущество использования нейронных сетей заключается в том, что некоторые модели способны обучаться не только при помощи специально подобранных наборов данных, но и в процессе работы в режиме реального времени, что увеличивает вероятность правильного срабатывания при обнаружении атаки.

Эффективность использования нейронных сетей также подтверждается в статье [5], в которой приведены результаты исследования по разработке модели, реализующей систему обнаружения вторжений на основе метода глубокого обучения. Авторы используют многослойную нейронную сеть прямого распространения для решения задач бинарной классификации данных, характеризующих классы «нормального» и «аномального» сетевого трафика. Результаты показывают, что использование корреляционной матрицы для выбора атрибутов и применение нейронной сети позволяют построить эффективную систему обнаружения атак.

В работе [6] для анализа трафика в корпоративных сетях и обнаружения атак с определением их класса предлагаются алгоритмы машинного обучения. Преимущество данных алгоритмов заключается в том, что они могут быть использованы для обнаружения новых типов или разновидностей атак в рамках описанных классов, что недоступно для традиционных сигнатурных методов.

Следовательно, нейронные сети способны адаптироваться к изменяющимся условиям, обнаруживать новые типы угроз и снижать количество ложноположительных срабатываний. Таким образом, использование нейронных сетей в СОА обеспечивает улучшение эффективности обнаружения атак по сравнению с традиционными СОА и делает их перспективным направлением в области построения систем безопасности информационных систем и компьютерных сетей.

2. Разработка системы обнаружения сетевых атак на основе нейронной сети и методов машинного обучения

На рис. 1 представлена структурная схема СОА, позволяющая обнаруживать сетевые атаки злоумышленника с помощью нейронной сети и методов машинного обучения.

Источником данных является сетевое оборудование L3 *1*. В модуле *1* происходит зеркалирование трафика с сетевого оборудования (L3-коммутатор, маршрутизатор) для сбора трафика. Также возможны размещение дополнительных сенсоров на сетевых узлах и передача раздельных потоков трафика с каждого сенсора.

Трафик канального уровня поступает в модуль сбора сетевого трафика CICFlowMeter *2* и используется для анализа и извлечения признаков с помощью CICFlowMeter для сетевых сессий. CICFlowMeter *2* преобразует сетевые данные в набор потоков (flows), кроме того, модуль может быть настроен на фильтрацию трафика, чтобы исключить из анализа несущественные пакеты. Набор признаков CICFlow передается в модули *3* и *8*. Модуль хранения сетевых сессий с набором признаков CICFlow *3* необходим для хранения предобработанного набора данных в $БД_1$ для дальнейшей обработки.

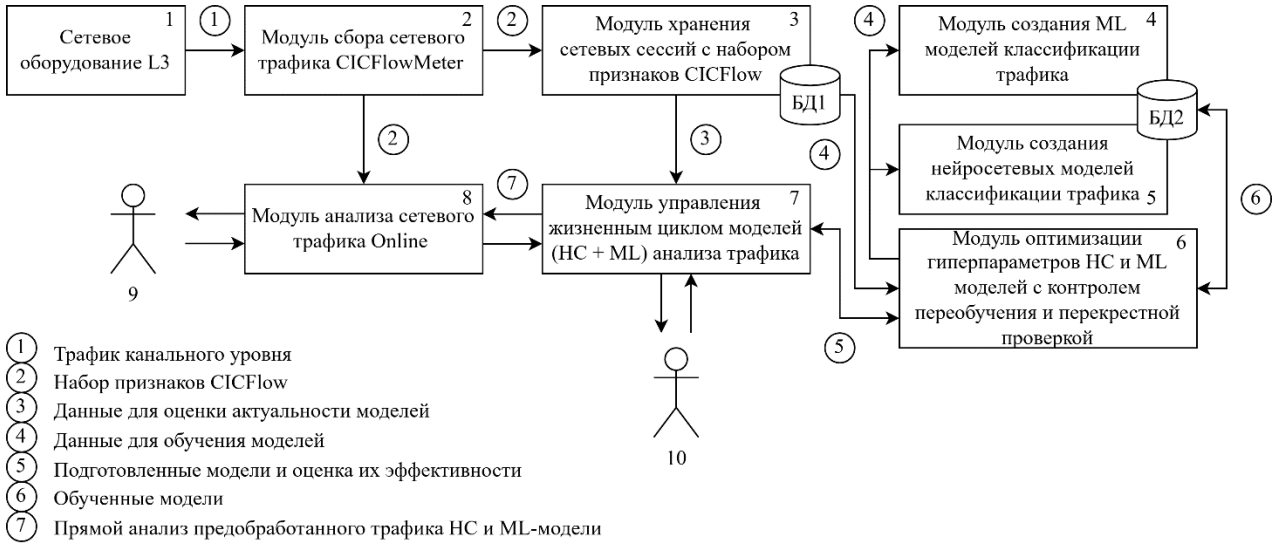

Рис. 1 Структурная схема СОА.

Модули создания ML-моделей *4* и нейросетевых моделей классификации трафика *5* используются для создания ML-моделей (Random Forest, CatBoost) и нейросетевых (НС) моделей (MLP) с целью анализа (классификации) сетевого трафика. Модели хранятся в $БД_2$.

Задача модуля оптимизации гиперпараметров *6* состоит в оптимизации гиперпараметров для моделей ML и нейронных сетей с помощью фреймворка Optuna. В модуле также контролируется переобучение и осуществляется перекрестная проверка для обеспечения высокой точности моделей.

Модуль управления жизненным циклом моделей (НС+ML) анализа трафика *7* контролирует и управляет жизненным циклом моделей, от их создания до обновления и удаления, обеспечивая постоянную актуальность и точность моделей анализа трафика. Специалист по ML *9* отвечает за создание и обновление моделей, оптимизацию их гиперпараметров, контролирует процесс анализа и обработки данных, качество анализа трафика и обнаружение атак.

Модуль анализа сетевого трафика Online *8* использует обученные и оптимизированные модели для анализа сетевого трафика в режиме реального времени. Специалист по сетевой безопасности *10* анализирует результаты классификации трафика и принимает необходимые меры по предотвращению атак, а также отвечает за настройку сетевого оборудования и сенсоров, за обеспечение безопасности данных, собираемых системой.

Принцип работы алгоритма сбора и предварительной обработки данных (рис. 2):

1. Разведочный анализ набора данных предполагает начальный анализ набора данных, который включает оценку типа данных, оценку важности (значимости) каждого признака.

2. Кодирование непрерывных признаков. Признак P_i нормируется с использованием метода RobustScaler (RS), который уменьшает влияние выбросов на значения признаков, масштабируя их в соответствии с межквартильным размахом.

3. Кодирование категориальных переменных. Признак P_i кодируется с использованием метода CategoricalEncoder (CE), который преобразует категориальные значения в числовые.

4. Кодирование выходной переменной. Признак P_i кодируется с использованием метода LabelEncoder (LE), который преобразует метки классов в числовые значения.

5. Данные разбиваются на k подмножеств для выполнения кросс-валидации (kCrossVal). Это необходимо для оценки обобщающей способности модели и предотвращения переобучения.

6. Создание независимого подмножества примеров для оценки обобщенной способности. Данные разбиваются на тренировочный и тестовый наборы (Split), что позволяет оценить производительность модели на данных, которые не использовались во время обучения.

Рис. 2 Алгоритм сбора и предварительной обработки данных.

Модель классификации сетевого трафика на основе обученной нейронной сети и моделей машинного обучения представлена на рис. 3.

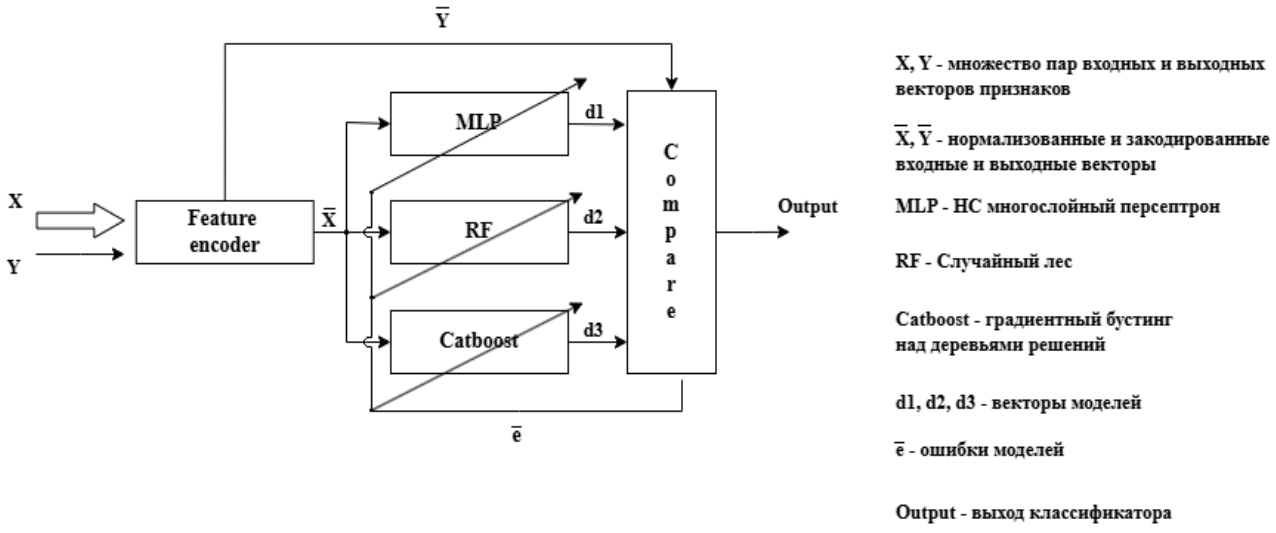

Рис. 3 Модель классификации сетевого трафика.

Описание работы модели классификации сетевого трафика:

1. Сбор и подготовка данных. Входные данные сетевого трафика X и Y передаются в модуль кодирования признаков для нормализации и кодирования.

2. Классификация. Нормализованные и закодированные векторы передаются на входы трех различных моделей классификации (MLP, RF, Catboost). Выходные данные моделей – предсказания (d_1, d_2, d_3).

3. Агрегация результатов. Модуль сравнения и агрегирования обрабатывает предсказания моделей, учитывая их ошибки, и формирует окончательное предсказание, которое является результатом работы классификатора.

Модель обеспечивает классификацию сетевого трафика за счет построения комитета моделей, что улучшает общую производительность и эффективность системы обнаружения атак. Кроме того, благодаря оптимизации гиперпараметров для каждой модели и использованию методов агрегации результатов модель может обеспечивать высокую точность классификации в режиме реального времени.

В качестве нейронной сети используется многослойный персептрон с двумя скрытыми слоями. Входной слой имеет размер вектора признаков, выходной слой определяет количество классов. Подбор гиперпараметров нейронной сети осуществляется с помощью метода Байесовской оптимизации.

Алгоритм обучения и тестирования нейронной сети представлен на рис. 4.

Рис. 3 Алгоритм обучения и тестирования НС.

Алгоритм включает в себя несколько ключевых этапов:

1. Инициализация гиперпараметров. На начальном этапе задаются диапазоны для всех гиперпараметров, включая количество нейронов в слоях, коэффициенты скорости обучения и типы функций активации.

2. Создание задачи оптимизации. На основе заданных гиперпараметров формируется задача оптимизации, которая включает все возможные комбинации параметров.

3. Создание и обучение модели. Для каждой комбинации гиперпараметров (P_i) создается модель многослойного персептрона (MLP). Сеть обучается на тренировочных данных, после чего происходит оценка результатов обучения (вычисление метрик: точность, ошибка и т. д.).

4. Сохранение результатов и выбор лучшей модели. После завершения всех циклов оптимизации выбирается лучшая модель на основе полученных метрик – по критерию наибольшей точности или минимальной ошибки на тестовых данных.

Основанный на NetFlow формат набора данных CSE-CIC-IDS2018, получивший название NF-CSE-CIC-IDS2018, имеет 8392401 запись, из которых 1019203 (12.14 %) являются образцами атак, а 7373198 (87.86 %) являются обычными потоками трафика [7]. В табл. 1 представлено распределение набора данных для обучения сети.

Таблица 1

Атаки в наборе данных

Тип	Количество	Описание
Benign	7373198	Потоки, не наносящие вреда
BruteForce	287597	Метод, направленный на получение имен пользователей и учетных данных паролей путем доступа к списку предопределенных возможностей
Bot	15683	Атака, которая позволяет злоумышленнику удаленно управлять несколькими захваченными компьютерами для выполнения вредоносных действий
DoS	269361	Попытка перегрузить ресурсы компьютерной системы с целью предотвращения доступа к ее данным или их доступности
DDoS	380096	Попытка, похожая на DoS, но имеющая несколько различных распределенных источников
Infiltration	62072	Внутренняя атака, которая отправляет вредоносный файл по электронной почте для использования приложения, а затем следует бэкдор, который сканирует сеть на наличие других уязвимостей.
Web Attacks	4394	Группа, включающая SQL-инъекции, внедрение команд и неограниченную загрузку файлов

Анализ полученных результатов экспериментов по оценке качества мультиклассовой и бинарной классификации атак показал лучшие результаты у классификатора на основе алгоритма случайного леса (Random Forest) (табл. 2).

Таблица 2

Показатели эффективности классификации

Показатель	Random Forest	Многослойный персептрон
Precision	0.99989	0.99954
Recall	0.99966	0.99868
Accuracy	0.99997	0.99987
F_1	0.99977	0.99911

Заключение

Представлена архитектура системы обнаружения сетевых атак на основе нейронной сети и методов машинного обучения. Программная реализация показывает высокую точность классификатора на основе алгоритма случайного леса на наборе данных (0.99 F_1).

Научная новизна предлагаемого решения основана на применении нейронной сети, моделей и алгоритмов машинного обучения в задаче классификации сетевого трафика. Отличие от существующих решений заключается в оптимизации гиперпараметров моделей с помощью алгоритма Байесовской оптимизации и построении итогового комитета моделей. Такой подход позволяет повысить эффективность обнаружения сетевых атак как по типам (многоклассовая классификация), так и в случае бинарной классификации.

Следует также отметить работы [8–12] по смежной тематике, оказавшие влияние на данное исследование.

Список литературы / References

[1] Болдырихин Н. В., Комоцкий Р. И., Лян Д. И. Исследование систем обнаружения вторжений // Молодой ученый. 2023. № 2 (449). С. 6–9. EDN VJSPJT. [[Boldyrikhin N. V., Komotsky R. I., Lyan D. I. “Research of intrusion detection systems” // Young Scientist. 2023. No. 2 (449), pp. 6–9. EDN VJSPJT. (In Russian).]]

[2] Гайфулина Д. А., Котенко И. В. Анализ моделей глубокого обучения для задач обнаружения сетевых аномалий интернета вещей // Информационно-управляющие системы. 2021. № 1. С. 28–37. EDN DTPPJY. [[Gaifulina D. A., Kotenko I. V. “Analysis of deep learning models for network anomaly detection in Internet of Things” // Information and Control Systems. 2021. No. 1, pp. 28-37. EDN DTPPJY. (In Russian).]]

[3] Bashurov V., Safonov P. Anomaly detection in network traffic using entropy-based methods: application to various types of cyberattacks // Issues in Information Systems. 2023. Vol. 24. No. 4. Pp. 82–94. DOI: https://doi.org/10.48009/4_iis_2023_107

[4] Куликова О. В., Корнилова А. В., Буровских Д. В. Обнаружение веб-атак с использованием машинного обучения // Молодой ученый. 2023. № 20 (467). С. 10–13. EDN DPKBIG. [[Kulikova O. V., Kornilova A. V., Burovskikh D. V. “Detection of web attacks using machine learning” // Young Scientist. 2023. No. 20 (467), pp. 10-13. EDN DPKBIG. (In Russian).]]

[5] Большаков А. С., Хусаинов Р. В., Осин А. В. Обнаружение аномалий трафика с использованием нейронной сети для обеспечения защиты информации // i-methods. 2021. Т. 13. № 4. С. 1–15. EDN PKCXWM. [[Bolshakov A. S., Khusainov R. V., Osin A. V. “Traffic anomaly detection using a neural network to ensure information protection” // i-methods. 2021. Vol. 13, no. 4, pp. 1-15. EDN PKCXWM. (In Russian).]]

[6] Бахарева Н. Ф., Тарасов В. Н., Шухман А.Е. и др. Выявление атак в корпоративных сетях с помощью методов машинного обучения // Современные информационные технологии и ИТ-образование. 2018. Т. 14. № 3. С. 626–632. EDN YYHQQX. [[Bakhareva N. F., Tarasov V. N., Shukhman A. E. et al. “Attack detection in enterprise networks by machine learning methods” // Modern Information Technologies and IT-Education. 2018. Vol.14, no. 3, pp. 626–632. EDN YYHQQX. (In Russian).]]

[7] Machine Learning-Based NIDS Datasets. The University of Queensland. [Online]. Available: https://staff.itee.uq.edu.au/marius/NIDS_datasets/#RA1. [Accessed Sept. 09, 2024].

[8] Кучкарова Н. В. Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов // СИИТ. 2024. Т. 6. № 2(17). С. 50–65. EDN NLDWBE. [[Kuchkarova N. V. “Assessment of current threats and vulnerabilities of critical information infrastructure objects using text mining technologies” // SIIT. 2024. Vol. 6, No. 2(17), pp. 50-65. EDN NLDWBE. (In Russian).]]

[9] Вульфин А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных // СИИТ. 2023. Т. 5. № 4(13). С. 50–76. EDN FJPFKC. [[Vulfin A. M. “Models and methods for comprehensive assessment of security risks of critical information infrastructure facilities based on intelligent data analysis” // SIIT. 2023. Vol. 5, No. 4(13), pp. 50-76. EDN FJPFKC. (In Russian).]]

[10] Васильев В. И., Картак В. М. Применение методов искусственного интеллекта в задачах защиты информации (по материалам научной школы УГАТУ) // СИИТ. 2020. Т. 2. № 2(4). С. 43–50. EDN ZTQFCW. [[Vasiliev V. I., Kartak V. M. “Application of artificial intelligence methods in information security problems (based on the materials of the scientific school of Ufa State Aviation Technical University)” // SIIT. 2020. Vol. 2, No. 2(4), pp. 43–50. EDN ZTQFCW. (In Russian).]]

[11] Кириллова А. Д. Оценка рисков информационной безопасности АСУ ТП промышленных объектов методами когнитивного моделирования // СИИТ. 2023. Т. 5. № 4(13). С. 77–93. EDN CUEUUP. [[Kirillova A. D. “Assessment of information security risks of industrial control systems using cognitive modeling methods” // SIIT. 2023. Vol. 5, No. 4(13), pp. 77–93. EDN CUEUUP. (In Russian).]]

[12] Шамсутдинов Р. Р., Васильев В. И., Вульфин А. М. Интеллектуальная система мониторинга информационной безопасности промышленного интернета вещей с использованием механизмов искусственных иммунных систем // СИИТ. 2024. Т. 6. № 4(19). С. 14–31. EDN LTXBSG. [[Shamsutdinov R. R., Vasiliev V. I., Vulfin A. M. “Intelligent system for monitoring information security of the industrial Internet of things using mechanisms of artificial immune systems” // SIIT. 2024. Vol. 6, No. 4(19), pp. 14-31. EDN LTXBSG. (In Russian).]]

Поступила в редакцию 11 декабря 2024 г.

МЕТАДАННЫЕ / METADATA

Title: Neural network system for network attack detection.

Abstract: The relevance of the study is due to the high labor intensity of ensuring the security of computer systems and networks associated with large-scale epidemics of network worms, DDoS attacks from botnets, and the use of automated tools for searching for vulnerabilities in networks. The purpose of the work is to improve the efficiency of detecting network attacks using machine learning models. The scientific novelty of the proposed solution is based on the use of neural network models and data preprocessing algorithms in the problem of classifying network traffic based on statistical features of network flows. The difference from existing solutions lies in the optimization of hyperparameters of neural network models using the Bayesian optimization algorithm and the construction of the final committee of models. This approach allows increasing the efficiency of detecting network attacks both by type (multi-class classification) and in the case of binary classification.

Key words: intrusion detection system; network attacks; machine learning; multilayer perceptron; hyperparameter optimization.

Язык статьи / Language: Русский / Russian.

Об авторах / About the authors:

ХАЙРУЛЛИН Эмиль Рамилевич
Уфимский университет науки и технологий, Россия.
Аспирант каф. вычислительной техники и защиты информации. Магистр информатики и вычислительной техники (Уфимск. гос. авиац. техн. ун-т, 2022). Иссл. в обл. интелл. технологий кибербезопасности сетевой инфраструктуры.
E-mail: khairullin.er@ugatu.su

ВУЛЬФИН Алексей Михайлович
Уфимский университет науки и технологий, Россия.
Профессор каф. вычислительной техники и защиты информации. Дипл. инж.-программист (Уфимск. гос. нефтяной. техн. ун-т, 2008). Д-р техн. наук по методам и системам защиты информации, инф. безопасности (Уфимск. гос. авиац. техн. ун-т, 2022). Иссл. в обл. инф. безопасности, интелл. систем, нечеткого и нейросетевого моделирования.
E-mail: vulfin.am@ugatu.su
ORCID: https://orcid.org/0000-0001-5857-2413

ВАСИЛЬЕВ Владимир Иванович
Уфимский университет науки и технологий, Россия.
Профессор каф. вычислительной техники и защиты информации. Дипл. инж. по пром. электронике (Уфимск. авиац. ин-т, 1970). Д-р техн. наук по сист. анализу и авт. управлению (ЦИАМ, 1990). Иссл. в обл. интелл. систем управления и защиты информации.
E-mail: vas0015@yandex.ru
ORCID: https://orcid.org/0000-0002-6105-5481

МАНДОВЕН Самуэл Александер
Уфимский университет науки и технологий, Россия.
Асп. каф. вычислительной техники и защиты информации. Магистр информационных технологий (Ун-т Чендравасих, Индонезия, 2022). Иссл. в обл. интелл. технологий обеспечения кибербезопасности.
E-mail: mandoven.sa@ugatu.su

KHAIRULLIN Emil Ramilevich
Ufa University of Science and Technology, Russia.
Postgrad. Student of the department computer technology and information security. Master's Degree of Informatics and Computing (USATU, 2022). Research in the field of intelligent technologies for ensuring cybersecurity of network infrastructure
E-mail: khairullin.er@ugatu.su

VULFIN Alexey Mikhailovich
Ufa University of Science and Technology, Russia.
Professor of the department computer technology and information security. Dipl. software engineer (UGNTU, 2008). Dr. Tech. Sciences on Methods and Systems of Information Security (USATU, 2022). Research in the field of information security, intelligent systems, fuzzy and neural network modeling.
E-mail: vulfin.am@ugatu.su
ORCID: https://orcid.org/0000-0001-5857-2413

VASILYEV Vladimir Ivanovich
Ufa University of Science and Technology, Russia.
Professor of the department computer technology and information security. Dipl. Engineer in Industrial Electronics (Ufa Aviat. Inst., 1970), Dr. of Tech. Sci. in systems analysis and automatic control (CIAM, 1990). Research. in intelligent systems of control and information security.
E-mail: vas0015@yandex.ru
ORCID: https://orcid.org/0000-0002-6105-5481

MANDOVEN Samuel Alexander
Ufa University of Science and Technology, Russia.
Postgrad. Student of the department computer technology and information security. Master's Degree of Information Technology (Cenderawasih Univ., Indonesia, 2022). Research in the field of intelligent technologies for ensuring cybersecurity.
E-mail: mandoven.sa@ugatu.su