ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.85

Проектирование гибридной архитектуры нейронной сети для обнаружения угроз в зашифрованном сетевом трафике

М.Д. Бердников, Н.В. Гапон, О.А. Сафарьян
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
В данной статье рассматривается проблема критического снижения эффективности традиционных систем глубокого инспектирования пакетов (DPI) в условиях тотального шифрования сетевых протоколов. Целью статьи является разработка и валидация гибридной нейросетевой архитектуры для выявления кибератак исключительно на основе метаданных. Объектом исследования выступает зашифрованный трафик датасета CIC-IoT23. Основное содержание исследования составляет анализ метаданных сетевых пакетов с применением межпотоковой (Inter-flow) методологии: формирование сбалансированного набора тензоров и проектирование легковесной модели, объединяющей одномерную сверточную сеть (1D-CNN) и энкодер трансформера. На основе изучения разработанного прототипа установлено, что предложенная архитектура достигает высокой точности бинарной классификации (94,42 %). Значительное внимание уделяется выявлению и обоснованию проблемы фонового шума в исходных обучающих данных. Авторы приходят к выводу, что созданная отказоустойчивая модель обладает высокой практической значимостью. В перспективе планируется алгоритмическая фильтрация датасета и масштабирование системы до многоклассовой классификации.

Ключевые слова: зашифрованный сетевой трафик, гибридная нейронная сеть, метаданные сетевых пакетов, трансформер, 1D-CNN, межпотоковый анализ

Для цитирования. Бердников М.Д., Гапон Н.В., Сафарьян О.А. Проектирование гибридной архитектуры нейронной сети для обнаружения угроз в зашифрованном сетевом трафике. *Молодой исследователь Дона.* 2026;11(4):43–48.

Designing Hybrid Neural Network Architecture for Detection of Threats in Encrypted Network Traffic

Mikhail D. Berdnikov, Nikolai V. Gapon, Olga A. Safaryan
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
The article studies the problem of crucial decrease of traditional Deep Packet Inspection (DPI) systems efficiency in the context of ubiquitous network protocol encryption. The aim of the study is to develop and validate the hybrid neural network architecture for detecting cyberattacks based solely on metadata. The object of the study is encrypted traffic of the CIC-IoT23 dataset. The research was focused mainly on the analysis of network packet metadata using the inter-flow methodology: formation of a balanced set of tensors and designing a lightweight model that combines a one-dimensional convolutional network (1D-CNN) and a transformer encoder. Based on the study of the developed prototype, it was established that the proposed architecture ensures high binary classification accuracy (94.42%). Considerable attention was paid to identification and substantiation of the problem of background noise in the original training data. The authors have come to the conclusion that the created fail-safe model has high practical value. In the future, algorithmic dataset filtering and scaling the system up to the multi-class classification are planned.

Keywords: encrypted network traffic, hybrid neural network, network packet metadata, transformer, 1D-CNN, inter-flow analysis

For Citation. Berdnikov MD, Gapon NV, Safaryan OA. Designing Hybrid Neural Network Architecture for Detection of Threats in Encrypted Net-work Traffic. *Young Researcher of Don*. 2026;11(4):43–48.

https://mid-journal.ru

© Бердников М.Д., Гапон Н.В., Сафарьян О.А., 2026

Введение. Стремительная эволюция сетевых инфраструктур и повсеместное внедрение криптографических стандартов нового поколения (TLS 1.3, DNS over HTTPS/TLS) фундаментально изменяют подходы к анализу сетевого трафика. Детерминированный подход к выявлению угроз, основанный на системах глубокого анализа пакетов (Deep Packet Inspection, DPI), стремительно утрачивает практическую эффективность [1]. Доступ к полезной нагрузке надежно блокируется, превращая содержимое пакетов в криптографический шум, не поддающийся классическому сигнатурному анализу [2] и исключающий прямое извлечение маркеров компрометации [3]. В этих жестких условиях векторы кибератак претерпевают качественную трансформацию. Злоумышленники целенаправленно используют протоколы шифрования для маскировки сложных, распределенных во времени угроз прикладного уровня (L7), что позволяет им эффективно обходить традиционные средства сетевой защиты. В современных гетерогенных сетях генерируется вредоносный трафик — рекурсивная разведка портов, сканирование уязвимостей, подбор учетных данных — который алгоритмически маскируется под легитимный фоновый профиль устройств. Стандартные пороговые системы обнаружения вторжений (IDS) и базовые алгоритмы классического машинного обучения оказываются невосприимчивыми к подобным микроаномалиям, демонстрируя критическое падение точности классификации при внедрении в реальную среду [4]. Стратегическим решением данной проблемы является полный отказ от попыток инспектирования полезной нагрузки в пользу интеллектуального анализа пространственно-временных метаданных сетевых потоков [5]. Целью данного исследования является проведение глубокого анализа зашифрованного сетевого трафика для выявления скрытых закономерностей кибератак. Извлечение этих нелинейных зависимостей, не требующее расшифровки пакетов, послужит строгим базисом для последующего проектирования отказоустойчивой нейросетевой архитектуры. Опираясь исключительно на паттерны метаданных, такая архитектура должна гарантировать не только высокоточную классификацию известных векторов компрометации, но и обеспечивать выявление скрытых аномалий нулевого дня (Zero-Day).

Формирование набора данных. В качестве эмпирического базиса для проведения исследования выбран современный набор данных CIC-IoT23, агрегирующий сетевой трафик от реальной топологии физических IoT-устройств [6]. Для прагматичной валидации предложенной концепции и подтверждения эффективности гибридной нейросетевой модели был разработан прототип (Proof of Concept, PoC). На данном этапе задача была алгоритмически сведена к бинарной классификации: математическому отделению легитимного фонового профиля устройств (класс Benign) от распределенной алгоритмической разведки (класс Recon-PortScan). Данный подход позволяет детально отладить механизмы слияния модальностей перед масштабированием системы на полный вектор угроз. Опираясь на ранее доказанную несостоятельность глубокого инспектирования полезной нагрузки в условиях тотального шифрования, процесс экстракции данных базируется исключительно на извлечении пространственно-временных метаданных уровней L3/L4 напрямую из сырых PCAP-дампов [7]. Вектор каждого отдельного пакета формируется из 9 микропризнаков: времени прибытия (IAT), длины пакета (IP_Len), состояния TCP-флагов, размера окна (Win_Size), портов источника и назначения (Src_Port, Dst_Port), типа протокола, времени жизни (TTL) и бинарного маркера TLS-рукопожатия. Поскольку единичный пакет не несет в себе достаточного контекста для выявления сложных L7-угроз, в основу архитектуры заложена Inter-flow (межпотоковая) методология [8]. Динамический парсинг трафика осуществляется с привязкой к IP-адресу источника (Src_IP) с применением механизма скользящего окна. Размер пространственно-временного тензора установлен на уровне N = 128 пакетов, с шагом сдвига в 64 пакета. Сдвиг окна на 50 % позволяет сохранить непрерывность контекста и не «разрывать» сигнатуры атак на границах. Чтобы модель лучше обобщала данные и не склонялась к доминирующему классу, выборку потребовалось строго сбалансировать. Нормальный трафик собирался из трех разных файлов дампов — по 4 000 окон из каждого. Такой подход позволил учесть естественную дисперсию сети. Итоговый набор данных включил по 12 000 тензоров для классов Benign и Recon-PortScan. Размерность обучающей матрицы составила (24000, 128, 9). Перед подачей в нейросеть признаки были нормализованы. Метрики существенно различаются по масштабу: например, значения IAT измеряются в микросекундах, а Win_Size достигает десятков тысяч байт. Приведение их к единому виду (нулевое среднее и единичная дисперсия) необходимо. Без этого градиенты рассчитываются нестабильно, а оптимизатор медленнее сходится в процессе обучения. Различия между классами хорошо видны на графике нормализованных тензоров (рис. 1). Нормальный трафик отличается равномерным изменением IAT и обращениями к ограниченному числу портов. При сканировании картина иная. В рамках одного окна из 128 пакетов происходит обращение к сотням уникальных портов. Именно этот аномальный охват портов должны улавливать механизмы внимания нейросети.

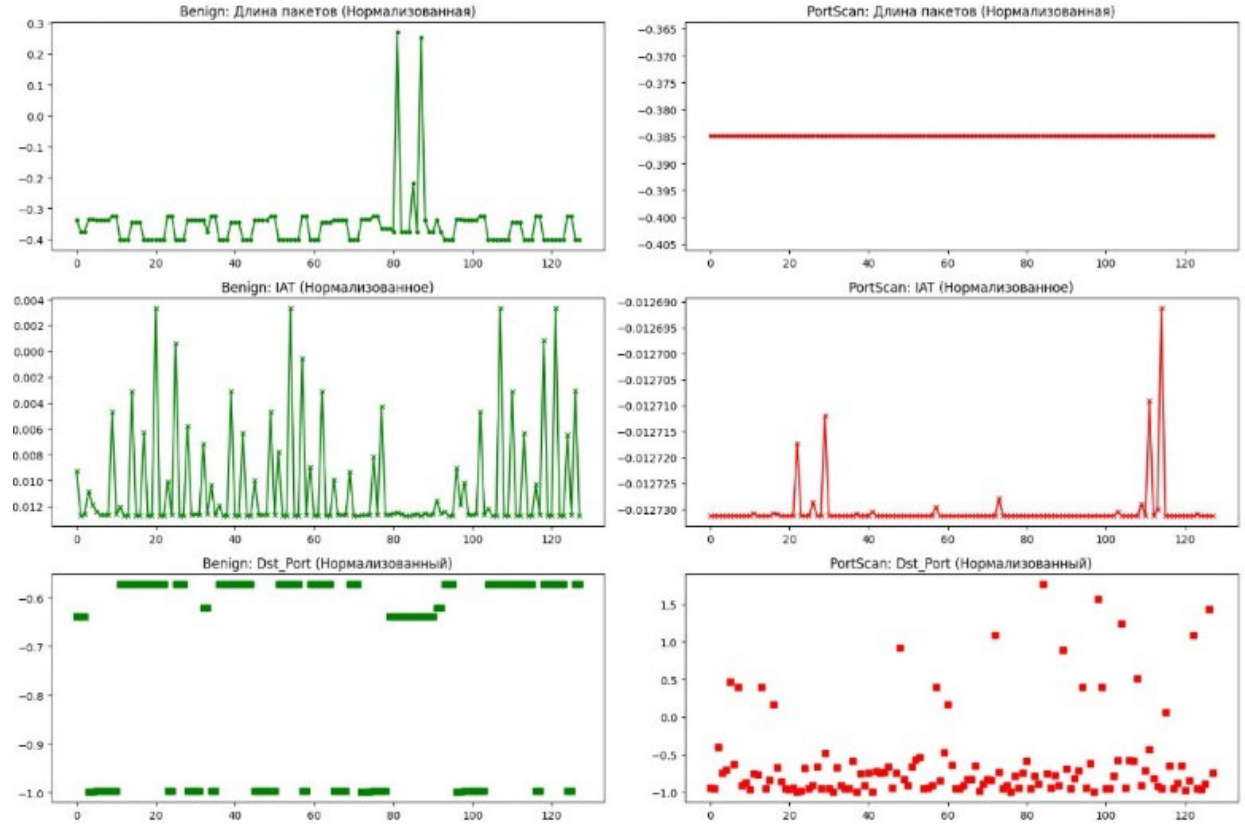

Рис. 1. График нормализованных тензоров: легитимный профиль/сканирование портов

Проектирование гибридной архитектуры нейронной сети. Проектирование гибридной архитектуры нейронной сети. Опираясь на результаты предыдущих экспериментов, мы существенно переработали архитектуру модели для более точного анализа признаков. От использования стандартных рекуррентных слоев (LSTM) было решено отказаться. Во-первых, они подвержены затуханию градиента на длинных последовательностях. Во-вторых, для их функционирования требуется сложная предварительная подготовка данных [9]. Вместо этого предложена гибридная архитектура, работающая параллельно и комбинирующая одномерную сверточную сеть (1D-CNN) с механизмами внимания Трансформера (рис. 2).

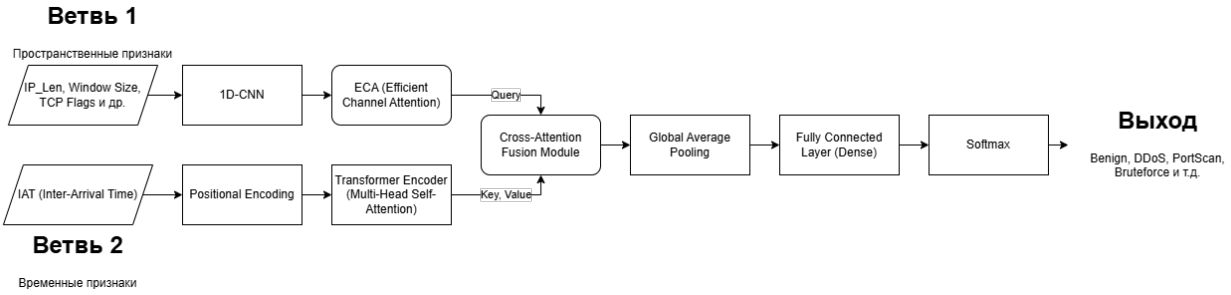

Рис. 2. Блок-схема гибридной параллельной архитектуры (1D-CNN + Transformer)

Для максимизации эффективности извлечения признаков входной тензор алгоритмически разделяется на две независимые вычислительные ветви: пространственную ветвь (1D-CNN + ECA), на вход которой подаются 8 геометрических и категориальных признаков пакета (IP_Len, TCP_Flags, Dst_Port и др.). Извлечение локальных паттернов, например штампованных размеров полезной нагрузки при фаззинге, осуществляется каскадом из двух слоев одномерной свертки с 64 фильтрами. Для подавления фонового шума IoT-устройств в ветвь интегрирован модуль эффективного канального внимания (Efficient Channel Attention, ECA). Сжимая тензор через слой глобального усреднения и применяя быструю одномерную свертку, ECA динамически перевзвешивает каналы нейросети, заставляя ее фокусироваться исключительно на критичных маркерах угрозы [10]. Временная ветвь (Transformer Encoder) изолированно обрабатывает колонку интервалов прибытия пакетов (IAT). Поскольку Трансформер лишен рекуррентности и обрабатывает данные параллельно, для математической фиксации порядка событий в окне применяется обучаемое позиционное кодирование (Positional Encoding). Линейно спроецированный вектор подается в легковесный модуль самовнимания (Multi-Head Self-Attention, 4 головы внима-

ния, размерность проекции 64 фильтра). Для стабилизации градиентов выходной тензор проходит через остаточные связи (Residual Connections) и слой нормализации (LayerNorm). Затем контекстуализированные данные обрабатываются сетью прямого распространения (Feed-Forward Network) с расширением размерности и повторной нормализацией. Данный механизм оценивает глобальный контекст сессии, позволяя сети безошибочно выявлять микросекундные аномалии и алгоритмическую цикличность машинных атак. Блок слияния (Cross-Attention Fusion Module) реализует синтез модальностей в центральном узле перекрестного внимания. Как показывают современные исследования, простая конкатенация признаков неэффективна для слияния разнородных данных [11]. Поэтому механизм матрично умножает запросы (Query), сформированные выявленными пространственными аномалиями (CNN), на временной контекст сессии (ключи и значения от трансформера). Итоговый тензор радикально сжимается слоем глобального усреднения (Global Average Pooling) для предотвращения переобучения и передается в полносвязный классификатор с функцией активации Softmax. Общее количество обучаемых параметров разработанной модели составило всего 178 146, что алгоритмически подтверждает ее архитектурную легковесность и высокую пригодность для интеграции в высоконагруженные сетевые узлы.

Обучение. Вычислительные эксперименты и компиляция модели проводились на базе фреймворка глубокого обучения TensorFlow 2.10.0 в операционной системе Windows 11. Аппаратная среда включала центральный процессор Intel Core i5-10400F (2.90 ГГц) и графический ускоритель NVIDIA RTX 3070, что обеспечило высокую скорость тензорных вычислений. Перед подачей в нейросеть сбалансированный набор данных был разделен на обучающую (Train) и валидационную (Test) выборки в классической пропорции 80/20 (19 200 обучающих и 4 800 тестовых тензоров). Обучение прототипа проводилось с использованием современного оптимизатора Adam (стартовый шаг обучения 0,001) и функции потерь Sparse Categorical Crossentropy. Для стабилизации сходимости градиентов был внедрен контроллер адаптивного шага обучения (ReduceLROnPlateau, снижающий шаг в 5 раз при плато валидационной ошибки) и механизм ранней остановки (EarlyStopping с ожиданием в 6 эпох). Модель сошлась и зафиксировала оптимальные веса на 30-й эпохе, не допустив переобучения (рис. 3).

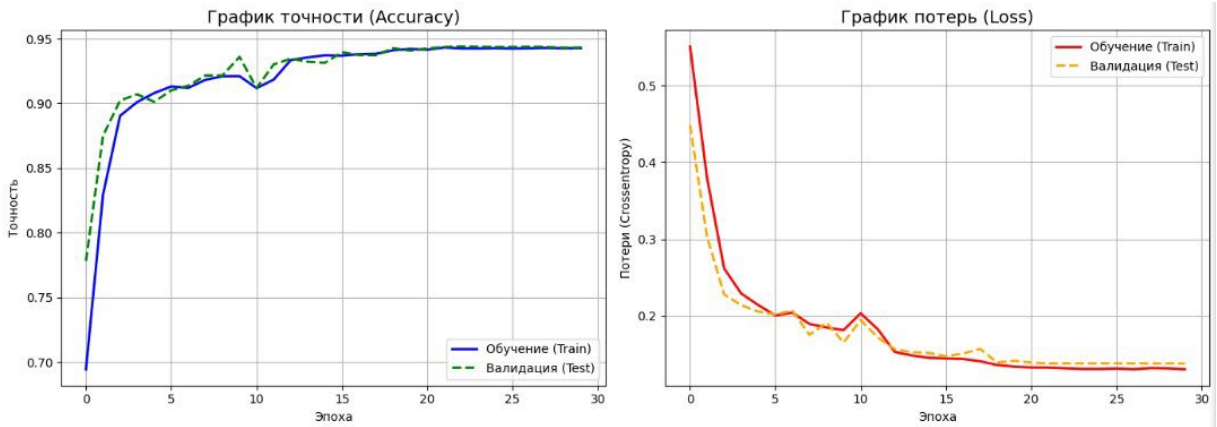

Рис. 3. Графики точности (Accuracy) и функции потерь (Loss)

Оценка эффективности на отложенной тестовой выборке (4 800 тензоров) подтвердила высокую обобщающую способность спроектированной архитектуры. В результате общая точность бинарной классификации достигла 94,42 %. Анализ распределения метрик на основе матрицы ошибок (рис. 4) и отчета классификации показал, что модель уверенно распознает нормальный трафик: полнота (Recall) для класса Benign составила 98,88 %.

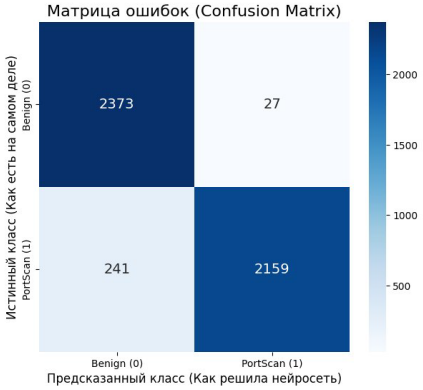

Рис. 4. Матрица ошибок легитимный профиль/сканирование портов

Для систем безопасности данный показатель означает крайне низкую долю ложных срабатываний. При этом полнота выявления сканирования (PortScan) составила 89,96 %. Пропуск около 10 % вредоносных окон связан не с недостаточной эффективностью предложенной архитектуры, а с особенностями исходного датасета. Анализ PCAP-файлов выявил высокую зашумленность. Внутри дампов с атаками присутствуют обычные пакеты IoT-устройств, которые авторы набора данных разметили как вредоносные. Модель закономерно интерпретирует их как нормальное поведение и классифицирует как Benign, за что получает статистический штраф. Несмотря на это, значение F1-меры (0,9441) подтверждает, что связка CNN и Трансформера уверенно справляется с классификацией зашифрованного трафика.

Заключение. Проведенное исследование подтверждает эффективность межпотокового анализа сетевых сессий. Разработанный прототип показывает, что анализ метаданных вместо глубокого инспектирования пакетов позволяет успешно выявлять скрытые угрозы прикладного уровня. Совмещение одномерных сверточных сетей и механизмов внимания позволило связать локальные признаки отдельных пакетов с общим ритмом сессии. В результате точность классификации достигла 94,42 %. Помимо оценки самой архитектуры, эксперимент выявил серьезную проблему открытых датасетов — наличие фонового шума. Трансформер смог распознать легитимный трафик даже внутри вредоносных файлов. Это означает, что дальнейший рост метрик обнаружения зависит не от усложнения структуры сети, а от математической очистки данных. В дальнейших исследованиях основное внимание будет уделено фильтрации обучающей выборки от фонового IoT-шума. Это повысит чувствительность сети к малозаметным сканированиям. Также планируется переход от бинарной к многоклассовой классификации для дифференциации более широкого спектра угроз [12]. Дополнительным направлением станет разработка методов защиты от атак нулевого дня (Zero-Day).

Список литературы

1. Полянская М. С. Анализ подходов к обнаружению атак в зашифрованном трафике. *Современные информационные технологии и ИТ-образование.* 2021;17(4):922–931. URL: http://sitito.cs.msu.ru/index.php/SITITO/article/view/802 (дата обращения: 20.04.2026).

2. Stein K, Mahyari A, Francia G, El-Sheikh E. A Transformer-Based Framework for Payload Malware Detection and Classification. In: Proceedings of *2024 IEEE World AI IoT Congress (AIIoT).* Seattle, WA, USA: IEEE; 2024. P. 105–111. http://doi.org/10.1109/AIIoT61789.2024.10579000

3. Huang H, Zhou Y, Jiang F. CLA-BERT: A Hybrid Model for Accurate Encrypted Traffic Classification by Combining Packet and Byte-Level Features. *Mathematics.* 2025;13(6):973. https://doi.org/10.3390/math13060973

4. Seydali M, Khunjush F, Akbari B, Dogani J. CBS: A Deep Learning Approach for Encrypted Traffic Classification with Mixed Spatio-Temporal and Statistical Features. *IEEE Access.* 2023;11:141674–141702. http://doi.org/ 10.1109/ACCESS.2023.3343189

5. Бердников М.Д., Гапон Н.В. Искусственный интеллект в задаче анализа и выявления угроз в зашифрованном сетевом трафике. Новые идеи. В*: труды Региональной научно-практической конференции, г. Ростов-на-Дону, 20–25 октября 2025 года. Ростов-на-Дону* : ДГТУ-Принт; 2025. С. 27–32

6. Neto ECP, Dadkhah S, Ferreira R, Zohourian A, Lu R, Ghorbani AA. CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. *Sensors.* 2023;23(13):5941. https://doi.org/10.3390/s23135941

7. Stein K, Mahyari A, Francia III G, El-Sheikh E. Packet Inspection Transformer: A Self-Supervised Journey to Unseen Malware Detection with Few Samples. *IEEE Access.* 2025;13:196336–196354. https://doi.org/10.1109/ACCESS.2025.3632207

8. Shi Q, Shi D, He L, Xiao Q, Zheng L, Ma J,TransGraphNet: Robust Detection of Malicious Encrypted Network Traffic via Transformer and Graph Neural Models. *PeerJ Computer Science*. 2025;11:e3353. https://doi.org/10.7717/peerj-cs.3353

9. Mei Y, Luktarhan N, Zhao G, Yang X. An Encrypted Traffic Classification Approach Based on Path Signature Features and LSTM. *Electronics.* 2024;13(15):3060. https://doi.org/10.3390/electronics13153060

10. Liu Z, Xie Y, Luo Y, Wang Y, Ji, X. TransECA-Net: A Transformer-Based Model for Encrypted Traffic Classification. *Applied Sciences.* 2025;15(6):2977. https://doi.org/10.3390/app15062977

11. Huang H, Zhou Y, Jiang F, Zhou X, Jiang Q. MFF: A Multimodal Feature Fusion Approach for Encrypted Traffic Classification. *Electronics.* 2025;14(13):2584. https://doi.org/10.3390/electronics14132584

12. Wang G, Gu Y. Multi-Task Scenario Encrypted Traffic Classification and Parameter Analysis. *Sensors.* 2024;24(10):3078. https://doi.org/10.3390/s24103078

Об авторах:

Михаил Дмитриевич Бердников, магистрант кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, Российская Федераций, г. Ростов-на-Дону, пл. Гагарина, 1), berdnikovmiha@gmail.com

Николай Валерьевич Гапон, кандидат технических наук, и. о. декана факультета «Автоматизация, мехатроника и управление», Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), ngapon@donstu.ru

Ольга Александровна Сафарьян, кандидат технических наук, доцент, заведующий кафедрой «Кибербезопасность информационных систем» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), osafaryan@donstu.ru

Конфликт интересов: **авторы заявляют об отсутствии конфликта интересов.**

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Mikhail D. Berdnikov, Master's Degree Student of the Cybersecurity of Information Systems Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), berdnikovmiha@gmail.com

Nikolai V. Gapon, Cand.Sci.(Engineering), Acting Dean of the Faculty of Automation, Mechatronics and Control, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), ngapon@donstu.ru

Olga A. Safaryan, Cand.Sci. (Engineering), Associate Professor, Head of the Cybersecurity of Information Systems Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), osafaryan@donstu.ru

Conflict of Interest Statement: **the authors declare no conflict of interest.**

All authors have read and approved the final manuscript.