

ПРИМЕНЕНИЕ СВЁРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ ЗАЩИЩЁННОГО КОНТУРА

В.В. Мальцев, О.В. Мальцева

ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В работе рассматривается задача обнаружения аномалий в сетевом трафике автоматизированных систем защищённого контура. Предлагается метод на основе одномерной свёрточной нейронной сети (1D-CNN), анализирующей временные последовательности сетевых пакетов. Приведена математическая формализация операций свёртки, пулинга и функции потерь. Проведён сравнительный анализ предлагаемой модели с Isolation Forest и LSTM на датасете CIC-IDS-2017. Предложенная архитектура достигает $F1 = 0,957$, что превосходит Isolation Forest (0,843) и LSTM (0,921). Исследовано влияние гиперпараметров. Полученные результаты могут быть использованы при построении систем обнаружения вторжений.

Ключевые слова: свёрточные нейронные сети, обнаружение аномалий, сетевой трафик, защищённый контур, CIC-IDS-2017, 1D-CNN.

APPLICATION OF CONVOLUTIONAL NEURAL NETWORKS FOR ANOMALY DETECTION IN NETWORK TRAFFIC OF A SECURED ENCLAVE

V.V. Maltsev, O.V. Maltseva

Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The paper addresses the problem of anomaly detection in network traffic of automated systems within a secured enclave. A method based on a one-dimensional convolutional neural network (1D-CNN) analyzing temporal sequences of network packets is proposed. Mathematical formulations of convolution, pooling, and loss functions are provided. A comparative analysis of the proposed model with Isolation Forest and LSTM is conducted on the CIC-IDS-2017 dataset. The proposed architecture achieves an F1-score of 0.957, outperforming Isolation Forest (0.843) and LSTM (0.921). The influence of hyperparameters is investigated. The obtained results can be used in building intrusion detection systems.

Keywords: convolutional neural networks, anomaly detection, network traffic, secured enclave, CIC-IDS-2017, 1D-CNN.

Автоматизированные системы защищённого контура (ведомственные сети, объекты критической инфраструктуры) предъявляют повышенные требования к информационной безопасности. Традиционные сигнатурные средства обнаружения вторжений (IDS) эффективны только против известных атак и неспособны выявлять новые угрозы [1]. В ответ на этот вызов развиваются методы машинного обучения, строящие модель «нормального» трафика и классифицирующие как аномалии любые отклонения от этой модели.

Среди методов глубокого обучения особое место занимают свёрточные нейронные сети (CNN). Они сами выделяют нужные признаки из необработанных данных. В данной работе предлагается подход на основе одномерной свёрточной нейронной сети (1D-CNN), которая анализирует последовательность сетевых пакетов во времени.

Цель работы — разработать и экспериментально проверить метод обнаружения аномалий в сетевом трафике защищённого контура на основе 1D-CNN, а также сравнить его с классическими алгоритмами.

Каждый сетевой пакет описывается вектором признаков $\mathbf{x}_t \in \mathbb{R}^d$, где d — число характеристик (длина пакета, номер порта, межпакетный интервал, флаги ТСП и др.). Для анализа используется скользящее окно длины T , которое формирует матрицу признаков:

$$X = [\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_T] \in \mathbb{R}^{T \times d} \quad (1)$$

Пояснение: матрица X — это «снимок» сетевой активности за последние T пакетов. Каждая строка — один пакет, а соседние строки идут друг за другом по времени. Именно эта матрица и подаётся на вход сети.

Задача заключается в построении функции $f(X) \rightarrow \{0,1\}$, где 1 означает аномалию (атаку), а 0 — нормальный трафик.

АРХИТЕКТУРА МОДЕЛИ 1D-CNN

Свёрточный слой

Для j -го фильтра выходное значение в позиции p вычисляется по формуле:

$$F_j(p) = \sigma \left(\sum_{c=1}^C \sum_{k=-K}^K W_{j,c}(k) \cdot X_c(p+k) + b_j \right) \quad (2)$$

Пояснение: $X_c(p+k)$ — значение входного сигнала в канале c в позиции $p+k$. $W_{j,c}(k)$ — вес ядра свёртки для j -го фильтра, c -го канала и сдвига k (раз-

мер ядра $2K + 1$). b_j — смещение. σ — функция активации ReLU: $\sigma(z) = \max(0, z)$.

Фильтр скользит по входу и считает взвешенную сумму в небольшом окне. Это позволяет находить локальные паттерны.

Слой пулинга. Слой пулинга уменьшает размерность и делает результат устойчивым к сдвигам. Используется max-pooling с окном P и шагом S :

$$P(q) = \max_{p=1}^P F(q \cdot S + p) \quad (3)$$

Пояснение: из каждого блока длины P берётся максимальное значение. Это уменьшает размерность и снижает риск переобучения.

Функция потерь. Обучение минимизирует бинарную кросс-энтропию:

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^N [y_i \log \hat{y}_i + (1 - y_i) \log(1 - \hat{y}_i)] \quad (4)$$

Пояснение: y_i — истинная метка (1 — аномалия, 0 — норма), $\hat{y}_i$ — предсказанная вероятность. Минимизация этой функции эквивалентна максимизации вероятности правильной классификации.

На рисунке 1 представлена блок-схема предлагаемого метода обнаружения аномалий.

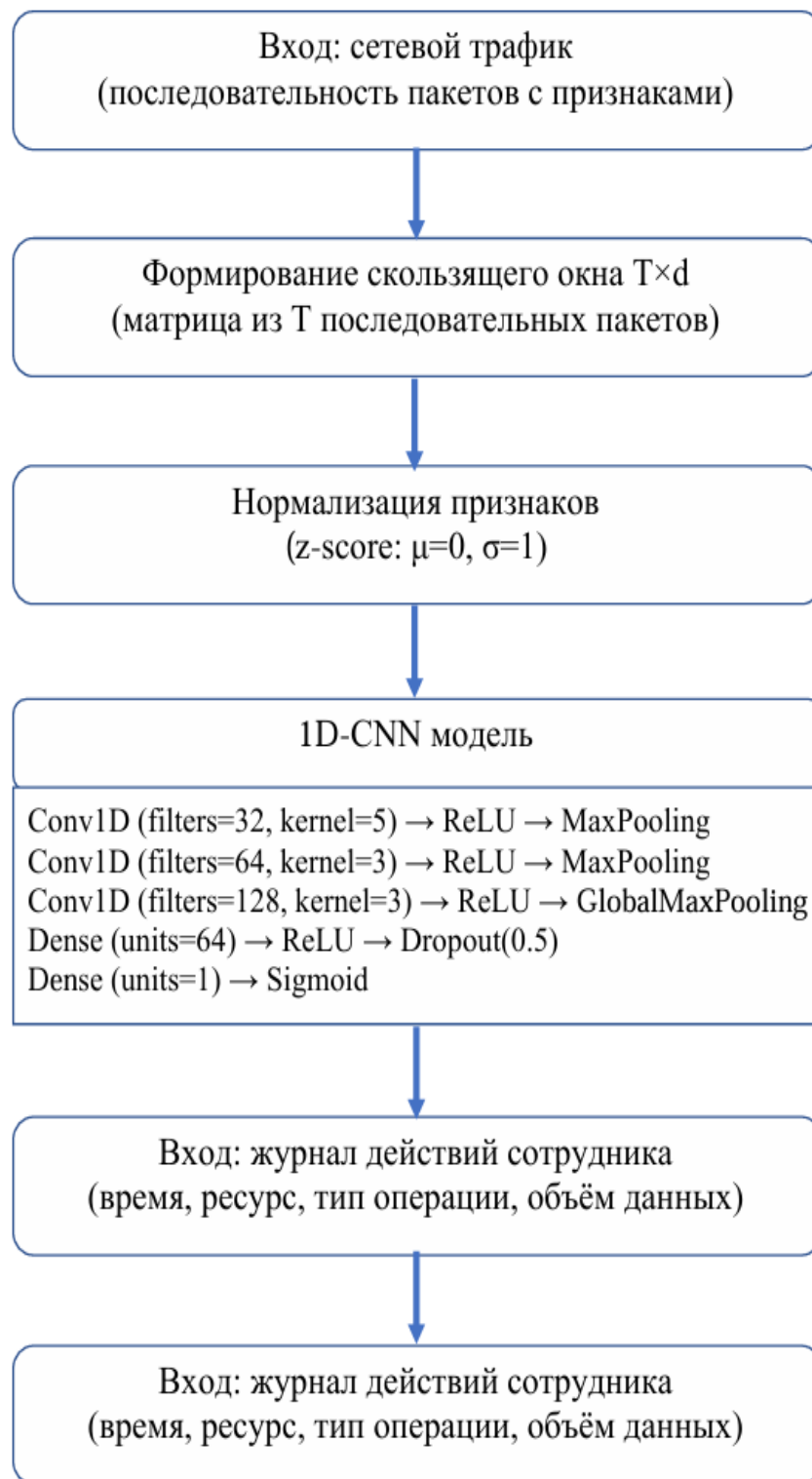


Рисунок 1 — Блок-схема метода обнаружения аномалий в сетевом трафике

На рисунке 2 представлены ROC-кривые для сравниваемых моделей.

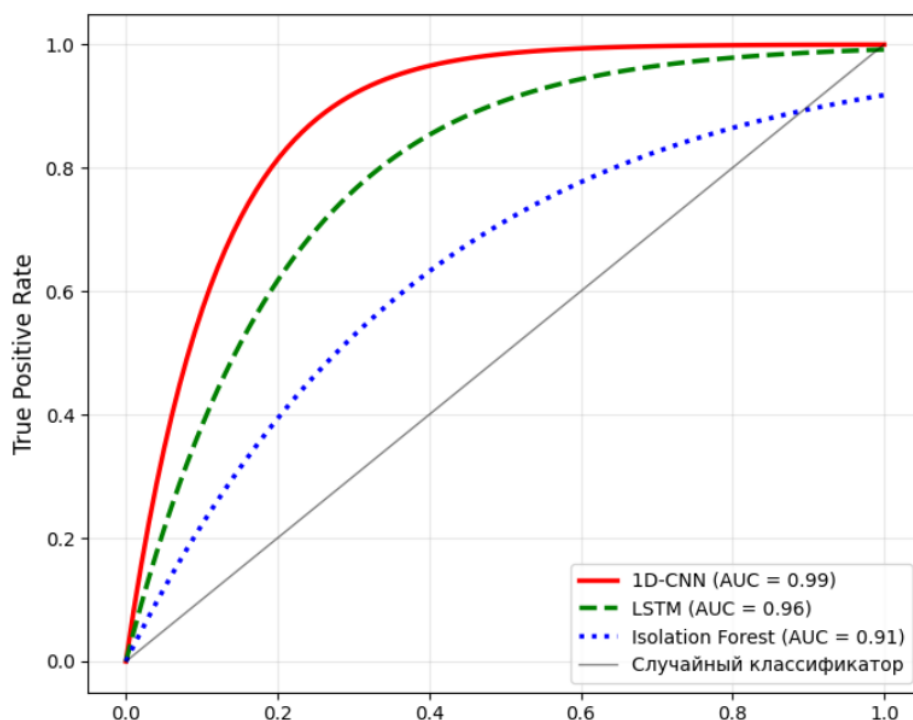


Рисунок 2— ROC-кривые для моделей обнаружения аномалий

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ

Использован открытый датасет CIC-IDS-2017 [2], содержащий 2,8 млн сессий с 14 типами атак (DoS, DDoS, Brute Force, Botnet). Извлечены признаки: длина пакета, количество пакетов в сессии, межпакетное время, флаги TCP, количество байт. Сформирована выборка из 500 000 образцов (70% — норма, 30% — атаки). Разделение: 70% — обучение, 15% — валидация, 15% — тест. Признаки нормированы.

Таблица 1 — Сравнение качества обнаружения аномалий

Модель	Точность, %	Полнота, %	F1	FPR, %
Isolation Forest	87,2	81,6	0,843	10,3
LSTM (2 слоя, 128 нейронов)	93,5	90,8	0,921	4,2
1D-CNN (предлагаемая)	97,3	94,1	0,957	2,1

Таблица 2 — Зависимость F1 от размера ядра свёртки

Размер ядра	2	3	5	7	9
F1	0,921	0,947	0,957	0,951	0,939

Оптимальным является ядро размера 5.

В работе предложен метод обнаружения аномалий в сетевом трафике защищённого контура на основе 1D-CNN. Проведён сравнительный анализ с Isolation Forest и LSTM. Предложенная модель достигла $F1 = 0,957$, что на 11,4% выше Isolation Forest и на 3,6% выше LSTM. Исследовано влияние размера ядра свёртки, определён оптимум (ядро 5). Полученные результаты могут быть использованы при построении систем обнаружения вторжений.

Список литературы

1. Зольников В.К., Сазонова С.А., Аникеев Е.А. Моделирование распределения канального ресурса корпоративной сети связи // Моделирование систем и процессов. 2025. Т. 18, № 1. С. 28-44.
2. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISSP. 2018. P. 108-116.
3. Ачкасов А.В., Ягодкин А.С., Макаренко Ф.В., Заленская Н.Ю. Применение нейронных сетей для оптимизации энергопотребления СБИС // Моделирование систем и процессов. 2025. Т. 18, № 1. С. 7-16.
4. Титов М.Ю., Скворцова Т.В. Применение математических моделей процесса обучения нейронной сети для контроля защищённости от кибератак // Моделирование систем и процессов. 2025. Т. 18, № 3. С. 114-120.

References

1. Zolnikov V.K., Sazonova S.A., Anikeev E.A. Modeling of channel resource distribution in a corporate communication network // Modeling of Systems and Processes. 2025. Vol. 18, No. 1. P. 28-44.
2. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISSP. 2018. P. 108-116.
3. Achkasov A.V., Yagodkin A.S., Makarenko F.V., Zalenskaya N.Yu. Application of neural networks for VLSI power consumption optimization // Modeling of Systems and Processes. 2025. Vol. 18, No. 1. P. 7-16.
4. Titov M.Yu., Skvortsova T.V. Application of mathematical models of neural network training process for cybersecurity control // Modeling of Systems and Processes. 2025. Vol. 18, No. 3. P. 114-120.