СТАТЬИ

УДК 004.056:004.032.26
DOI

ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ СЕТЕВОГО ТРАФИКА НА ОСНОВЕ АНСАМБЛЯ СПЕЦИАЛИЗИРОВАННЫХ ИМПУЛЬСНЫХ НЕЙРОННЫХ СЕТЕЙ

Абаев В. А. ORCID ID 0000-0002-1967-8116,
Будаев Е. С. ORCID ID 0000-0002-3718-0282,
Хасанова З. Р. ORCID ID 0000-0002-4683-1673

Федеральное государственное образовательное бюджетное учреждение высшего образования «Финансовый университет при Правительстве Российской Федерации», Москва, Российская Федерация, e-mail: esbudaev@fa.ru

Цель исследования – разработка и количественная оценка математико-программного обеспечения интеллектуальной подсистемы анализа сетевого трафика на основе ансамбля специализированных импульсных нейронных сетей в условиях сокращенного признакового пространства и междоменного переноса. В рамках исследования выполнены задачи: формирование редуцированного инженерного пространства признаков для датасетов UNSW-NB15, CIC-IDS-2017 и TON_IoT; математическая формализация этапов нормализации, спайкового кодирования, стохастического инференса и ансамблевой агрегации; построение программно-алгоритмического контура обработки сетевых признаков; сравнительный анализ специализированных SNN-архитектур; оценка качества бинарной классификации по метрикам Precision, Recall, F1, FPR и MCC; анализ устойчивости программно-алгоритмического решения при переносе на внешние датасеты без дообучения; сопоставление ансамблевого подхода с универсальной SNN-моделью; оценка применимости событийно-ориентированной обработки данных в задачах интеллектуального анализа сетевого трафика. Исследование опирается на имитационное моделирование полного цикла функционирования интеллектуальной подсистемы анализа сетевого трафика – от инженерного преобразования признаков и нормализации до спайкового кодирования, стохастического инференса, ансамблевой агрегации и формирования итогового решения. Проведен сравнительный анализ специализированных архитектур, стратегий ансамблевого голосования и кросс-датасетного переноса. Предложено математико-программное решение, основанное на редуцированном пространстве признаков, ансамбле специализированных SNN-моделей и калибруемом механизме принятия решения. В статье обосновано, что эффективная интеллектуальная обработка сетевого трафика требует не только построения классификатора, но и согласованного программно-алгоритмического контура, учитывающего неоднородность сетевых событий, стохастическую природу спайкового кодирования, переносимость между доменами наблюдений и ограничения вычислительных ресурсов. Ключевым результатом исследования является подтверждение того, что ансамбль специализированных импульсных нейронных сетей в компактном признаковом пространстве может служить основой интеллектуальной подсистемы анализа сетевого трафика в информационно-телекоммуникационных системах.

Ключевые слова: интеллектуальные методы обработки данных, архитектура вычислительной модели, анализ сетевого трафика, информационно-телекоммуникационные системы, инженерия признаков

INTELLIGENT ANALYSIS OF NETWORK TRAFFIC BASED ON AN ENSEMBLE OF SPECIALIZED IMPULSE NEURAL NETWORKS

Abaev V. A. ORCID ID 0000-0002-1967-8116,
Budaev E. S. ORCID ID 0000-0002-3718-0282,
Khasanova Z. R. ORCID ID 0000-0002-4683-1673

Federal State Educational Budgetary Institution of Higher Education "Financial University under the Government of the Russian Federation", Moscow, Russian Federation, e-mail: esbudaev@fa.ru

The purpose of the research is to develop and quantify mathematical software for an intelligent subsystem for network traffic analysis based on an ensemble of specialized impulse neural networks in conditions of reduced feature space and cross–domain transfer. Within the framework of the study, the following tasks were performed: formation of a reduced engineering feature space for datasets UNSW-NB15, CIC-IDS-2017 and TON_IoT; mathematical formalization of the stages of normalization, spike coding, stochastic inference and ensemble aggregation; construction of a software-algorithmic contour for processing network features; comparative analysis of specialized SNN architectures; evaluation of the quality of binary classification using Precision, Recall, F1, FPR and MCC metrics; analysis of the stability of a software-algorithmic solution when transferred to external datasets without additional training; comparison of an ensemble approach with a universal SNN model; assessment of the applicability of an event-oriented data processing in network traffic mining tasks. The research is based on simulation modeling of the full cycle of the intelligent subsystem of network traffic analysis – from engineering transformation of features and normalization to spike coding, stochastic inference, ensemble aggregation and the formation of the final solution. A comparative analysis of specialized architectures, ensemble voting strategies, and cross-dataset migration has been performed. A mathematical and software solution based on a reduced feature space, an ensemble of specialized SNN models, and a calibrated decision-making mechanism is proposed. The article proves that effective intelligent processing of network traffic requires not only the construction of a classifier, but also a consistent software-algorithmic contour that considers the heterogeneity of network events, the stochastic nature of spike coding, portability between observation domains and limitations of computing resources. The key result of the study is the confirmation that an ensemble of specialized impulse neural networks in a compact feature space can serve as the basis for an intelligent subsystem for analyzing network traffic in information and telecommunications systems.

Keywords: intelligent data processing methods, network traffic analysis, computational model architecture, information and telecommunication systems, feature engineering

Введение

Одним из ключевых аспектов разработки интеллектуальных подсистем анализа сетевого трафика является построение согласованного математико-программного контура обработки данных, включающего инженерное преобразование признаков, нормализацию, событийное кодирование, нейросетевой инференс и процедуру принятия решения. В информационно-телекоммуникационных системах анализ сетевого трафика связан не только с задачей классификации состояний «норма» / «атака», но и с необходимостью разработки воспроизводимого программно-алгоритмического решения [1], устойчивого к сокращению признакового пространства, стохастической обработке входных данных и изменению домена наблюдений.

Прикладная значимость такой подсистемы определяется возможностью использования ее результатов для поддержки принятия решений при выявлении аномальных и атакующих сценариев в компьютерных сетях. При этом высокая стоимость пропуска реального атакующего воздействия по сравнению с затратами на обработку ложных срабатываний определяет приоритет полноты обнаружения (Recall), тогда как сохранение приемлемой точности (Precision) необходимо для ограничения избыточных тревог и обеспечения эксплуатационной пригодности программного решения [2, 3]. Сочетание инженерии признаков, ансамблевого обучения и импульсных нейронных сетей позволяет формировать интеллектуальные механизмы анализа сетевого трафика, ориентированные на обработку данных в компактном признаковом пространстве, событийное представление входов и переносимость между различными наборами сетевых наблюдений [4, 5].

Цель исследования – разработка и количественная оценка математико-программного обеспечения интеллектуальной подсистемы анализа сетевого трафика на основе редуцированного признакового пространства, вероятностного спайкового кодирования и ансамбля специализированных импульсных нейронных сетей в условиях междоменного переноса.

Материалы и методы исследования

Задача обнаружения сетевых атак рассматривается как бинарная классификация сетевого трафика («норма» / «атака») в условиях сокращенного признакового пространства и междоменного переноса. Целевой функцией является обеспечение высокой полноты обнаружения (Recall) при приемлемом уровне точности (Precision) и контролируемой доле ложноположительных срабатываний (FPR), поскольку пропуск атакующего воздействия в информационно-телекоммуникационной системе является более критичным, чем единичное ложное срабатывание.

Важной задачей является инженерное конструирование признакового пространства, поскольку в работе исследуется не прямая классификация в исходном пространстве признаков, а классификация в специально сформированном компактном представлении, обладающем интерпретируемостью и переносимостью между датасетами [6, 7]. Категории инженерных признаков, их содержательное назначение и обоснование выбора представлены в табл. 1.

Таблица 1

Категории признаков модели

Категория	Содержательное назначение	Обоснование
Интенсивность трафика	Характеризует общий уровень сетевой активности	Позволяет выявлять аномальное увеличение или снижение нагрузки
Аномалии транспортного уровня	Отражает отклонения в сетевых соединениях и транспортных характеристиках	Существенна для выявления сетевых аномалий и DoS-сценариев
Неуспешные попытки аутентификации	Характеризует признаки нарушений при доступе	Позволяет выявлять атаки, связанные с аутентификацией
Признаки эскалации привилегий	Отражает попытки повышения уровня доступа	Существенна для детекции атак, связанных с повышением привилегий
Поведенческие отклонения	Характеризует нетипичное поведение объектов наблюдения	Позволяет выделять аномальные сценарии активности
Сигналы средств безопасности	Отражает срабатывания и сопутствующие признаки из защитного контура	Вносит дополнительный прикладной контекст в модель
Временной контекст	Учитывает динамику и последовательность событий	Необходим для выявления распределенных во времени атакующих сценариев

Примечание: составлена авторами на основе полученных данных в ходе исследования.

Формально переход от исходного признакового пространства сетевого потока к компактному инженерному представлению задается оператором

$$\Phi : \mathbb{R}^{49} \to \mathbb{R}^{13},\ e = \Phi(x),\ e \in \mathbb{R}^{13}, \quad (1)$$

где x – исходный вектор признаков;

e – редуцированное инженерное представление входных данных.

Использование полного 49-мерного пространства в работе не рассматривается как целевая конфигурация вследствие его избыточности, ограниченной интерпретируемости части исходных полей и слабой переносимости между датасетами.

Поскольку инженерные признаки различаются по физической природе и численному масштабу, следующим необходимым этапом является нормализация. В модели вводится оператор

$$N : \mathbb{R}^{13} \to [0,1]^{13}, \quad (2)$$

который действует покоординатно по схеме min-max нормализации:

$$\tilde{e} = \frac{e_j - e_j^{min}}{e_j^{max} - e_j^{min}}, \quad (3)$$

где e_j^{max}, e_j^{min} – минимальное и максимальное значения j-го признака, вычисленные по обучающей выборке.

Использование именно такой нормализации обусловлено тем, что на следующем этапе каждый признак интерпретируется как интенсивность события в процедуре спайкового кодирования. Принципиально важно, что параметры нормализации фиксируются по обучающей выборке и затем переносятся на тестовые и внешние датасеты. Это исключает утечку информации из тестовых данных в процедуру предварительной обработки.

После нормализации система переходит от статического числового представления к событийной временной динамике, пригодной для обработки импульсными нейронными сетями. Для этого вводится оператор спайкового кодирования

$$S : [0,1]^{13} \to \{0;1\}^{13 \times T}, \quad (4)$$

где T – длина временного окна кодирования, а результатом является бинарная матрица спайков. В основной конфигурации используется вероятностное rate coding, при котором каждый нормализованный признак интерпретируется как параметр бернуллиевского процесса генерации спайков [8, 9]:

$$\Pr\left(S_j[t] = x\right) = \tilde{e}_j^{\,x}\left(1 - \tilde{e}_j\right)^{1-x},\ x \in \{0,1\}. \quad (5)$$

Иными словами, чем больше значение $\tilde{e}$, тем выше вероятность генерации спайка на каждом временном шаге. Такое кодирование научно оправдано по двум причинам. Во-первых, оно обеспечивает естественное согласование между непрерывным входным пространством и дискретной событийной природой SNN. Во-вторых, оно позволяет рассматривать обработку входа как стохастическую динамическую процедуру, что методически важно для моделирования системы, ориентированной на реальную сетевую среду, в которой наблюдения по своей природе подвержены шуму, вариативности и случайным отклонениям. Следствием вероятностного кодирования является стохастичность выхода модели даже для одного и того же входного объекта, и именно поэтому в исследовании использовался многократный стохастический инференс с последующим усреднением результатов.

На рисунке представлена структурно-логическая схема реализации подсистемы анализа данных. Она фиксирует последовательность преобразований от сетевого потока к решению об атаке и тем самым задает структуру всей методики оценки.

После преобразования входа в спайковую форму данные подаются на ансамбль специализированных импульсных нейронных сетей. Формально ансамбль задается множеством:

$$M = \{f_1, f_2, \ldots, f_m\}, \quad (6)$$

где каждая модель f_m отображает спайковое представление входного объекта в частную вероятность наличия атаки. Для нового объекта x функция принятия решения (предсказания) выглядит так:

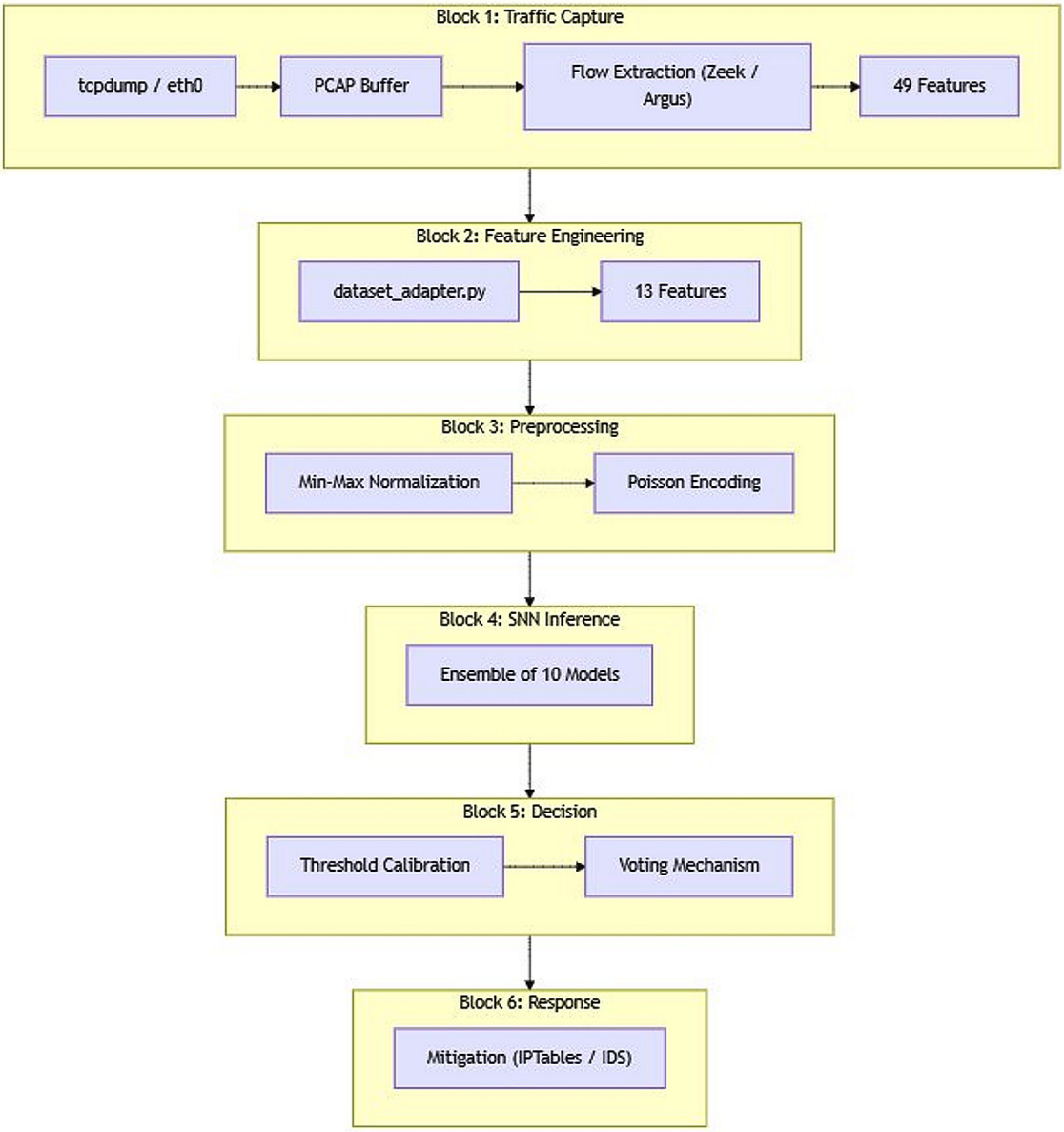
$$p_m(x, S) = f_m\left(S\left(N\left(\Phi(x)\right)\right)\right). \quad (7)$$

В исследовании рассматривались несколько архитектур-кандидатов, из которых в финальный ансамбль были включены семейства Attention Spike Net, Multi Scale SpikeNet и Anomaly Spike Autoencoder, показавшие наилучшее сочетание качества классификации, устойчивости к калибровке порога и переносимости на внешние датасеты.

Базовым вычислительным элементом используемых сетей является нейрон типа Leaky Integrate-and-Fire [8, 10]. Его мембранный потенциал на шаге времени t описывается уравнением

$$U[t] = \beta U[t-1] + I[t], \quad (8)$$

где $U[t]$ – внутренний потенциал нейрона, β – коэффициент утечки (затухания), $I[t]$ – входное воздействие [11, 12].



Структурно-логическая схема реализации подсистемы анализа данных
Примечание: составлен авторами по результатам данного исследования

Спайк возникает при превышении потенциалом порога:

$$S[t] = H\left(U[t] - U_{thr}\right). \qquad (9)$$

после чего выполняется сброс мембранного потенциала:

$$U[t] \leftarrow U[t]\left(1 - S[t]\right). \qquad (10)$$

Поскольку отдельные модели ансамбля решают частные задачи обнаружения атак, их выходы агрегируются в единое итоговое решение.

В работе используется стратегия мягкого голосования, при которой итоговая вероятность атаки определяется как среднее значение частных вероятностей:

$$p_{ens}(x) = \frac{1}{M}\sum_{m=1}^{M} p_m(x). \qquad (11)$$

Итоговое бинарное решение задается порогом τ:

$$\tilde{y} = \begin{cases} 1, p_{ens}(x) \geq \tau \\ 0, p_{ens}(x) < \tau \end{cases}. \qquad (12)$$

Из-за стохастической природы rate coding выход каждой модели для фиксированного входного объекта рассматривается

как случайная величина. Поэтому в работе используется многократный стохастический инференс с последующим усреднением:

$$p_m(x) = \frac{1}{K}\sum_{k=1}^{K} p_m\left(x, S^{(k)}\right). \quad (13)$$

В проведенном исследовании использовалось $K = 10$. Эта процедура эквивалентна приближенной оценке математического ожидания выхода модели по случайности, вносимой этапом кодирования, и тем самым делает итоговые оценки качества более воспроизводимыми и методологически корректными.

Экспериментальная схема построена таким образом, чтобы разделить этапы обучения параметров, выбора рабочей конфигурации и финальной оценки обобщающей способности. [13]. Исходная обучающая часть данных разбивается на три непересекающихся подмножества:

$$D_{train} = D_{learn} \cup D_{val} \cup D_{cal}, \quad (14)$$

где D_{learn} использовалось для обновления весов моделей, D_{val} – для ранней остановки и выбора чекпоинтов, D_{cal} – для калибровки рабочего порога τ.

В качестве основного источника данных используется датасет UNSW-NB15 [14], содержащий как нормальный трафик, так и различные типы атак. Для оценки междоменной устойчивости дополнительно используются датасеты CIC-IDS-2017 [15, 16] и TON_IoT [17], при этом обучение выполняется только на UNSW-NB15, а тестирование на внешних датасетах проводится без обновления параметров модели:

$$\theta^* = \arg\min_{\theta} \sum_{(x_i, y_i)\in D_{learn}} L\left(f_\theta(x_i), y_i\right). \quad (15)$$

В качестве функции потерь используется Focal Loss с пер-классовыми весами. Для повышения устойчивости обучения применяются ранняя остановка, регуляризация, label smoothing, mixup, ограничение нормы градиентов и усреднение весов.

Для обеспечения воспроизводимости численного эксперимента программная реализация методики была выполнена в виде модульного вычислительного контура на языке Python 3.10 с использованием библиотек NumPy, pandas и scikit-learn для загрузки, предобработки и формирования инженерного признакового пространства, а также фреймворков PyTorch 2.1 и snnTorch 0.9 для реализации, обучения и инференса специализированных импульсных нейронных сетей [18]. Структура программного проекта включала блок предварительной обработки сетевых flow-признаков, блок формирования редуцированного 13-мерного инженерного признакового пространства, модуль min-max нормализации, модуль вероятностного rate coding, набор специализированных SNN-моделей, модуль K-кратного стохастического инференса, модуль ансамблевой агрегации решений по схеме soft voting и модуль калибровки порога. Все параметры нормализации вычислялись исключительно по обучающей выборке и далее без изменения применялись к валидационным, калибровочным, тестовым и внешним наборам данных, что исключало утечку информации из тестовых данных в процедуру предварительной обработки. Эксперименты выполнялись в CPU-only режиме на вычислительном узле fin-104 при фиксированной схеме предобработки, едином наборе инженерных признаков, числе стохастических прогонов K = 10 и неизменяемых параметрах модели при переносе на внешние датасеты CIC-IDS-2017 и TON_IoT без дообучения.

Калибровка порога принятия решения рассматривается как самостоятельный этап. Оптимальное значение τ^* подбирается на калибровочном множестве как компромисс между качеством классификации и допустимым уровнем ложных срабатываний:

$$\tau^* = \arg\max F1\,(\tilde{y}_\tau)$$

при ограничении на $FPR(\tilde{y}_\tau)$. (16)

Для оценки устойчивости модели используется кросс-датасетное тестирование без дообучения, при котором параметры ансамбля, обученного на UNSW-NB15, переносятся на выборки CIC-IDS-2017 и TON_IoT без обновления весов. Анализируются изменение F1, изменение Recall и рост FPR. Такой подход позволяет оценить частичную инвариантность системы к смене распределения входных данных и таксономии атак.

Результаты исследования и их обсуждение

Экспериментальные исследования показали, что предложенная архитектура обеспечивает устойчивое качество обнаружения сетевых атак в условиях сокращенного признакового пространства. Среднее значение F1 по функциональным группам составило 0,831, средний Recall – 0,872, что подтверждает целесообразность архитектурной специализации моделей. Наилучшие результаты на основном датасете UNSW-NB15 получены при ансамблевой агрегации по схеме soft voting с порогом 0,50: F1 = 0,848, Recall = 0,906. Это показывает, что коллективное решение специализированных детекторов эффективнее отдельной универсальной модели [19, 20].

Таблица 2

Сводные показатели качества и вычислительной эффективности реализации

Сценарий	Объем и длительность	Качество классификации	Вычислительные характеристики
Основной стендовый прогон	1000 flow, 35 мин	Precision = 0,978; Recall = 0,960; F1 = 0,969; FPR = 0,022	Throughput = 0,48 flow/sec; latency = 2,10 sec/flow; RSS variation ≤ 0,1 %; IPS bypass = 0 / 509
Длительный прогон стабильности	15 000 flow, 6 ч	Precision = 0,978; Recall = 0,958; F1 = 0,968; FPR = 0,021	Throughput = 0,69 flow/sec; latency = 1,44 sec/flow; RSS variation = 0,047 %

Примечание: составлена авторами на основе полученных данных в ходе исследования

Анализ полноты обнаружения по типам атак показал, что для категорий Reconnaissance, Shellcode, Analysis и Worms достигнут Recall = 1,000. Для Generic значение Recall составило 0,994, для DoS – 0,967, для Fuzzers – 0,945, для Exploits – 0,927. Следовательно, редуцированное 13-мерное инженерное пространство признаков сохраняет существенную различающую информацию, хотя для наиболее вариативных атак полнота снижается.

Кросс-датасетное тестирование без дообучения подтвердило частичную междоменную устойчивость системы. На CIC-IDS-2017 получено F1 = 0,729, на TON_IoT – F1 = 0,894. Различие результатов указывает на зависимость переносимости от согласованности внешнего домена с выбранным инженерным представлением признаков и процедурой нормализации. Сопоставление с единой универсальной SNN-моделью показало преимущество ансамблевой декомпозиции, особенно для задач аутентификации, разведки и аномального поведения.

Для оценки вычислительной эффективности и устойчивости программной реализации была проведена стендовая проверка IPS-конфигурации на сценарии CIC-IDS-2017 Friday DDoS в CPU-only режиме [21]. Оценивались качество классификации, средняя скорость обработки, задержка обработки flow-записи и стабильность потребления оперативной памяти. Основные результаты представлены в табл. 2.

Полученные результаты показывают, что разработанная реализация сохраняет устойчивое качество обработки сетевого трафика при увеличении объема входного потока с 1000 до 15 000 flow-записей. В длительном прогоне изменение F1 составило менее 0,001 относительно основного стендового прогона, а variation RSS после прогрева не превысил 0,047 %, что указывает на стабильность потребления памяти в проверенном CPU-only режиме. При этом нагрузочная проверка выявила ограничение текущей реализации: обработка потока до 10 flow/sec выполнялась без потерь, тогда как при 20 flow/sec фиксировались пропуски, что определяет направление дальнейшей оптимизации инференса.

Заключение

В результате исследования разработан и экспериментально оценен программно-алгоритмический контур интеллектуальной подсистемы анализа сетевого трафика на основе редуцированного признакового представления, вероятностного спайкового кодирования, специализированных импульсных нейронных сетей и ансамблевой агрегации решений. Предложенное математико-программное решение реализует полный цикл обработки сетевого объекта: формирование инженерного признакового пространства, нормализацию, rate coding, K-кратный стохастический инференс, soft voting, калибровку порога и формирование итогового решения.

Экспериментальная оценка показала, что использование ансамбля специализированных SNN-моделей в компактном 13-мерном признаковом пространстве обеспечивает устойчивое качество бинарной классификации, высокую полноту выявления атакующих сценариев и частичную устойчивость к смене домена данных. На основном датасете UNSW-NB15 получены F1 = 0,848 и Recall = 0,906, а кросс-датасетное тестирование на CIC-IDS-2017 и TON_IoT подтвердило применимость предложенного программно-алгоритмического подхода без дообучения модели.

Ключевым результатом является подтверждение того, что ансамблевая SNN-конфигурация может рассматриваться не только как модель обнаружения атак, но и как основа математико-программного обеспечения интеллектуальной подсистемы анализа сетевого трафика в информа-

ционно-телекоммуникационных системах. Дальнейшее развитие исследования связано с расширением сравнительного анализа программно-алгоритмических решений, уточнением ресурсных характеристик реализации и проверкой переносимости подхода на дополнительные классы сетевых сценариев.

Список литературы

1. Serban A., van der Blom K., Hoos H., Visser J. Software engineering practices for machine learning – Adoption, effects, and team assessment // Journal of Systems and Software. 2023. Vol. 209. Art. 111907. DOI: 10.1016/j.jss.2023.111907.

2. Berman D. S., Buczak A. L., Chavis J. S., Corbett C. L. A Survey of Deep Learning Methods for Cyber Security // Information. 2019. Vol. 10. Is. 4. Article 122. DOI: 10.3390/info10040122.

3. Tokar V. Integration of Intelligent Information Systems into the Architecture of National Economic Security within the Framework of European Digital Transformation. In Proceedings of the International Conference on Economics, Accounting and Finance (ICEAF 2025). Scientific Center of Innovative Research. 2025. DOI: 10.36690/ICEAF-2025-31.

4. Петросов Д. А., Пальчевский Е. В., Хасанов И. И., Свирина А. Г., Горохова Р. И., Никитин П. В., Корчагин С. А., Коровин Д. И., Беспалова Н. В., Абаев В. А., Косарев В. Е., Сердечный Д. В., Мисюков Г. И., Раздьяконов Е. С., Жолобов О. А. Анализ и применение интеллектуальных моделей и методов проактивной защиты и обнаружения кибератак на объекты критической информационной инфраструктуры финансового сектора: монография. М.: ООО «Русайнс», 2025. 234 с. EDN: DQALVT. ISBN 978-5-466-08528-0.

5. Mahdavifar S., Ghorbani A. A. Application of deep learning to cybersecurity: A survey // Neurocomputing. 2019. Vol. 347. P. 149–176. DOI: 10.1016/j.neucom.2019.02.056.

6. Карпухин А. И. Оценка уровня защищенности объектов критической инфраструктуры с использованием машинного обучения и семантического анализа текстового описания угроз и уязвимостей // Экономика строительства. 2025. № 6. С. 479–482. URL: https://econom-journal.ru/upload/iblock/929/wmu8lbymtrnh60jdvu06rg8ah6716b8m/№6%202025%20ЭС.pdf (дата обращения: 17.05.2026). EDN: KGSPPL.

7. Alom M. Z., Taha T. M. Network Intrusion Detection for Cyber Security Using Unsupervised Deep Learning Approaches // 2017 IEEE National Aerospace and Electronics Conference (NAECON). Dayton, OH, 2017. P. 63–69.DOI: 10.1109/NAECON.2017.8268746.

8. Neftci E. O., Mostafa H., Zenke F. Surrogate Gradient Learning in Spiking Neural Networks: Bringing the Power of Gradient-Based Optimization to Spiking Neural Networks // IEEE Signal Processing Magazine. 2019. Vol. 36. Is. 6. P. 51–63. DOI: 10.1109/MSP.2019.2931595.

9. Zhou S., Li X., Chen Y., Chandrasekaran S. T., Sanyal A. Temporal-coded deep spiking neural network with easy training and robust performance // Proceedings of the AAAI Conference on Artificial Intelligence. 2021. Vol. 35. Is. 12. P. 11143–11151. DOI: 10.1609/aaai.v35i12.17329.

10. Tavanaei A., Ghodrati M., Kheradpisheh S. R., Masquelier T., Maida A. Deep learning in spiking neural networks // Neural Networks. 2019. Vol. 111. P. 47–63. DOI: 10.1016/j.neunet.2018.12.002.

11. Roy K., Jaiswal A., Panda P. Towards spike-based machine intelligence with neuromorphic computing // Nature. 2019. Vol. 575. P. 607–617. DOI: 10.1038/s41586-019-1677-2.

12. Pfeiffer M., Pfeil T. Deep Learning With Spiking Neurons: Opportunities and Challenges // Frontiers in Neuroscience. 2018. Vol. 12. Art. 774. DOI: 10.3389/fnins.2018.00774.

13. Gundersen O. E., Shamsaliei S., Langseth H. On Reporting Robust and Trustworthy Conclusions from Model Comparison Studies Involving Neural Networks and Randomness // Proceedings of the 2023 ACM Conference on Reproducibility and Replicability (ACM REP '23). Santa Cruz, CA, USA. 2023. 25 p. DOI: 10.1145/3589806.3600044.

14. Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) // 2015 Military Communications and Information Systems Conference (MilCIS). Canberra. 2015. P. 1–6. DOI: 10.1109/MilCIS.2015.7348942.

15. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018). 2018. P. 108–116. DOI: 10.5220/0006639801080116.

16. Sharafaldin I., Lashkari A. H., Ghorbani A. A. A Detailed Analysis of the CICIDS2017 Data Set // Information Systems Security and Privacy. Communications in Computer and Information Science. 2019. P. 172–188. DOI: 10.1007/978-3-030-25109-3_9.

17. Moustafa N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets // Sustainable Cities and Society. 2021. Vol. 72. Art. 102994. DOI: 10.1016/j.scs.2021.102994.

18. Ayasi Bahgat, Cristóbal J. Carmona, Mohammed Saleh, Angel M. García-Vico. 2025. "A Practical Tutorial on Spiking Neural Networks: Comprehensive Review, Models, Experiments, Software Tools, and Implementation Guidelines" Eng 6. № 11: 304. DOI: 10.3390/eng6110304.

19. Пальчевский Е. В., Антонов В. В., Хасанов И. И., Суворова В. А. Разработка импульсной нейронной сети для количественной оценки защищенности объектов критической информационной инфраструктуры // Программная инженерия. 2026. Т. 17. № 1. С. 3–13. EDN: HLACFS. DOI: 10.17587/prin.17.3-13.

20. Хасанов И. И., Пальчевский Е. В., Стешникова А. Д., Сурова Н. Ю. Подходы к количественной оценке уровня защищенности объектов критической информационной инфраструктуры финансового сектора на основе машинного обучения // Экономика строительства. 2025. № 8. С. 466–468. URL: https://econom-journal.ru/upload/iblock/13a/o61euadw90lkme2w732yaznx0zezylor/№8 %202025 %20ЭС.pdf (дата обращения: 17.05.2026). EDN: OQYIZH.

21. Babu A., Abubeker K. M., Bushara A. R., Mathew M. P. A scalable MLOps-integrated intrusion detection framework using Bi-GRU and attention mechanisms with Kubeflow and KServe // Engineering Research Express. 2025. Vol. 7. Art. 035274. DOI: 10.1088/2631-8695/adfbd0.

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest: The authors declare that there is no conflict of interest.

Финансирование: Статья подготовлена по результатам исследований, проведенных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве Российской Федерации.

Financing: The article was prepared based on the results of research carried out at the expense of budgetary funds on the state assignment of the Financial University under the Government of the Russian Federation.