Оригинальная статья / Original article

УДК 004.056
http://doi.org/10.35854/1998-1627-2026-5-634-643

Интеллектуальная модель управления киберрисками в критической информационной инфраструктуре финансового сектора на основе импульсных нейронных сетей

Ильнур Ильдарович Хасанов[1]✉, Алексей Александрович Никифоров[2]

[1, 2] *Финансовый университет при Правительстве Российской Федерации, Москва, Россия*

[1] *iikhasanov@fa.ru, https://orcid.org/0000-0002-3422-1237*

[2] *aanikiforov@fa.ru, https://orcid.org/0009-0000-5180-7822*

Аннотация

Цель. Разработка модели управления киберрисками в критической информационной инфраструктуре финансового сектора, базирующейся на применении импульсных нейронных сетей и ориентированной на повышение обоснованности, оперативности принятия решений при выявлении аномалий сетевого трафика.

Задачи. Провести анализ существующих подходов к управлению инцидентами информационной безопасности в финансовых организациях; разработать структуру интеллектуальной системы поддержки принятия решений для выявления сетевых атак; определить информативные признаки сетевой активности и способы их представления в импульсной форме; выполнить экспериментальную оценку эффективности предложенного подхода в контуре управления безопасностью.

Методология. В процессе исследования применены методы машинного обучения и импульсных нейронных сетей. Обработка сетевых событий реализована с использованием различных архитектур SNN, включая сверточные и рекуррентные модели. Представление входных данных основано на преобразовании параметров сетевого трафика в импульсные последовательности с применением вероятностных и временных методов кодирования. Для оценки результатов использованы стандартные метрики классификации; дополнительно проанализирован вопрос о том, каким образом полученные значения влияют на качество принимаемых решений.

Результаты. Разработана структура интеллектуальной системы, которая может быть интегрирована в контур управления информационной безопасностью финансовой организации. В системе использованы специализированные модели импульсных нейронных сетей для анализа различных типов сетевых угроз. Эксперименты показали, что применение SNN повышает точность выявления атак и снижает количество ложных срабатываний. В результате уменьшается нагрузка на операторов и улучшается эффективность процессов реагирования.

Выводы. Полученные результаты свидетельствуют о целесообразности применения импульсных нейронных сетей при выполнении задач управления кибербезопасностью финансовых организаций. Разработанный подход может быть интегрирован в системы поддержки принятия решений, в которых он способствует повышению устойчивости критической информационной инфраструктуры и снижению последствий киберугроз.

Ключевые слова: *поддержка принятия решений, финансовый сектор, импульсные нейронные сети, информационная безопасность, анализ сетевого трафика, критическая информационная инфраструктура*

Для цитирования: Хасанов И. И., Никифоров А. А. Интеллектуальная модель управления киберрисками в критической информационной инфраструктуре финансового сектора на основе импульсных нейронных сетей // *Экономика и управление.* 2026. Т. 32. № 5. С. 634–643. http://doi.org/10.35854/1998-1627-2026-5-634-643

Благодарности: статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве Российской Федерации.

Intelligent cyberrisk management model for critical information infrastructure in the financial sector based on spiking neural networks

Ilnur I. Khasanov[1]✉, **Alexey A. Nikiforov**[2]

[1, 2] *Financial University under the Government of the Russian Federation, Moscow, Russia*

[1] *iikhasanov@fa.ru, https://orcid.org/0000-0002-3422-1237*

[2] *aanikiforov@fa.ru, https://orcid.org/0009-0000-5180-7822*

Abstract

Aim. This work aimed to develop a cyberrisk management model for the critical information infrastructure of the financial sector based on spiking neural networks (SNNs), focused on improving the validity and efficiency of decision-making when detecting network traffic anomalies.

Objectives. To analyze existing approaches to information security incident management in financial organizations; to develop the structure of an intelligent decision support system for detecting network attacks; to identify informative features of network activity and methods for their representation in spiking form; and to perform an experimental evaluation of the proposed approach's effectiveness within the security management loop.

Methods. The research applies machine learning methods and spiking neural networks. Network event processing is implemented using various SNN architectures, including convolutional and recurrent models. Input data representation is based on converting network traffic parameters into spike trains using probabilistic and temporal encoding methods. Standard classification metrics are used to evaluate the results; additionally, the analysis examines how the obtained values affect the quality of decisions made.

Results. The structure of an intelligent system is developed, which can be integrated into the information security management loop of a financial organization. The system uses specialized spiking neural network models to analyze different types of network threats. Experiments show that using SNNs increases attack detection accuracy and reduces the number of false positives. Consequently, operator workload is reduced, and the efficiency of response processes is improved.

Conclusion. The obtained results demonstrate the feasibility of using spiking neural networks for cybersecurity management tasks in financial organizations. The proposed approach can be integrated into decision support systems, where it helps increase the resilience of critical information infrastructure and mitigate the consequences of cyberthreats.

Keywords: *decision support, financial sector, spiking neural networks, information security, network traffic analysis, critical information infrastructure*

For citation: Khasanov I.I., Nikiforov A.A. Intelligent cyberrisk management model for critical information infrastructure in the financial sector based on spiking neural networks. *Ekonomika i upravlenie = Economics and Management.* 2026;32(5):634-643. (In Russ.). http://doi.org/10.35854/1998-1627-2026-5-634-643

Acknowledgments: This paper was prepared based on the results of research funded under the state assignment of the Financial University under the Government of the Russian Federation.

Введение

В условиях активной цифровизации экономики и широкого внедрения информационных технологий в финансовом секторе возрастает значение обеспечения безопасности информационных систем и сетевой инфраструктуры. Финансовые организации, включая банки, платежные системы и финтех-компании, функционируют как сложные организационно-технические системы, в которых надежность обработки данных

и устойчивость сетевой инфраструктуры напрямую связаны с качеством принимаемых управленческих решений. Нарушение функционирования критической информационной инфраструктуры (КИИ) может приводить к техническим сбоям и значительным экономическим потерям, снижению доверия клиентов и дестабилизации финансовых процессов.

В этих условиях задачи обеспечения кибербезопасности следует рассматривать не только как техническую проблему, но и как задачу управления, связанную со своевременным выявлением угроз, оценкой их значимости и выбором мер реагирования. Одним из ключевых элементов контура управления информационной безопасностью служат системы обнаружения вторжений (Intrusion Detection Systems, IDS). Они обеспечивают мониторинг сетевого трафика и формируют информацию, необходимую для принятия решений при реагировании на инциденты.

Современные IDS опираются на широкий спектр методов анализа сетевых событий, в том числе статистические, сигнатурные и интеллектуальные подходы. В течение последних лет активно развиваются методы машинного и глубокого обучения, позволяющие выявлять сложные закономерности в сетевых данных и тем самым повышать качество обнаружения атак [1; 2]. В частности, применение нейронных сетей делает возможным выявление нелинейных зависимостей и обнаружение ранее неизвестных типов угроз [3].

В ряде работ показано, что использование глубоких нейронных сетей, в том числе сверточных и рекуррентных архитектур, существенно повышает эффективность классификации сетевых атак [4; 5]. Такие модели способны учитывать сложные пространственно-временные зависимости в сетевом трафике, что особенно важно при анализе многоэтапных атак [6]. Вместе с тем их применение в практических системах управления информационной безопасностью связано с рядом ограничений. К ним относятся высокая вычислительная сложность, значительные требования к ресурсам, трудности при обработке потоковых данных в режиме реального времени [7].

Ввиду изложенного актуальной задачей остается поиск моделей, способных эффективнее работать с потоковыми данными и учитывать временную структуру сетевых событий. Одно из перспективных направлений — импульсные нейронные сети (Spiking Neural Networks, SNN), относящиеся к третьему поколению искусственных нейронных сетей. Их ключевая особенность состоит в использовании временных импульсов для передачи информации, что помогает естественным образом учитывать динамику входных сигналов [8].

Результаты современных исследований указывают на значительный потенциал применения импульсных нейронных сетей при выполнении задач информационной безопасности. Показано, что использование специализированных архитектур способствует повышению точности обнаружения атак и снижению количества ложных срабатываний [9]. Кроме того, применение ансамблей моделей и гибридных подходов повышает устойчивость систем к изменяющимся условиям функционирования сети [10].

Существенный вклад в развитие интеллектуальных методов обеспечения кибербезопасности вносят и отечественные исследования. В работах российских авторов рассмотрены вопросы применения методов искусственного интеллекта для анализа сетевых инцидентов и обеспечения защиты информационных систем [11]. Ученые исследуют также модели защиты систем обнаружения вторжений от атак на компоненты машинного обучения [12]. Отдельное внимание уделено анализу современных подходов к построению IDS и формулировке актуальных научных задач в этой области [13; 14; 15].

Несмотря на значительное количество исследований, большинство существующих решений ориентировано на разработку отдельных моделей обнаружения атак и их точностных характеристик. В меньшей степени раскрыты вопросы интеграции таких моделей в контур управления информационной безопасностью и их влияния на процессы принятия решений. В частности, применение импульсных нейронных сетей в составе комплексных систем управления безопасностью КИИ финансового сектора остается недостаточно изученным.

Таким образом, актуальной научной задачей служит разработка методов интеллектуального анализа сетевых событий, ориентированных на повышение точности обнаружения атак и улучшение качества управления кибербезопасностью за счет роста оперативности и обоснованности принимаемых решений. Цель исследования —

разработка модели поддержки принятия решений в системе управления кибербезопасностью КИИ финансового сектора на основе импульсных нейронных сетей и оценка эффективности ее применения при анализе сетевых событий.

Научная новизна заключается в разработке архитектуры интеллектуальной системы, интегрируемой в контур управления информационной безопасностью и основанной на использовании совокупности специализированных моделей импульсных нейронных сетей, ориентированных на анализ различных типов сетевых угроз. В отличие от существующих решений, предложенный подход предусматривает распределение функций обнаружения атак между несколькими моделями, что повышает надежность выявления угроз и снижает уровень ложных срабатываний, обеспечивая тем самым более эффективную поддержку процессов принятия решений.

Материалы и методы

В настоящем исследовании анализ сетевых событий рассмотрен как элемент информационного обеспечения процессов управления кибербезопасностью в финансовых организационных системах. В качестве исходных данных использован набор [16], содержащий записи сетевого трафика и различные типы сетевых атак. Этот набор широко применяют при изучении систем обнаружения вторжений, поскольку он включает в себя и нормальную сетевую активность, и различные категории атак, в том числе сканирование сети, атаки отказа в обслуживании и эксплуатацию уязвимостей.

Для создания информационной основы принятия решений использован набор признаков сетевой активности, отражающих параметры функционирования сетевой инфраструктуры и потенциальные отклонения от нормального поведения. В исследовании сформирован вектор признаков, включающий в себя 13 признаков, таких как количество переданных пакетов, активность нестандартных портов, количество аномальных фрагментов, попытки неуспешной аутентификации, признаки повышения привилегий и показатели задержек сетевых соединений.

Предварительная обработка данных направлена на обеспечение сопоставимости и устойчивости анализа в контуре управления. В частности, применена min–max нормализация признаков с приведением значений к диапазону [0; 1], что позволяет повысить стабильность функционирования моделей при обработке потоковых данных. Далее выборка разделена на обучающую (80 %) и тестовую (20 %).

В отличие от традиционных подходов, в настоящей работе находит отражение архитектура интеллектуальной подсистемы анализа, интегрируемой в контур управления информационной безопасностью. В качестве главного инструмента применены импульсные нейронные сети (SNN), помогающие учитывать временную структуру сетевых событий и обрабатывать данные в режиме, близком к реальному времени.

Подсистема предусматривает несколько специализированных моделей, каждая из которых ориентирована на выявление определенных типов сетевых угроз, как видно на рисунке 1. Такой подход дает возможность выполнить распределенную обработку событий и повысить надежность выявления атак в условиях высокой изменчивости сетевой среды.

В процессе исследования реализованы следующие архитектуры моделей:

- сверточная импульсная нейронная сеть (ConvSpikeNet), предназначенная для анализа пространственных зависимостей между признаками сетевого трафика;
- глубокая импульсная нейронная сеть с остаточными связями (DeepResidualSpikeNet), обеспечивающая устойчивое обучение глубоких SNN-моделей;
- модель AttentionSpikeNet, использующая механизм временного внимания (temporal self-attention) для анализа временных зависимостей между сетевыми событиями;
- рекуррентная импульсная нейронная сеть (RecurrentSpikeNet), предназначенная для анализа временных зависимостей в последовательностях сетевых событий;
- мультимасштабная архитектура (MultiScaleSpikeNet), обеспечивающая анализ сетевых данных на различных временных масштабах;
- импульсный автоэнкодер (AnomalySpikeAutoencoder), предназначенный для обнаружения аномального поведения в сетевом трафике.

Для представления входных данных в форме, пригодной для обработки в SNN, использованы методы spike-encoding, обеспечивающие преобразование числовых

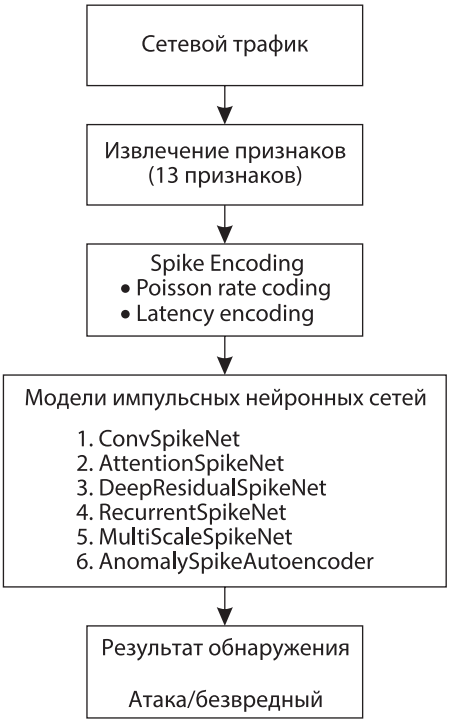

Рис. 1. Архитектура системы обнаружения сетевых атак на основе импульсных нейронных сетей
Fig. 1. Architecture of the network attack detection system based on spiking neural networks

Источник: составлено авторами.

значений признаков в последовательности временных импульсов. Применены вероятностное кодирование по распределению Пуассона и кодирование по времени возникновения импульса [17].

Обучение моделей осуществлено с помощью методов оптимизации параметров нейронных сетей, при использовании стохастического градиентного спуска и обратного распространения ошибки через временную динамику сети. В качестве функции потерь для задачи классификации применена Focal Loss, повышающая устойчивость обучения моделей при наличии несбалансированных классов сетевых событий [18].

С целью большей надежности функционирования подсистемы анализа в условиях реальной эксплуатации дополнительно использованы методы балансировки классов, регуляризации и ансамблирования архитектур. Реализация моделей выполнена посредством библиотеки PyTorch [19], а также специализированного инструментария snnTorch для построения импульсных нейронных сетей [20]. Для обработки и анализа данных использованы библиотеки NumPy и Pandas, предназначенные для выполнения численных вычислений и обработки табличных данных; при визуализации результатов экспериментов — библиотека Matplotlib, которая помогает строить графики и диаграммы, отражающие результаты обучения моделей [21].

Оценка эффективности разработанных моделей обнаружения атак проведена с помощью стандартных метрик классификации, широко применяемых при выполнении задач информационной безопасности. В частности, для анализа качества моделей использованы следующие показатели:

- точность классификации (Accuracy);
- точность предсказаний (Precision);
- полнота обнаружения атак (Recall);
- F1-мера;
- уровень ложных срабатываний (False Positive Rate).

Кроме того, для более полного анализа качества моделей применен коэффициент корреляции Мэттьюса (MCC), с помощью которого комплексно оценено качество классификации при несбалансированных данных.

Итак, предлагаемая методика обеспечивает формирование интеллектуальной подсистемы анализа сетевых событий, ориентированной на использование в контуре управления информационной безопасностью и повышение обоснованности принимаемых решений при выявлении кибератак.

Таблица 1

Сравнение эффективности моделей обнаружения атак

Table 1. Comparison of effectiveness of attack detection models

Архитектура	Precision	Recall	F1	FPR
ConvSpikeNet	0,54	0,49	0,51	0,09
DeepResidualSpikeNet	0,59	0,55	0,57	0,08
AttentionSpikeNet	0,61	0,56	0,58	0,07
RecurrentSpikeNet	0,66	0,63	0,64	0,05
MultiScaleSpikeNet	0,73	0,70	0,71	0,04
AnomalySpikeAutoencoder	0,42	0,37	0,39	0,20

Источник: составлено авторами.

Результаты и обсуждение

В процессе исследования выполнена экспериментальная оценка эффективности разработанной интеллектуальной подсистемы анализа сетевых событий, рассматриваемой как элемент контура управления кибербезопасностью финансовой организации. Эксперименты проведены с использованием набора данных [16], содержащего записи сетевого трафика и различные категории атак.

В рамках предложенного подхода реализован набор специализированных архитектур импульсных нейронных сетей, каждая из которых ориентирована на выявление определенных типов угроз. Такое распределение функций между моделями помогает формировать более детализированную информацию о состоянии сети и, соответственно, повышает обоснованность принимаемых решений в процессе реагирования на инциденты.

Для оценки эффективности использованы метрики классификации (Precision, Recall, F1, FPR), которые интерпретируются нами с точки зрения их влияния на качество управления безопасностью. Так, показатель Recall отражает способность системы выявлять реальные инциденты, а уровень ложных срабатываний (FPR) напрямую влияет на нагрузку среди операторов и эффективность процедур реагирования.

В таблице 1 представлены результаты оценки эффективности разработанных моделей импульсных нейронных сетей.

Анализ полученных данных дает возможность оценить вклад различных архитектур в повышение эффективности управления кибербезопасностью, как видно на рисунке 2.

Наиболее сбалансированные результаты показала архитектура MultiScaleSpikeNet (F1 = 0,71; FPR = 0,04). С точки зрения управления это выражено в повышении надежности выявления инцидентов при одновременном снижении количества ложных сигналов. В результате уменьшается избыточная нагрузка на персонал, повышается оперативность реагирования. Использование нескольких временных масштабов помогает выявлять краткосрочные аномалии и длительные аномальные процессы, что особенно видится важным при анализе сложных распределенных атак.

Архитектура RecurrentSpikeNet также показала высокие результаты (Recall = 0,63), что свидетельствует о ее способности выявлять последовательные зависимости в сетевых событиях. Это позволяет эффективнее обнаруживать атаки, развивающиеся во времени, и снижает вероятность пропуска инцидентов, что критично для систем с повышенными требованиями к надежности.

Модель AttentionSpikeNet (F1 = 0,58) обеспечивает выделение наиболее значимых фрагментов временных последовательностей. За счет этого растет уровень точности анализа, появляется возможность выбора приоритета событий, требующих первоочередного реагирования со стороны системы управления безопасностью.

Архитектура ConvSpikeNet (F1 = 0,51) демонстрирует более ограниченные возможности при учете длительных зависимостей, однако эффективно выявляет локальные аномалии. В составе комплексной системы такую модель целесообразно использовать как вспомогательный инструмент для анализа отдельных типов атак.

Наиболее низкие показатели получены для модели AnomalySpikeAutoencoder (F1 = 0,39; FPR = 0,20). Тем не менее ее применение может быть оправданным при решении задач предварительного выявления

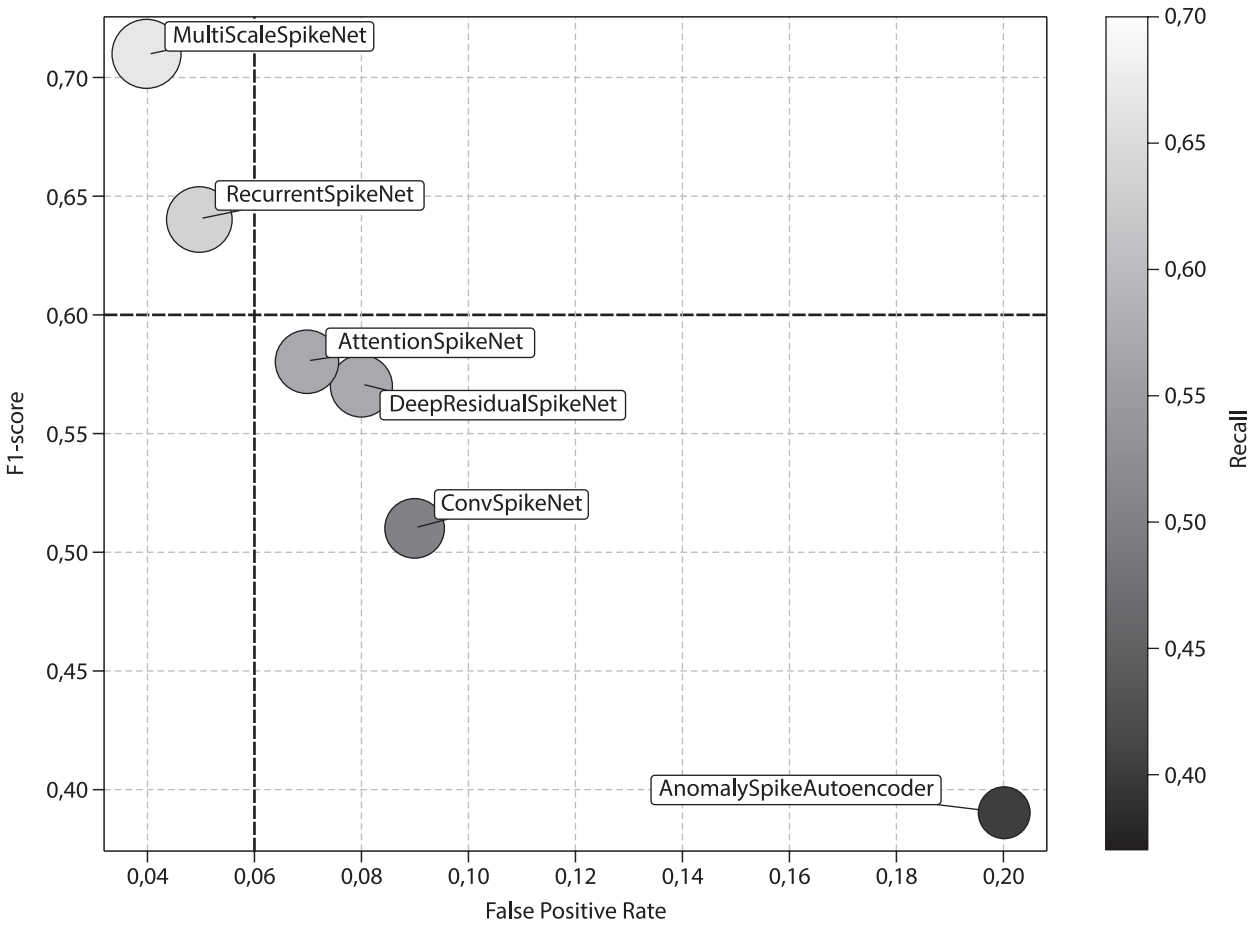

Рис. 2. Сравнение архитектур импульсных нейронных сетей по соотношению F1-меры и уровня ложных срабатываний

Fig. 2. Comparison of spiking neural network architectures by the F1-score to false positive rate ratio

Источник: составлено авторами.

нетипичного поведения. Вместе с тем высокий уровень ложных срабатываний ограничивает ее самостоятельное использование без дополнительных механизмов фильтрации.

В целом результаты экспериментов указывают на то, что использование набора специализированных моделей обеспечивает более устойчивую работу системы по сравнению с применением одной универсальной архитектуры. Это проявляется в повышении надежности выявления угроз, снижении неопределенности при анализе сетевых событий и улучшении качества принимаемых решений. Полученные результаты также подтверждают целесообразность применения импульсных нейронных сетей при обработке потоковых данных, что дает возможность использовать их в системах мониторинга, функционирующих в режиме, близком к реальному времени.

Таким образом, предложенный подход позволяет сформировать интеллектуальную подсистему анализа, повышающую эффективность процессов управления кибербезопасностью и обеспечивающую устойчивое функционирование КИИ финансового сектора.

Выводы

В статье предложена модель интеллектуальной поддержки управления кибербезопасностью КИИ финансового сектора, основанная на использовании специализированных архитектур импульсных нейронных сетей. Разработанный подход ориентирован на анализ сетевых событий с учетом их временной структуры, обеспечивает формирование информативных признаков для принятия решений при выявлении различных типов сетевых угроз.

Результаты проведенных экспериментов показали, что использование совокупности специализированных SNN-моделей повы-

шает надежность выявления атак и снижает уровень ложных срабатываний. С точки зрения управления находит отражение в уменьшении неопределенности при анализе сетевых событий, снижении нагрузки на персонал и повышении оперативности реагирования на инциденты. Наиболее эффективные результаты прослеживаются при использовании мультимасштабного подхода, обеспечивающего учет различных временных характеристик сетевой активности.

Практическая значимость работы заключается в возможности интеграции предложенного подхода в системы мониторинга и управления информационной безопасностью финансовых организаций. Применение разработанной модели способствует повышению устойчивости функционирования цифровой финансовой инфраструктуры и совершенствованию процессов управления киберрисками.

Дальнейшее развитие темы исследования может быть связано с расширением информационной базы анализа, адаптацией моделей к изменяющимся условиям функционирования сетевой среды, а также с разработкой адаптивных интеллектуальных систем, ориентированных на поддержку управленческих решений в режиме реального времени.

Список источников

1. *Rahman M., Al Shakil S., Mustakim M. R.* A survey on intrusion detection systems in IoT networks // Cyber Security and Applications. 2025. Vol. 3. Article 100082. https://doi.org/10.1016/j.csa.2024.100082
2. *Hozouri A., Mirzaei A., Effatparvar M.* A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges // Discover Artificial Intelligence. 2025. Vol. 5. No. 1. Article 314. https://doi.org/10.1007/s44163-025-00578-1
3. *Zhang Y., Muniyandi R. C., Qamar F.* A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance // Applied Sciences. 2025. Vol. 15. No. 3. Article 1552. https://doi.org/10.3390/app15031552
4. *Lampe B., Meng W.* A survey of deep learning-based intrusion detection in automotive applications // Expert Systems with Applications. 2023. Vol. 221. Article 119771. https://doi.org/10.1016/j.eswa.2023.119771
5. *Xu Z., Wu Y., Wang S. et al.* Deep learning-based intrusion detection systems: A survey // Journal of the ACM 2025. Vol. 1. No. 1. Article 1. https://doi.org/10.48550/arXiv.2504.07839
6. *Arnob A. K. B., Chowdhury R. R., Chaiti N. A., Saha S., Roy A.* A comprehensive systematic review of intrusion detection systems: Emerging techniques, challenges, and future research directions // Journal of Edge Computing. 2025. Vol. 4. No. 1. P. 73–104. https://doi.org/10.55056/jec.885
7. *Mohammed A. A. A.* Improving intrusion detection systems by using deep learning methods on time series data // Engineering, Technology and & Applied Science Research. 2025. Vol. 15. No. 1. P. 19267–19272. https://doi.org/10.48084/etasr.9417
8. *Shone N., Ngoc T. N., Phai V. D., Shi Q.* A deep learning approach to network intrusion detection // IEEE Transactions on Emerging Topics in Computational Intelligence. 2018. Vol. 2. No. 1. P. 41–50. https://doi.org/10.1109/TETCI.2017.2772792
9. *Tang T. A., Mhamdi L., McLernon D., Zaidi S. A., Ghogho M.* DeepIDS: Deep learning approach for intrusion detection in software defined networking // Electronics. 2020. Vol. 9. No. 9. Article 1533. https://doi.org/10.3390/electronics9091533
10. *Yin C., Zhu Y., Fei J., He X.* A deep learning approach for intrusion detection using recurrent neural networks // IEEE Access. 2017. Vol. 5. P. 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418
11. *Котенко И. В.* Искусственный интеллект для кибербезопасности: новая стадия противоборства в киберпространстве // Искусственный интеллект и принятие решений. 2024. № 1. С. 3–19. https://doi.org/10.14357/20718594240101
12. *Ичетовкин Е. А., Котенко И. В.* Модели и алгоритмы защиты систем обнаружения вторжений от атак на компоненты машинного обучения // Computational Nanotechnology. 2025. Т. 12. № 1. С. 17–25. https://doi.org/10.33693/2313-223X-2025-12-1-17-25
13. *Новикова Е. С., Федорченко Е. В., Котенко И. В., Холод И. И.* Аналитический обзор подходов к обнаружению вторжений, основанных на федеративном обучении: преимущества использования и открытые задачи // Информатика и автоматизация. 2023. Т. 22. № 5. С. 1034–1082. https://doi.org/10.15622/ia.22.5.4
14. *Труфанов В. Н., Огарок А. Л., Нестеров С. Г.* Исследование сетевых систем обнаружения вторжений, использующих методы машинного обучения // Информатизация и связь. 2023. № 4. С. 59–72. https://doi.org/10.34219/2078-8320-2023-14-4-59-72

15. *Ичетовкин Е. А.* Исследование устойчивости систем обнаружения вторжений с компонентами машинного обучения к состязательным атакам // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2025. № 2. С. 76–87. https://doi.org/10.24143/2072-9502-2025-2-76-87
16. *Moustafa N., Slay J.* UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) // Military communications and information systems conf. (MilCIS). (Canberra, November 10-12, 2015). New York, NY: IEEE, 2015. P. 1–6. https://doi.org/10.1109/MilCIS.2015.7348942
17. *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. https://doi.org/10.1016/j.neunet.2018.12.002
18. *Lin T.-Y., Goyal P., Girshick R., He K., Dollár P.* Focal loss for dense object detection // Proc. of the IEEE Int. conf. on computer vision (ICCV). (Venice, October 22–29, 2017). New York, NY: IEEE, 2017. P. 2980–2988. https://doi.org/10.1109/ICCV.2017.324
19. *Paszke A., Gross S., Massa F. et al.* PyTorch: An imperative style, high-performance deep learning library // Proc. 33rd Int. conf. on neural information processing systems (NeurIPS 2019). (Vancouver, BC, December 8–14, 2019). New York, NY: ACM, 2019. P. 8024–8035. URL: https://proceedings.neurips.cc/paper_files/paper/2019/file/bdbca288fee7f92f2bfa9f7012727740-Paper.pdf (дата обращения: 15.04.2026).
20. *Eshraghian J. K., Ward M., Neftci E. O. et al.* Training spiking neural networks using lessons from deep learning // Proceedings of the IEEE. 2023. Vol. 111. No. 9. P. 1016–1054. https://doi.org/10.1109/JPROC.2023.3308088
21. *McKinney W.* Data structures for statistical computing in Python // Proc. of the 9th Python in science conf. (SciPy 2010). (Austin, TX, June 28 – July 03, 2010). Austin, TX: SciPy, 2010. P. 51–56. https://doi.org/10.25080/Majora-92bf1922-00a

References

1. Rahman M., Al Shakil S., Mustakim M.R. A survey on intrusion detection systems in IoT networks. *Cyber Security and Applications*. 2025;3:100082. https://doi.org/10.1016/j.csa.2024.100082
2. Hozouri A., Mirzaei A., Effatparvar M. A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. *Discover Artificial Intelligence*. 2025;5(1):314. https://doi.org/10.1007/s44163-025-00578-1
3. Zhang Y., Muniyandi R. C., Qamar F. A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance. *Applied Sciences*. 2025;15(3):1552. https://doi.org/10.3390/app15031552
4. Lampe B., Meng W. A survey of deep learning-based intrusion detection in automotive applications. *Expert Systems with Applications*. 2023;221:119771. https://doi.org/10.1016/j.eswa.2023.119771
5. Xu Z., Wu Y., Wang S., et al. Deep learning-based intrusion detection systems: A survey. *Journal of the ACM*. 2025;1(1):1. https://doi.org/10.48550/arXiv.2504.07839
6. Arnob A.K.B., Chowdhury R.R., Chaiti N.A., Saha S., Roy A.A Comprehensive systematic review of intrusion detection systems: Emerging techniques, challenges, and future research directions. *Journal of Edge Computing*. 2025;4(1):73-104. https://doi.org/10.55056/jec.885
7. Mohammed A.A.A. Improving intrusion detection systems by using deep learning methods on time series data. *Engineering, Technology & Applied Science Research*. 2025;15(1):19267-19272. https://doi.org/10.48084/etasr.9417
8. Shone N., Ngoc T.N., Phai V.D., Shi Q. A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*. 2018;2(1):41-50. https://doi.org/10.1109/TETCI.2017.2772792
9. Tang T.A., Mhamdi L., McLernon D., Zaidi S.A., Ghogho M. DeepIDS: Deep learning approach for intrusion detection in software defined networking. *Electronics*. 2020;9(9):1533. https://doi.org/10.3390/electronics9091533
10. Yin C., Zhu Y., Fei J., He X. A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*. 2017;5:21954-21961. https://doi.org/10.1109/ACCESS.2017.2762418
11. Kotenko I.V. Artificial intelligence for cyber security: A new stage of confrontation in cyberspace. *Iskusstvennyi intellekt i prinyatie reshenii = Artificial Intelligence and Decision Making*. 2024;(1):3-19. (in Russ.).
12. Ichetovkin E.A., Kotenko I.V. Models and algorithms for protecting intrusion detection systems from attacks on machine learning components. *Computational Nanotechnology*. 2025;12(1):17-25. (In Russ.). https://doi.org/10.33693/2313-223X-2025-12-1-17-25
13. Novikova E.S., Fedorchenko E.V., Kotenko I.V., Kholod I.I. Analytical review of intelligent intrusion detection systems based on federated learning: Advantages and open challenges. *Informatika i avtomatizatsiya = Informatics and Automation*. 2023;22(5):1034-1082. (In Russ.). https://doi.org/10.15622/ia.22.5.4

14. Trufanov V.N., Ogarok A.L., Nesterov S.G. A research on network intrusion detection systems using machine learning techniques. *Informatizatsiya i svyaz' = Informatization and Communication.* 2023;(4):59-72. https://doi.org/10.34219/2078-8320-2023-14-4-59-72
15. Ichetovkin E.A. Investigating the resistance of intrusion detection systems with machine learning components to adversarial attacks. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika = Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics.* 2025;(2):76-87. (In Russ.). https://doi.org/10.24143/2072-9502-2025-2-76-87
16. Moustafa N., Slay J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: Military communications and information systems conf. (MilCIS). (Canberra, November 10-12, 2015). New York, NY: IEEE; 2015:1-6. https://doi.org/10.1109/MilCIS.2015.7348942
17. Tavanaei A., Ghodrati M., Kheradpisheh S.R., Masquelier T., Maida A. Deep learning in spiking neural networks. *Neural Networks*. 2019;111:47-63. https://doi.org/10.1016/j.neunet.2018.12.002
18. Lin T.-Y., Goyal P., Girshick R., He K., Dollár P. Focal loss for dense object detection. In: Proc. IEEE Int. conf. on computer vision (ICCV). (Venice, October 22-29, 2017). New York, NY: IEEE; 2017:2980-2988. https://doi.org/10.1109/ICCV.2017.324
19. Paszke A., Gross S., Massa F., et al. PyTorch: An imperative style, high-performance deep learning library. In: Proc. 33rd Int. conf. on neural information processing systems (NeurIPS 2019). (Vancouver, BC, December 8-14, 2019). New York, NY: ACM; 2019:8024-8035. URL: https://proceedings.neurips.cc/paper_files/paper/2019/file/bdbca288fee7f92f2bfa9f7012727740-Paper.pdf (accessed on 15.04.2026).
20. Eshraghian J.K., Ward M., Neftci E.O., et al. Training spiking neural networks using lessons from deep learning. *Proceedings of the IEEE*. 2023;111(9):1016-1054. https://doi.org/10.1109/JPROC.2023.3308088
21. McKinney W. Data structures for statistical computing in Python. In: Proc. 9th Python in science conf. (SciPy 2010). (Austin, TX, June 28 – July 03, 2010). Austin, TX: SciPy; 2010:51-56. https://doi.org/10.25080/Majora-92bf1922-00a

Информация об авторах

Ильнур Ильдарович Хасанов

кандидат технических наук, доцент,
доцент кафедры информационных технологий,
старший научный сотрудник Института цифровых финансов

Финансовый университет
при Правительстве Российской Федерации

125167, Москва, Ленинградский пр., д. 49/2

SPIN-код: 7233-2018

Алексей Александрович Никифоров

младший научный сотрудник
Института цифровых финансов

Финансовый университет
при Правительстве Российской Федерации

125167, Москва, Ленинградский пр., д. 49/2

Поступила в редакцию 18.03.2026
Прошла рецензирование 10.04.2026
Подписана в печать 27.05.2026

Information about the authors

Ilnur I. Khasanov

PhD in Technical Sciences, Associate Professor,
Associate Professor at the Information Technology Department, senior research fellow at the Institute of Digital Finance

Financial University
under the Government of the Russian Federation

49/2 Leningradskiy Ave., Moscow 125167, Russia

SPIN: 7233-2018

Alexey A. Nikiforov

junior research fellow at the Institute of Digital Finance

Financial University
under the Government of the Russian Federation

49/2 Leningradskiy Ave., Moscow 125167, Russia

Received 18.03.2026
Revised 10.04.2026
Accepted 27.05.2026

Конфликт интересов: авторы декларируют отсутствие конфликта интересов, связанных с публикацией данной статьи.

Conflict of interest: the authors declare no conflict of interest related to the publication of this article.