УДК 004.056.5

Пономарчук Юлия Викторовна, кандидат физ.-мат. наук, доцент кафедры цифровая индустрия и защита информации, Дальневосточный государственный университет путей сообщения, г. Хабаровск

Мамедова Эмилия Алевтиновна, магистрант, Дальневосточный государственный университет путей сообщения, г. Хабаровск

НЕЙРОСЕТЕВЫЕ МЕТОДЫ ПРОГНОЗИРОВАНИЯ ПОСЛЕДСТВИЙ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ НА СЛОЖНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Аннотация

Статья посвящена исследованию нейросетевых методов прогнозирования последствий деструктивных воздействий на сложные информационные системы. Анализируются проблемы, связанные с моделированием поведения сложных гетерогенных систем в условиях неопределенности. Рассматриваются архитектуры искусственных нейронных сетей, наиболее применимые для задач прогнозирования, включая многослойные перцептроны, рекуррентные сети и LSTM-модели. Особое внимание уделяется ансамблевым нейросетевым моделям, повышающим надежность прогноза за счет интеграции нескольких классификаторов. Исследуются практические аспекты построения прогностических моделей - от подготовки обучающих выборок до верификации результатов. Доказывается эффективность нейросетевых методов для прогнозирования развития аварийных сценариев и оценки рисков в корпоративных информационных системах.

Annotation

The article focuses on investigating neural network methods for forecasting consequences of destructive impacts on complex information systems. The analysis covers challenges related to modeling behavior of complex heterogeneous systems under uncertainty conditions. The study examines artificial neural network architectures most applicable for forecasting tasks, including multilayer perceptrons, recurrent networks and LSTM models. Special attention is paid to ensemble neural models that enhance forecast reliability through integration of multiple classifiers. Practical aspects of building predictive models - from training data preparation to results verification - are thoroughly investigated. The effectiveness of neural network methods for predicting emergency scenarios development and risk assessment in corporate information systems is substantiated.

Ключевые слова: нейросетевые методы, прогнозирование последствий, деструктивные воздействия, сложные информационные системы, искусственные нейронные сети, LSTM-сети, ансамблевые модели, многослойный перцептрон, киберфизические системы, верификация моделей.
Keywords: neural network methods, consequence forecasting, destructive impacts, complex information systems, artificial neural networks, LSTM networks, ensemble models, multilayer perceptron, cyber-physical systems, model verification.

Колоссальный рост сложности современных информационных систем, характеризующихся иерархической структурой и гетерогенностью компонентов, порождает существенные неопределенности в их функционировании [5]. Наличие этих неопределенностей делает точное аналитическое описание поведения системы крайне затруднительным, а прямое математическое моделирование зачастую неприменимым на практике. Одновременно с этим наблюдается постоянное наличие деструктивных воздействий на информационные инфраструктуры. К их числу относятся кибератаки, программные сбои и физические аварии. Каждое из этих воздействий обладает потенциалом для резкого изменения состояния системы.

Актуальность прогнозирования возможных последствий подобных воздействий напрямую связана с задачей заблаговременного планирования защитных и восстановительных мероприятий для сложных информационных комплексов.

В качестве одного из наиболее перспективных инструментов для решения задач прогнозирования выступают искусственные нейронные сети. Данные модели зарекомендовали себя как мощные универсальные аппроксиматоры нелинейных функций. После завершения процедуры обучения искусственная нейронная сеть способна восстанавливать сложные зависимости между параметрами системы на основе предоставленных временных рядов. Способность к обобщению обучающих примеров позволяет конструировать прогностические системы, которые по имеющейся последовательности значений оценивают будущие состояния объекта. Эффективность нейросетевой аппроксимации эмпирических данных находится на уровне, сопоставимом с возможностями нечетких и нейро-нечетких моделей. При условии корректной настройки параметров сети формирование прогноза может осуществляться практически мгновенно, что имеет фундаментальное значение для систем управления.

Ряд научных работ демонстрирует практическое применение искусственных нейронных сетей в системах прогнозирования событий информационной безопасности. В частности, разработана технология применения нейронной сети для предсказания инцидентов информационной безопасности на уровне предприятия [2]. Для повышения точности классификации угроз применяются ансамблевые нейросетевые модели, объединяющие несколько частных классификаторов. Предлагаемые методики включают адаптивный отбор наиболее компетентных моделей и процедуры голосования по их выходным сигналам. Данный подход позволяет нивелировать ошибки отдельных сетей и повышать общую надежность итогового прогноза. Проведенные численные эксперименты подтверждают, что комплексные нейросетевые ансамбли демонстрируют высокую

эффективность при решении задач детектирования угроз и классификации событий безопасности в корпоративных информационных системах [1].

Процедура построения нейросетевой модели прогноза инициируется с этапа подготовки обучающей выборки. Необходимо осуществить отбор набора входных переменных, адекватно описывающих состояние системы и параметры внешних воздействий, с последующей их нормировкой для обеспечения корректности обучения. В обучающую выборку включаются исключительно признаки, оказывающие существенное влияние на прогнозируемую величину, что позволяет снизить размерность решаемой задачи и улучшить общее качество модели. Для описания динамики технической системы могут привлекаться данные о нагрузках, температурных режимах, скорости потоков информации, тогда как нерелевантные показатели подлежат исключению.

Важным этапом является выбор архитектуры искусственной нейронной сети. На практике широкое применение находят многослойные перцептроны, способные моделировать сложные нелинейные зависимости. Также используются сети адаптивного резонанса и самоорганизующиеся карты Кохонена. Для работы с временными рядами применяются рекуррентные нейронные сети, включая архитектуры с длинной кратковременной памятью. Сети LSTM доказали высокую эффективность при анализе последовательностей и моделировании долговременных зависимостей в исходных данных. В контексте киберфизических систем рекомендуется применение LSTM-сетей для выявления аномалий и неожиданных сбоев в компонентах системы [6]. После выбора архитектуры проводится обучение сети с учителем на исторических данных с последующим тестированием на контрольной выборке. Верификация модели выполняется на данных, не участвовавших в обучении, что позволяет объективно оценить ее прогностическую способность.

Нейросетевые подходы находят успешное применение в прогнозировании последствий деструктивных воздействий в различных

прикладных областях. Кобяков и Мельников разработали численный метод, основанный на интеграции искусственной нейронной сети и метода анализа иерархий, для оценки уровня опасности вредоносных программ. В рамках исследования были выделены связанные поведенческие паттерны вредоносных утилит и построена прямая нейронная сеть с параметрами, обеспечивающими требуемую точность оценок [3]. Полученная модель была модифицирована с учетом зависимостей между признаками, а ее верификация на экспертных данных показала непротиворечивость результатов.

В другом исследовании искусственная нейронная сеть была использована для прогнозирования состояния технических систем в условиях аварийных ситуаций. Продемонстрировано, что многослойный перцептрон позволяет описать изменение состояния объекта при возникновении непредвиденных ограничений и на основе обучающей выборки выдать оценку критического параметра в следующий момент времени [4]. Формирование прогностических оценок может осуществляться в режиме реального времени. Разработанная сетевая архитектура использует входные данные за несколько предыдущих временных шагов для прогнозирования значений на будущий период. Практический эксперимент и численное тестирование подтверждают, что нейросетевой подход адекватно моделирует развитие аварийных сценариев и предсказывает ключевые показатели состояния системы.

Нейросетевые методы представляют собой эффективный инструментарий для прогнозирования последствий деструктивных воздействий на сложные информационные системы. Искусственные нейронные сети позволяют моделировать комплексные нелинейные зависимости между эндогенными параметрами системы и экзогенными факторами воздействия. Данные модели эффективно обобщают исторические данные и обеспечивают корректный прогноз в условиях экстремальных ситуаций. Развитие архитектур глубокого обучения и их гибридизация с другими аналитическими методами формируют перспективные направления для дальнейших научных изысканий. Интеграция нейросетевых компонентов

в системы предупреждения и управления рисками способствует повышению адаптивности и точности прогноза. Реализация этого подхода в конечном счете усиливает устойчивость критических информационных инфраструктур к потенциальным деструктивным воздействиям.

Список литературы

1. Бабаш А.В., Микрюков А.А., Сизов В.А. Классификация событий в системах обеспечения информационной безопасности на основе нейросетевых технологий // Открытое образование. 2019. № 23(1). С. 57–63.

2. Катасёв А.С., Катасёва Д.В., Кирпичников А.П. Нейросетевое прогнозирование инцидентов информационной безопасности предприятия // Вестник Казанского технологического университета. 2015. Т. 18. № 9. С. 215-218.

3. Кобяков Н.С., Мельников А.В. Численный метод модификации моделей, разработанных на основе метода анализа иерархий, с использованием искусственной нейронной сети // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2024. № 4.

4. Ковзель А.А. Прогнозирование последствий чрезвычайных ситуаций с применением нейросетевых технологий // Научный Лидер. 2021. № 11 (13). URL: https://scilead.ru/article/183-prognozirovanie-posledstvij-chrezvichajnikh-si (дата обращения: 10.11.2025).

5. Рей А.С., Калашников А.О. Комплексная оценка информационных рисков. i: краткий обзор подходов и методов: Complex information risks assessment. i: a brief overview of approaches and methods // [Электронный ресурс]. 2024. July. DOI: 10.25728/ubs.2024.110.3. URL: https://www.researchgate.net/publication/385392025_Kompleksnaa_ocenka_informacionnyh_riskov_i_kratkij_obzor_podhodov_i_metodov_Complex_information_risks_assessment_i_a_brief_overview_of_approaches_and_methods (дата обращения: 10.11.2025).

6. Сметанина О.Н., Сазонова Е.Ю., Андрушко Д.Ю. Программно-аппаратный комплекс для оценки надежности с использованием искусственного интеллекта // Современные наукоемкие технологии. 2020. № 7. С. 90-97. URL: https://top-technologies.ru/ru/article/view?id=38140 (дата обращения: 10.11.2025).

References

1. Babash A.V., Mikryukov A.A., Sizov V.A. Classification of events in information security systems based on neural network technologies // Open Education. 2019. No. 23(1). P. 57–63.

2. Katasiev A.S., Kataseva D.V., Kirpichnikov A.P. Neural network forecasting of enterprise information security incidents // Bulletin of Kazan Technological University. 2015. Vol. 18. No. 9. P. 215-218.

3. Kobyakov N.S., Melnikov A.V. Numerical method for modifying models developed based on the analytic hierarchy process using an artificial neural network // Bulletin of Voronezh State University. Series: System Analysis and Information Technologies. 2024. No. 4.

4. Kovzel A.A. Forecasting the consequences of emergency situations using neural network technologies // Scientific Leader. 2021. No. 11 (13). URL: https://scilead.ru/article/183-prognozirovanie-posledstvij-chrezvichajnikh-si (accessed: 10.11.2025).

5. Rey A.S., Kalashnikov A.O. Comprehensive assessment of information risks. i: a brief overview of approaches and methods: Complex information risks assessment. i: a brief overview of approaches and methods [Electronic resource]. 2024. July. DOI: 10.25728/ubs.2024.110.3. URL: https://www.researchgate.net/publication/385392025_Kompleksnaa_ocenka_informacionnyh_riskov_i_kratkij_obzor_podhodov_i_metodov_Complex_information_risks_assessment_i_a_brief_overview_of_approaches_and_methods (accessed: 10.11.2025).

6. Smetanina O.N., Sazonova E.Yu., Andrushko D.Yu. Software and hardware complex for reliability assessment using artificial intelligence // Modern High-Tech

Technologies. 2020. No. 7. P. 90-97. URL: https://top-technologies.ru/ru/article/view?id=38140 (accessed: 10.11.2025).