DOI: 10.58168/CISMP2024_118-121
УДК 004.9

АНАЛИЗ ВРЕМЕННЫХ РЯДОВ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКОЙ ЛОГИКИ ДЛЯ ПРОГНОЗИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ

Р.В. Дорошенко[1], А.В. Прокофьев[1], К.В. Стародубов[2]

[1] ООО «Региональные системы комплексной безопасности»
[2] ФГБОУ ВО «МИРЭА - Российский технологический университет»

Аннотация. В статье рассматриваются подходы к выявлению аномалий в системах информационной безопасности с использованием нечеткой логики для анализа временных рядов. Аномалии могут сигнализировать о сбоях или угрозах безопасности, и для их эффективного обнаружения необходимо гибкое описание нормального поведения системы, позволяющее учитывать допустимые отклонения. Нечеткая логика адаптирует модели к изменениям в поведении системы и помогает выявлять сложные аномалии, которые традиционные методы могут пропустить. Статья также обсуждает важность прогнозирования угроз на основе исторических данных, моделирования тенденций и динамической адаптации систем. Рассматриваются гибридные подходы, включая нейро-нечеткие системы и комбинации с машинным обучением. Особое внимание уделяется вызовам, связанным с настройкой моделей, обработкой больших данных и объяснением решений.

Ключевые слова: нечеткая логик, временные ряды, обнаружение аномалий, информационная безопасность, прогнозирование угроз.

TIME SERIES ANALYSIS WITH FUZZY LOGIC FOR THREAT PREDICTION IN INFORMATION SECURITY

R.V. Doroshenko[1], A.V. Prokofyev[1], K.V. Starodubov[2]

[1]LLC "Regional Systems of Comprehensive Security"
[2]Federal State Budgetary Educational Institution of Higher Education "MIREA - Russian Technological University"

Abstract. The article discusses approaches to anomaly detection in information security systems using fuzzy logic for time series analysis. Anomalies can signal system failures or security threats, and effective detection requires a flexible description of normal system behavior that accounts for permissible deviations. Fuzzy logic adapts models to changes in system behavior and helps identify complex anomalies that traditional methods may miss. The article also emphasizes the importance of threat prediction based on historical data, trend modeling, and dynamic system adaptation. Hybrid approaches are considered, including neuro-fuzzy systems and combinations with machine learning. Special attention is given to challenges related to model tuning, big data processing, and explaining decision-making processes.

Keywords: fuzzy logic, time series, anomaly detection, information security, threat prediction.

Обнаружение аномалий – одна из ключевых задач в анализе временных рядов для обеспечения информационной безопасности. Аномалии могут сигнализировать о различных деструктивных воздействий или нарушения в работе системы [1].

Использование нечетких правил для описания нормального поведения: Временные ряды часто характеризуются сложной структурой данных, где нормальное поведение системы может включать в себя множество допустимых отклонений. Нечеткие правила позволяют описывать это поведение гибко, без жестких границ, что помогает лучше учитывать вариативность данных.

Адаптация к изменениям в поведении системы: Системы информационной безопасности должны адаптироваться к изменениям, которые могут происходить в нормальной работе. Например, сезонные колебания или изменения в поведении пользователей могут влиять на временные ряды. Нечеткая логика позволяет системе учитывать эти изменения и адаптировать свои модели для поддержания высокой точности обнаружения аномалий.

Выявление сложных аномалий: Некоторые виды аномалий могут быть неочевидными и проявляться через комбинацию небольших отклонений в нескольких временных рядах [2]. Нечеткая логика помогает интегрировать информацию из различных источников и выявлять сложные, мультифакторные аномалии, которые могли бы остаться незамеченными при использовании традиционных методов анализа.

Прогнозирование угроз – важный аспект проактивного обеспечения безопасности. С использованием временных рядов и нечеткой логики можно создавать модели, которые предсказывают возможные инциденты на основе исторических данных [3].

Моделирование тенденций и аномалий: Нечеткая логика позволяет моделировать тенденции во временных рядах, учитывая неопределенность и возможные шумы. Это особенно важно для прогнозирования, так как модели могут учитывать различные сценарии развития событий, основываясь на предыдущем опыте и текущих данных.

Предсказание вероятности угрозы: Нечеткие модели могут использоваться для предсказания вероятности возникновения угрозы на основе текущего состояния временных рядов. Например, если определенные параметры начинают показывать отклонения, система может использовать нечеткие правила для оценки вероятности, что эти отклонения приведут к инциденту безопасности [4].

Динамическая адаптация моделей: Прогнозирующие модели, основанные на нечеткой логике, могут динамически адаптироваться к изменяющимся условиям. Это позволяет системе оставаться эффективной даже при изменении характера временных рядов, например, при переходе на новые типы данных или при изменении профилей угроз.

Для достижения максимальной эффективности анализа временных рядов в системах информационной безопасности нечеткая логика может быть

интегрирована с другими методами, такими как машинное обучение, статистический анализ и глубокое обучение [4].

Нейро-нечеткие системы: Комбинация искусственных нейронных сетей и нечеткой логики (нейро-нечеткие системы) позволяет создавать модели, которые могут обучаться на данных и одновременно учитывать неопределенности. [5] Эти системы могут использоваться для более точного обнаружения аномалий и прогнозирования угроз, сочетая преимущества глубокого обучения и гибкость нечеткой логики.

Фуззификация временных рядов: Нечеткая логика может использоваться для предварительной обработки временных рядов, так называемой "фуззификации", где данные преобразуются в нечеткие множества. Это позволяет моделям лучше справляться с шумами и неопределенностью, а также улучшает их способность выявлять скрытые паттерны в данных.

Гибридные методы анализа: В некоторых случаях наиболее эффективным подходом является использование гибридных методов, которые объединяют нечеткую логику с традиционными статистическими методами или алгоритмами машинного обучения. Такие подходы могут быть особенно полезны для анализа больших объемов данных и повышения точности в условиях высоких требований к безопасности [6].

Применение нечеткой логики в анализе временных рядов для обеспечения информационной безопасности сталкивается с рядом вызовов, но также открывает перспективы для дальнейшего развития:

Сложность настройки и оптимизации: Разработка и настройка нечетких моделей требует глубоких знаний в области математического моделирования и специфики данных. Оптимизация таких моделей для работы в реальном времени остается технически сложной задачей.

Эффективность в условиях больших данных: Временные ряды, генерируемые современными системами, могут достигать огромных объемов данных. Применение нечеткой логики в таких условиях требует разработки эффективных алгоритмов, способных обрабатывать большие объемы данных с высокой скоростью.

Интерпретация результатов: Объяснимость решений, принимаемых на основе нечеткой логики, остается важным аспектом. Необходимо разрабатывать методы, которые позволят операторам информационной безопасности понимать логику работы системы и причины, по которым та или иная активность была классифицирована как угроза.

Интеграция с новыми технологиями: С развитием новых технологий, таких как искусственный интеллект и квантовые вычисления, появятся новые возможности для интеграции нечеткой логики с более продвинутыми методами анализа данных. Это позволит создавать еще более мощные и адаптивные системы обеспечения информационной безопасности.

Выводы

Нечеткая логика представляет собой мощный инструмент для анализа временных рядов в системах обеспечения информационной безопасности,

предлагая гибкость и адаптивность в условиях неопределенности и сложных данных. Развитие этой области будет способствовать созданию более надежных и интеллектуальных систем, способных эффективно защищать информационные ресурсы в условиях постоянно меняющихся угроз.

Искусственные нейронные сети (ИНС) и нечеткая логика могут быть тесно интегрированы для решения задач анализа временных рядов в системах обеспечения информационной безопасности. Эти две технологии обладают различными, но взаимодополняющими свойствами, что делает их совместное использование особенно эффективным в условиях сложных, нелинейных и неопределенных данных.

Список литературы

1. Бабушкина И. А., Котельников,А. А. Нечеткая логика и ее применение в системах обработки данных // Научные труды. Серия "Информатика". – 2021. – Т. 12. – С. 34-45.

2. Дьяков, А. В., Семенов, П. И. Методы анализа временных рядов для мониторинга информационной безопасности // Вестник информационной безопасности. – 2022. – № 4. – С. 56-62.

3. Кузнецов, С. Н. Прогнозирование угроз на основе анализа временных рядов и нечеткой логики // Технологии безопасности информации. – 2023. – Т. 8. – С. 78-90.

4. Петрова, Е. А., Васильев, Р. М. Гибридные методы анализа больших данных для обеспечения безопасности // Журнал компьютерных наук и информационных технологий. – 2020. – № 6. – С. 12-22.

References

1, Babushkina, I. A., Kotelnikov, A. A. Nechyetkaya logika i yeё primeneniye v sistemakh obrabotki dannykh // Nauchnyye trudy. Seriya "Informatika". – 2021. – T. 12. – S. 34-45.

2. D'yakov, A. V., Semenov, P. I. Metody analiza vremennykh ryadov dlya monitoringa informatsionnoy bezopasnosti // Vestnik informatsionnoy bezopasnosti. – 2022. – № 4. – S. 56-62.

3. Kuznetsov, S. N. Prognozirovaniye ugroz na osnove analiza vremennykh ryadov i nechetkoy logiki // Tekhnologii bezopasnosti informatsii. – 2023. – T. 8. – S. 78-90.

4. Petrova, E. A., Vasilyev, R. M. Gibridnyye metody analiza bol'shikh dannykh dlya obespecheniya bezopasnosti // Zhurnal komp'yuternykh nauk i informatsionnykh tekhnologiy. – 2020. – № 6. – S. 12-22.