DOI: 10.37791/2687-0649-2023-18-5-77-90

Метод двухэтапной нечеткой кластеризации инцидентов кибербезопасности для субъектов экономической деятельности

В.А. Сизов[1]***, А.Д. Киров***[1*]
[1]*Российский экономический университет им. Г. В. Плеханова, Москва, Россия*
[*]*Kirov.AD@rea.ru*

Аннотация. Работа направлена на повышение эффективности управления кибербезопасностью (КБ) субъектов экономической деятельности (СЭД) за счет организации эффективного мониторинга КБ, учитывающего такие особенности его процесса, как неоднородность источников исходных данных мониторинга КБ, их представление в разных форматах, их неточность, во многом неопределенность и зашумленность, а также большое количество событий КБ, обрабатываемых неоднородными компонентами системы мониторинга КБ СЭД. В данной работе, в отличие от существующих методов, предлагается комплексный двухэтапный метод нечеткой кластеризации событий КБ, учитывающий оценки критичности событий КБ и функциональные возможности системы мониторинга КБ СЭД. На первом этапе используется модель кластеризации событий КБ на основе метода нечетких с-средних. Эта модель позволяет разбить множество событий КБ на несколько нечетких кластеров по критерию априорной вероятности того, что событие КБ является инцидентом. На втором этапе для уточнения результатов кластеризации событий КБ, полученных на первом этапе, используется модель кластеризации инцидентов КБ на основе метода выделения α-ядер нечетких кластеров. Эта модель позволяет выбирать вручную пороги степеней принадлежности инцидентов КБ нечетким кластерам с учетом дополнительной информации и особенностей обработки инцидентов КБ в системе мониторинга КБ конкретного СЭД. В работе приводится оценка работоспособности и эффективности двухэтапного метода нечеткой кластеризации инцидентов КБ в системе мониторинга КБ СЭД. Предложенный подход позволяет повысить эффективность мониторинга КБ СЭД и сократить период времени, необходимый для принятия решения на управление КБ СЭД за счет комплексного учета особенностей обработки событий КБ в системе мониторинга КБ конкретного СЭД.

Ключевые слова: кибербезопасность субъекта экономической деятельности, мониторинг кибербезопасности, событие кибербезопасности, инцидент, нечеткая кластеризация

Для цитирования: *Сизов В.А., Киров А.Д.* Метод двухэтапной нечеткой кластеризации инцидентов информационной безопасности для субъектов экономической деятельности // Прикладная информатика. 2023. Т. 18. № 5. С. 77–90. DOI: 10.37791/2687-0649-2023-18-5-77-90

Method of two-stage cybersecurity incidents fuzzy clustering for economic entities

V. Sizov[1], ***A. Kirov***[1*]
[1]*Plekhanov Russian University of Economics, Moscow, Russia*
[*]*Kirov.AD@rea.ru*

Abstract. The work is aimed at improving the efficiency of cybersecurity management (CS) of economic entities (SED) by organizing effective CB monitoring, taking into account such features of its process as the heterogeneity of sources of initial CB monitoring data, their presentation in different data formats, their inaccuracy, and largely uncertainty and noisiness, as well as a large number of KB events processed by heterogeneous components of the ERMS KB monitoring system. In this paper, in contrast to existing methods, a complex two-stage method for fuzzy clustering of SI events is proposed, taking into account the assessment of the criticality of SI events and the functionality of the ES IS monitoring system. At the first stage, the KB event clustering model based on the fuzzy c-means method is used. This model allows splitting the set of CI events into several fuzzy clusters according to the a priori probability that the CI event is an incident. At the second stage, to refine the results of the clustering of SI events obtained at the first stage, the model of clustering of SI incidents based on the method of extracting α-kernels of fuzzy clusters is used. This model allows you to manually select the thresholds for the degree of belonging of SI incidents to fuzzy clusters, taking into account additional information and features of processing SI incidents in the SI monitoring system of a particular EDMS. The paper evaluates the effectiveness of the two-stage method of fuzzy clustering of KB incidents in the EDMS KB monitoring system. The proposed approach makes it possible to increase the efficiency of ERMS CM monitoring and reduce the period of time required to make a decision on the ERMS CM management due to the complex consideration of the features of CM event processing in the ERMS CM monitoring system.

Keywords: economic entity cybersecurity, cybersecurity monitoring, cybersecurity event, incident, fuzzy clustering

For citation: Sizov V., Kirov A. Method of two-stage cybersecurity incidents fuzzy clustering for economic entities. *Prikladnaya informatika*=Journal of Applied Informatics, 2023, vol.18, no.5, pp.77-90 (in Russian). DOI: 10.37791/2687-0649-2023-18-5-77-90

Введение

Развитие технологий искусственного интеллекта и их проникновение в различные сферы деятельности, включая сферу кибербезопасности (КБ), требуют переосмысления применения методов искусственного интеллекта в управлении КБ. Например, использование Chat GPT в настоящее время позволяет эффективно создавать полиморфные вирусы, защита от которых не всегда надежно обеспечивается применением антивирусного программного обеспечения, и только комплексное выявление признаков этих вирусов, в том числе с помощью систем мониторинга КБ, позволяет своевременно выявлять подобные инциденты КБ и локализовывать их действия в корпоративной информационной системе субъекта экономической деятельности