DOI: 10.37791/2687-0649-2023-18-4-76-96

Разработка моделей для автоматизированного формирования компетентностей специалиста по кибербезопасности на основе сценарного подхода

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

Аннотация. Работа посвящена разработке моделей для автоматизированного формирования компетентностей специалиста по кибербезопасности на основе сценарного подхода. Актуальность работы определяется необходимостью своевременного обновления требований к профессиональным компетентностям специалиста по кибербезопасности в условиях развития способов, инструментальных средств информационного противоборства и отсутствием теоретического аппарата, позволяющего автоматизировать этот процесс. Целью данной работы является разработка моделей для автоматизированного формирования компетентностей специалиста по кибербезопасности на основе сценарного подхода, позволяющих анализировать информацию о действиях нарушителя кибербезопасности и на основе этой информации определять актуальный набор профессиональных компетентностей специалиста по кибербезопасности. Для достижения этой цели решается задача разработки модели действий нарушителя кибербезопасности и связанной с ней модели системы противодействия, определяющей актуальный набор компетентностей специалиста по кибербезопасности. Совокупность разработанных моделей учитывает техники и тактики действий нарушителя кибербезопасности, соответствующие им способы и инструментальные средства противодействия. Предложенный подход структурирования системы противодействия в виде совокупности взаимосвязанных модулей по результатам анализа используемых нарушителем кибербезопасности сценариев атак, техник и соответствующих тактик позволяет учесть особенности атак, которые наиболее часто реализуются, сформировать совокупность профессиональных действий специалиста по кибербезопасности на основе использования соответствующих способов и инструментов противодействия этим техникам, сгруппированным по функциональным модулям. Анализ результатов проведенного компьютерного эксперимента показал работоспособность предложенных моделей.

Ключевые слова: информационное противоборство, кибербезопасность, профессиональные компетенции специалиста, моделирование, оптимизация

Для цитирования: *Сизов В.А., Киров А.Д., Алейников В.В., Рудь И.П.* Разработка моделей для автоматизированного формирования компетентностей специалиста по кибербезопасности на основе сценарного подхода // Прикладная информатика. 2023. Т. 18. № 4. С. 76–96. DOI: 10.37791/2687-0649-2023-18-4-76-96

Development of models for the automated formation of competencies of a cybersecurity specialist based on a scenario approach

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

Abstract. The work is devoted to the development of models for the automated formation of competencies of a cybersecurity specialist based on a scenario approach. The relevance of the work is determined by the need to timely update the requirements for professional competencies of a cybersecurity specialist in the context of the development of methods and tools for information warfare and the lack of a theoretical apparatus that allows automating this process. The purpose of this work is to develop models for the automated formation of competencies of a cybersecurity specialist based on a scenario approach, which allow analyzing information about the actions of a cybersecurity violator and, based on this information, determining the current set of professional competencies of a cybersecurity specialist. The task of developing models for the automated formation of competencies of a cybersecurity specialist based on a scenario approach is to develop a model of actions of a cybersecurity violator and an associated model of a countermeasure system that determines the actual set of competencies of a cybersecurity specialist. In contrast to existing expert approaches to determining the professional competence model of a cybersecurity specialist, this paper uses a scenario approach that allows describing scenarios of actions of a cybersecurity violator at a formalized level, integrating the data obtained into the appropriate graph model and forming an activity professional model of a cybersecurity specialist based on optimizing the structure of the system counteraction. The set of developed models for the automated formation of competencies of a cybersecurity specialist based on a scenario approach takes into account many factors of information confrontation, such as: techniques and tactics of cybersecurity offenders, their corresponding methods and tools of counteraction. The proposed approach of structuring the countermeasure system in the form of a set of interrelated modules based on the results of the analysis of attack scenarios, techniques and corresponding tactics used by the violator of cybersecurity allows taking into account the features of attacks that are most often implemented, forming a set of professional actions of a cybersecurity specialist based on the use of appropriate methods and tools to counter these techniques grouped by functional modules. Analysis of the results of the conducted computer experiment showed the operability of the proposed models for the automated formation of competencies of a cybersecurity specialist based on the scenario approach.

Keywords: information confrontation, cybersecurity, professional competencies of a specialist, modeling, optimization

For citation: Sizov V., Kirov A., Aleinikov V., Rud I. Development of models for the automated formation of competencies of a cybersecurity specialist based on a scenario approach. *Prikladnaya informatika*=Journal of Applied Informatics, 2023, vol.18, no.4, pp.76-96 (in Russian). DOI: 10.37791/2687-0649-2023-18-4-76-96