DOI: 10.37791/2687-0649-2024-19-4-126-143

Оптимизация компонентного состава систем информационной безопасности на основе эволюционно-симулятивных моделей

В. А. Конявский[1,2]***, Г. В. Росс***[3*]

[1]*Московский физико-технический институт (Национальный исследовательский университет), Москва, Россия*

[2]*АО «Особое конструкторское бюро систем автоматизированного проектирования», Москва, Россия*

[3]*Российский экономический университет им. Г. В. Плеханова, Москва, Россия*

[*]*Ross-49@mail.ru*

Аннотация. В статье рассмотрены задачи модернизации системы информационной безопасности распределенной вычислительной системы. В условиях роста агрессивности среды объекты, защищенность которых ранее считалась достаточной, теперь нуждаются в дополнительных мерах по защите. В качестве примеров можно привести значимые объекты критической информационной инфраструктуры, которые в настоящее время относятся к объектам госрегулирования. Для решения задачи синтеза компонентного состава систем информационной безопасности в статье предложен комплексный алгоритм, включающий шаги, на которых применяется различный математический аппарат. Использование такого подхода позволяет осуществить выбор приемлемого варианта совокупности программно-технических средств, обеспечивающих возможность блокирования атак на заданном уровне защиты. Задачу предполагается решить на основе функциональных возможностей программно-технических компонентов, их параметров и функциональных взаимосвязей. Новизна результатов исследования заключается в представлении дискретной модели системы информационной безопасности в виде симулятивной модели (частный случай стохастического программирования), позволяющей учесть функциональные особенности аппаратных и программных средств программно-технических средств при модернизации системы информационной безопасности. Предложен алгоритм симуляции, учитывающий характеристики системы информационной безопасности, которые могут принимать как детерминированные, так и вероятностные значения. При этом введены необходимые определения, положения которых иллюстрируются численными примерами. Расчеты позволяют выявить наиболее дефицитные ресурсы, установить, насколько удачны специализация и структура системы информационной безопасности, оценить результаты изменений системы информационной безопасности, перераспределения ее функций и материальных средств.

Ключевые слова: системы защиты информации, информационная безопасность, имитационные модели, стохастическое программирование, проектирование информационных систем

Для цитирования: *Конявский В. А., Росс Г. В.* Оптимизация компонентного состава систем информационной безопасности на основе эволюционно-симулятивных моделей // Прикладная информатика. 2024. Т. 19. № 4. С. 126–143. DOI: 10.37791/2687-0649-2024-19-4-126-143

Optimization of the component composition of information security systems based on evolutionary simulation models

V. Konyavskiy[1,2]***, G. Ross***[3*]
[1]*Moscow Institute of Physics and Technology (National Research University), Moscow, Russia*
[2]*Joint Stock Company "Special Design Bureau of Computer-aided Design Systems", Moscow, Russia*
[3]*Plekhanov Russian University of Economics, Moscow, Russia*
[*]*Ross-49@mail.ru*

Abstract. The article discusses the tasks of modernizing the information security system of a distributed computing system. In an increasingly aggressive environment, objects whose security was previously considered sufficient now require additional protection measures. Examples include significant objects of critical information infrastructure, which are currently subject to government regulation. To solve the problem of synthesizing the component composition of information security systems, the article proposes a complex algorithm that includes steps in which various mathematical tools are used. Using this approach allows to select an acceptable option for a set of software and hardware tools that provide the ability to block attacks at a given level of protection. The problem is supposed to be solved based on the basis of the functionality of software and hardware components, their parameters and functional relationships. The novelty of the research results lies in the presentation of a discrete model of an information security system in the form of a simulation model (a special case of stochastic programming), which makes it possible to take into account the functional features of hardware and software when modernizing the information security system. A simulation algorithm is proposed that takes into account the characteristics of the information security system, which can take on both deterministic and probabilistic values. At the same time, the necessary definitions are introduced, the provisions of which are illustrated with numerical examples. A simulation algorithm is proposed that takes into account the characteristics of the information security system, which can take on both deterministic and probabilistic values. Also the necessary definitions are introduced, the provisions of which are illustrated with numerical examples. Calculations make it possible to identify the most scarce resources, establish how successful the specialization and structure of the information security system are, evaluate the results of changes in the information security system, redistribution of its functions and material resources.

Keywords: information security systems, information security, simulation models, stochastic programming, information systems design

For citation: Konyavskiy V., Ross G. Optimization of the component composition of information security systems based on evolutionary simulation models. *Prikladnaya informatika*=Journal of Applied Informatics, 2024, vol.19, no.4, pp.126-143 (in Russian). DOI: 10.37791/2687-0649-2024-19-4-126-143

Введение

Достаточный уровень защищенности информационных и производственных систем с компьютерным управлением определяется изменяющимся уровнем агрессивности среды и, соответственно, возможными потерями от реализации информационных атак. В свою очередь, рост агрессивности среды фиксируется регуляторами, отражается в изменении требований к защищенности систем. Меняются модель угроз и модель нарушителя. Объекты, защищен-