INTELLIGENT SYSTEM OF COMPUTER NETWORK SECURITY ANALYSIS

Stepashkin M.V., Kotenko I.V.

Saint-Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
199178, Russia, Saint-Petersburg, 14th Line, 39
stepashkin@comsec.spb.ru, ivkote@comsec.spb.ru

This paper presents the intelligent system of computer network security analysis. This system is based on the automatic generation of general attack graph and the usage of qualitative security metrics. The general attack graph reflects the possible distributed attacks scripts taking into account the network configuration, security policy as well as the infringer's location, goals, knowledge level and strategy. Security metrics allow to estimate computer network security with various detailing and in view of different aspects. The paper considers the system structure, the used models, in particular, the ones of attack graph formation and security level evaluation. The system operation is demonstrated on a test example.