Choice of the Data Mining technologies for intrusion detection systems into a corporate network

©T.I. Buldakova, A.Sh. Dzhalolov
Bauman Moscow State Technical University, Moscow, 105005, Russia

The problem of intrusion detection into a corporate network is considered in this article. The main components of intrusion detection system are allocated and their functions are described. Various approaches to identification of violations of information security are analysed. For this purpose, the characteristic of the main methods of intrusion detection is given, their merits and demerits are allocated. It is shown that to increase the efficiency of detection of possible invasion situations, it is necessary to use advanced data mining technologies. So for the purpose of application in intrusion detection the features of the data mining technologies are investigated, by the results of their comparative analysis hybrid means for identification of attacks are offered. It is shown that is the most perspective for a considered task use of neuro-fuzzy methods. The architecture of neuro-fuzzy system for intrusion detection into a network is offered.

Keywords*: information security, invasion, corporate network, data mining, neuro-fuzzy system.*

Buldakova T. I. graduated from Bauman Moscow Higher Technical School in 1980. Dr. Sci. (Eng.), Professor of the Information Security Department of Bauman Moscow State Technical University. Author of about 150 published works. Sphere of scientific interests: information and analytical systems, intellectual technologies, the system analysis, modeling. e-mail: buldakova@bmstu.ru

Dzhalolov A. Sh. graduated from Financical Academy under the Government of the Russian Federation in 2010. Post-graduate student of Information Security Department of Bauman Moscow State Technical University. Author of 6 published works. Sphere of scientific interests: informatization of public administration, situational centers, decision support systems.