BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 3, Number 373 (2018), 6 – 14

UDC 004.056

B. B. Akhmetov[1], V. A. Lakhno[2], B. S. Akhmetov[3], V. P. Malyukov[2]

[1]Yessenov University, Aktau, Kazakhstan,
[2]Department of management of information systems and cybersecurity,
European University, Kiev, Ukraine,
[3]Kazakh National Pedagogical University named after Abay, Almaty, Kazakhstan.
E-mail: berik.Akhmetov@kguti.kz, Valss21@ukr.net, bakhytzhan.akhmetov.54@mail.ru,
volod.malyukov@gmail.com

THE CHOICE OF PROTECTION STRATEGIES DURING THE BILINEAR QUALITY GAME ON CYBER SECURITY FINANCING

Abstract. There is developed a model for the module of an intellectualized system for decision-making support on the cyber security means financing of the information object. The model is based on the toolkit use of the theory of multi-step games in which the steps are made alternately by the sides of cyber security and attacker. There was obtained a solution that enables interested parties to evaluate financial strategies for effective cyber security systems construction in the condition of not complete information about the financial state of the attacking party (hackers). The model differs from existing approaches by solving a bilinear multi-step quality game with several terminal surfaces.

In work, there is performed a computational experiment and is given the corresponding results. Confirmed during the simulation experiment solution takes into account the financial components of cyber security strategies at any ratio of parameters describing the process of cyber security financing in the condition of information lack about the financial condition of hackers.

Keywords: objects of informatization, cyber security, multi-step quality game, optimal financing strategies, decision-making support system.

Introduction. The researches of authors [1] have the information that managers of many organizations and companies do not have a deep understanding of the need to solve the permanent task of financing cyber security means (CSM) of their information systems and technologies (IST). As a result, in the condition of increasing amount of cyber threats [2] in combination with the lack of an appropriate funding strategy in CSM there are appeared situations in which there is a high degree of risk associated with the loss of important information or its discrediting. In the coming years, successful cyber attacks will unlikely be the result of one or two technological tools of hacking. Now there is formed a trend according to which hackers will use many different steps and elements to hack into IST.

Most small and medium-sized companies and organizations are limited to the standard procedure of IST protection, which in practice are focused on the deployment of antivirus systems and on the configuration of firewalls. However, we will note that such a strategy of cyber security (CS) (in some cases caused by limited financial resources from the protection side) may subsequently have a significant impact on the prospects of being attacked by computer intruders. And even in a situation where the