EXAMPLE OF THESIS PRESENTATION

UDC 004.056, 004.75

Dudykevych Volodymyr, Harasym Yuriy
vdudykev@polynet.lviv.ua,, igarasym@space-it.com.ua

1National University "Lviv Polytechnic", Lviv
[2]Space IT, Київ

The use of fuzzy set theory in the tasks of evaluating the resilience of information security systems

At the design stage of an information security system (ISS) in a corporate communication network (CCN) with the property of resilience, an important task is to obtain an accurate and timely risk assessment. Due to the lack of sufficient statistical data on the probability of information security threats materializing, there is also no single developed universally accepted methodology for quantitative risk assessment. This paper employs qualitative risk assessment methods proposed in the international standards ISO 17799 and ISO 27001, which have gained widespread acceptance in global practice.

The information security system in CCN is often a distributed information system operating under the uncertainty of destabilizing factors [1]. The use of fuzzy set theory to describe the structure and predict its parameters at the stage of building an adaptive ISS model allows for the assessment of the general characteristics of the system with further development of decisions to increase efficiency and optimize its operating modes.

The resilience indicator of the ISS is determined through the resilience function, i.e., through a set of function values characteristic of each specific ISS topology [2]. When calculating resilience functions, each of the finitely many threats ($i = \overline{1,n}$) is described using fuzzy set theory. Threats are represented by a function of two parameters – the probability of occurrence $P_{t\square reat}$ (expressed qualitatively through expert assessments) and the potential decrease in the system's resilience indicator $\Delta d^{t\square reat}$ (can be expressed as both qualitative and quantitative indicators, depending on the adopted performance indicators of the system's functions).

At the stage of mathematical modeling, we represent the system as a bipartite graph. Each of the system's nodes is characterized by indicators of operational quality, the criticality of the information processed, the effectiveness of protection measures, and the vector of threats.

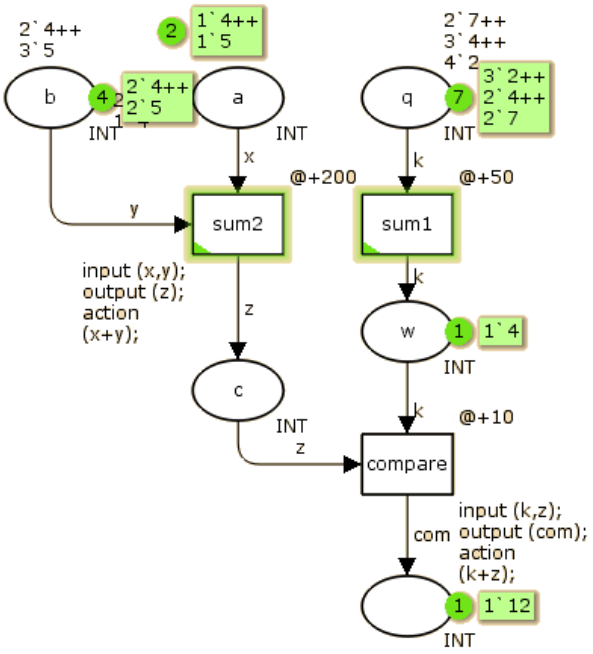

Fig. 1. Elementary model of an information security system

The choice of a rational topology for the information security system is based on the total indicator of averted threats, calculated for each of the possible initial system topologies

$\overline{W} = F(P_{i_{t\square reat}}; \Delta d_i^{neutr}; P_{i_{t\square reat}}{}^{neutr}; i = \overline{1,n})$, — where $P_{i_{t\square reat}}{}^{neutr}$ – Is the probability of neutralizing the n-th threat.

References

V. B. Dudykevych, Y. R. Harasym, and V. V. Nechipor, "Methods of modeling information security systems for corporate communication networks," Scientific and Technical Journal "Modern Information Protection," no. 4, pp. 54 – 60, 2011.

V. V. Nechipor, and Y. R. Harasym, "Assessment of the resilience of information security systems using CPN TOOLS," Proceedings of the VIII International Scientific and Technical Conference of Students and Youth "The World of Information and Telecommunications," Kyiv, 2011, pp. 104 – 105.