**Z. Koval**

# DYNAMICS OF THE WORLD GOVERNMENT REACTION TO CYBER THREATS: LESSONS FOR UKRAINE

**Problem setting** Ensuring public administration with information security of Ukraine in terms of cyber threats is still in an uncertain state. Ukraine suffers from an increasing complex of current and hidden cyber threats. Clear concepts, key legal mechanisms of information security management of Ukraine in terms of cyber threats has not been formed, and the experience of advanced countries is not introduced on time.

**Recent research and publications analysis** This problem is discussed in print and on the Internet, it was developed by Ukrainian military and civilian analysts such as: Doctor of Technical Sciences, Academician Yu. Danyk, Ph.D., associate professor V. Farushev, deputies of Ukraine Volodymyr Oliinyk, Yu. Samoilenko, O. Kuzmuk, researchers I. Izhutova, S. Oleksandrov, B. Butkevych, V. Yakovenko, T. Narytnyk, I. Serhiienko, M. Konstantynov, Yu. Pasternak, foreign experts: E. Kasperskyi, I. Morozovitska, R. Khalilov.

**Unsolved parts of the general problem** Approaches to ensuring information security management of Ukraine in terms of cyber threats have not yet deployed their fragmented vision and disagreement. In this segment of national security in Ukraine the situation is still one of the worst in the CIS.

**Paper objective** The purpose of this publication is to attempt to identify ways to improve information security of Ukraine on the basis of the experience of operational management reaction against cyber threads of advanced countries and from the standpoint of system analysis.

**Paper main body** Around us the world is relentlessly globalizing while international competition is exacerbating. The central scene of clashes and rivalry of various national interests became the information space. During the transition to the information society the virtual space of the Internet becomes a strategic battleground, changing the political, geopolitical and military priorities. The main aim of the new information war is information dominance. Information and technological superiority, which are based on the network, generate Network-centric war, or cyberwar. The main content of the new Internet era theory of war is that the war becomes a network phenomenon, and military actions - a type of network processes. There is a need in the formation of information forces that will develop into the information army. In terms of cyberwar civilians and military units are combined into a single network on which information circulates.