SUMMARY

Subject of the thesis: Cyberterrorism as a threat to national security of the Russian Federation.

Author: Mikhail Klimenskiy.

Academic Adviser: Soloveva E.A., Assistant Professor, PhD, Political Science.

Organization: School of International Relations, Chair of International Relations, World Economy and International Law, Pyatigorsk State Linguistic University.

Relevance of the research issue is defined by a significant increase of communicativeness in modern socio-political environment, which has intensified the use of information and information flows both in favorable and destructive-oriented goals. As a result of these trends such phenomena as information warfare, using of mass media in extremist and terrorist purposes and cyber-terrorism have appeared. These processes, as a new component in the system of threats to national and international security, require study and political conceptualization.

The purpose of the research is to analyze cyberterrorism as a new component in the system of threats to national security of the Russian Federation and to find ways to its neutralization.

Research objectives:

- to study conceptual approaches to the definition of cyberterrorism in the context of political science;
- to examine cyberterrorism as a socio-political phenomenon that represents a threat to national security;
- to analyze Russian and international experience in field of opposing cyberterrorism;
- to develop recommendations for improving state policy of opposing cyberterrorism.

Scientific novelty: As a result of the research conceptual approaches to the definition of term "cyber-terrorism" have been systematized. The factors that generate cyberterrorism in the Russian Federation have been worked out, along with features and trends of its operation at the present stage. Comparative analysis of international experience in opposing cyberterrorism has been conducted. Also, main directions for improving the effectiveness of policy against cyberterrorism in Russia have been suggested.

Structure: an introduction, two chapters, containing four paragraphs, a conclusion and 105-reference bibliography (22 of which are in foreign languages) and 9 appendixes. The total volume is 86 pages.

Summary: In the modern world it is impossible to imagine our life without computer systems, the global network which enable communication, exchange and storage of information, and also management and control of bank systems, infrastructure of branches of industries and even combat systems and military facilities.

In this regard, it can be concluded that cyber security, as part of the information security appears a key aspect of national security.

Political, social and economic factors jointly contribute to the emergence of cyberterrorism in the Russian Federation. Its basic features are – public nature, distance from the site of the terrorist attack, anonymity. Current trends which define the development of cyberterroristic threat to the Russian Federation at present stage include politicization of cyber-terrorism, growth of the level of threat, and growth of technological equipment of subjects who perform it.

In consideration of the factors that give rise to cyberterrorism, prevention of cyberterracts is a complex task. Consequently, political, social, economic, historical, psychological reasons should be the subject of constant attention and preventive intervention by the state and civil society.

To counteract cyberterrorism successfully it is necessary to adopt comprehensive legislation on electronic security, in accordance with international standards, the organization of effective cooperation with foreign states and their law enforcement and intelligence agencies, as well as with international organizations, and the creation of national units to combat cybercrime and international contact point for aiding to respond to transnational computer incidents.