INFORMATION TERRORISM: GENERAL INFORMATION AND WAYS OF PREVENTION

Ivanova Olha

National Aviation University, Kyiv

XXI century - a time of rapid development of the information space, the world of globalization and the formation of the information society, in these conditions, terrorism began to act as an independent factor that could threaten the integrity of the state and destabilize the international situation.

The term «information terrorism» is more general and covers the use of various methods and means of informational influence on various aspects of human society (physical, informational, cognitive, social).

Information terrorism should be understood as one of the types of terrorist activity aimed at the use of various forms and methods of temporary or irreversible decommissioning of the state's information infrastructure or its elements, as well as the targeted use of this infrastructure to create catastrophic conditions for different parties. vital activity of society and the state [1].

Among the political causes of information terrorism, the main one is political instability. If we consider the socio-economic reasons, the main factor is considered to be the low standard of living in the country. Terrorism today is a business that can bring its organizers a considerable income that can be compared with the income from the oil business [2]. Trade in weapons, drugs, hostages allows you to make huge profits.

The analysis and generalization of the existing experience of anti-terrorist activity allowed to formulate tasks on protection of critical infrastructure from cyberterrorism and the basic measures directed on their decision at national level [3]:

- coordination of measures of state and non-state agencies to prevent threats to information security in open networks. To this end, a single policy should be developed and adopted, aimed at respecting the legal rights of citizens to information and intellectual property, which provides for the protection of network equipment in the country from the penetration of hidden elements of information weapons. This is especially important in the context of mass purchases of foreign information technology and network equipment;

- development of the state program of improvement of the information technologies providing connection of national and corporate networks to world open networks at observance of requirements of safety of information resources;

- development of national legislation regarding the rules of handling information resources, regulations of rights, duties and responsibilities of users of open world networks [3];

- organization of interstate cooperation in the work of international organizations, public committees and commissions in projects for the development of global information networks;

- active participation in the development of international legislation and regulatory support for the functioning of global open networks; - creation of a single anti-terrorist space of allied countries.

A comprehensive solution to these problems will allow to take the necessary countermeasures to combat information terrorism in a centralized manner, significantly reduce the likelihood of its threats to critical infrastructure and ensure the protection of their national interests [2]. Economic and scientific-technical policy of connection to the world's open networks should be considered through the prism of solving the issue of national information security. Russia's participation in international telecommunications and information exchange systems must be planned, carried out in accordance with real needs, economic and technological capabilities, and be a state monopoly.

References:
1. Gorbunov, Yu.S. Terrorism and legal regulation of counteraction to it /

45

POLIT.Challenges of science today, 5-9 April 2021

Yu.S. Gorbunov. M.: Young Guard, 2008
2. John Arquilla, David Ronfeldt, and Michelle Zaninni, "Networks, Netwar, and Information Age Terrorism" in Countering the New Terrorism (Washington DC: RAND Corporation, 1998).
3. INFORMATION AGE TERRORISM: TOWARD CYBERTERROR [Electronic resource] - Resource access mode: https://fas.org/irp/threat/cyber/docs/npgs/terror.htm