AUTHOR	*Maria V. Smekalova* — PhD Candidate at the Institute for the US and Canadian Studies, Russian Academy of Sciences (e-mail: mashasmekalova@gmail.com).
TITLE	**EVOLUTION OF U.S. POLICY APPROACHES TO ENSURING CYBERSECURITY AND DEFENSE OF CRITICAL INFORMATION INFRASTRUCTURE**
SUMMARY	Rapid development of the Internet technologies has brought both unprecedented opportunities for economic development and a number of dangers for international community. In the early 2000s, challenges and threats emanating from the cyberspace were prioritized by leading world powers. The United States were among the first to elaborate legal framework for cyberpolicy aiming at providing national security after terrorist attacks of 2001. As time passed, dozens of legislation acts were adopted, and a number of agencies and committees responsible for ensuring information security emerged. The article examines the evolution of the U.S. conceptual approaches to information security (cybersecurity of the U.S. official documents) during the presidency of George Bush Jr. (during his tenure in office, the first National Strategy to Secure Cyberspace was accepted), Barack Obama and Donald Trump. The author traces priority changes that took place in this area as well as analyzes U.S. relationships with other major actors in the cybersphere, especially Russia and China. A particular attention is paid to the U.S. policy directed at ensuring security of critical information infrastructures (CII). The author emphasizes that, although a set of regulating document has been adopted, the security level of CII objects remains relatively low. In general, the analysis of national policy documents allowed the author to outline several tendencies, characterizing development of the U.S. policy in cybersphere in recent years. In particular, there is an increasing tendency towards unilateralism relating to the sanctions measures against particular countries and their companies. In this context, the cybersecurity issues are often considered not as an end in itself but as means of achieving wider goals of external and internal policy. The author concludes that the U.S. cybersecurity policy is reactive in nature, which directly affects its effectiveness.
KEYWORDS	the United States of America, the U.S., information security, cybersecurity, cyberthreats, cyberstrategy, critical information infrastructure (CII), sanctions.