AUTHOR	*Igor A. Sheremet* — Doctor of Sciences (Engineering), Professor, Corresponding Member of the Russian Academy of Sciences, Chief Research Fellow at the School of World Politics, Lomonosov Moscow State University; Deputy Director for Science of the Russian Foundation for Basic Research.
TITLE	**ENSURING CYBERSECURITY IN THE CONTEXT OF DIGITAL ECONOMY DEVELOPMENT**
SUMMARY	Strategic documents of the Russian Federation consider opportunities created by digital economy as one of the key factors capable of ensuring economic growth and national sovereignty as well as of stimulating production in all spheres of social and economic activities. However, the author stresses, that uncontrolled digitalization of economy can drastically increase its vulnerability to cyberthreats. In that context, it is necessary to address more specifically challenges and threats associated with the digitalization process in the economic sphere. The paper examines key approaches to the definition of the phenomenon of 'digital economy' as well as the most promising directions for global information infrastructure development in general and its hardware/software elements in particular. The author notes that in this context the quest for the most effective management mechanisms of sociotechnological systems (STS) that make up the digital economy, is of special importance. At the same time one can observe a rapid expansion of cyberthreats realized by means of various infotechnological impacts. The paper provides a detailed analysis of the main types of cyberattacks and outlines their potential impact on critical infrastructures of the digital economy. The author emphasizes that the high level of interdependence of its elements significantly increases destructiveness of the so called chained effects of cyberattacks. In view of the impossibility of reaching complete protection of the digital economy from the cyberthreats resilience of the sociotechnological systems is of particular importance. Cybersustainability implies the ability of a system to perform its functions under successful attacks on its resources (probably less effectively within in a short period of time necessary to neutralize cyberthreats and their impacts). Turning to the issue of ensuring cybersustainability of the emerging digital economy of the Russian Federation, the author examines the main types of system-destructing cyberattacks and highlights the steps taken by the Russian government to tackle these threats. The author concludes that it will impossible to achieve independence and resilience of the Russian information infrastructure without relevant capacity-building in science and technology as well as without training a new generation of S&T personnel.
KEYWORDS	Russian Federation, digital economy, global information infrastructure, sociotechnological system, cyberattack, cybersecurity, cybersustainability.