DOI: 10.18572/1813-1190-2020-6-35-39

Совершенствование правового обеспечения трехуровневой доктрины США по киберсдерживанию и защите цифровых данных*

Танимов Олег Владимирович,
доцент кафедры теории государства и права
Московского государственного юридического университета имени О.Е. Кутафина (МГЮА),
кандидат юридических наук, доцент
tanimov@mail.ru

Зульфугарзаде Теймур Эльдарович,
доцент кафедры гражданско-правовых дисциплин
Российского экономического университета имени Г.В. Плеханова,
кандидат юридических наук, доцент
zulfugarzade.te@rea.ru

Цель. В статье в качестве предмета исследования определены стратегические направления развития и совершенствования международно-правового обеспечения безопасности в киберинформационной среде, основанные на действующей трехуровневой доктрине киберпространственного сдерживания, выработанной США в 2018 г., новационная базовая модель которой предусматривает восстановление межгосударственного сотрудничества, выработку и принятие государствами — членами ООН стратегии сдерживания, прежде всего, киберугроз, включая защиту цифровых данных. **Методика исследования** основана на выявлении недостатков в формулировках необязательных норм поведения в киберинформационном пространстве и обеспечении кибербезопасности посредством международного сотрудничества между всеми заинтересованными субъектами международного права, а также институтов гражданского общества и коммерческих организаций. **Научную новизну** исследования определяют выводы, в соответствии с которыми, в частности, одностороннее принятие решения о возложении (фактически приписывание) ответственности за нарушение необязательных норм и принятие карательных или возмездных мер может быть по меньшей мере юридически некорректным и как результат весьма проблематичным, отсутствие в требованиях возрастания легитимности однозначности усиливает негативное отношение к самому доказательственному процессу, что, в свою очередь, может повлиять на законность любого действия, предпринятого в качестве контрмеры; для обоснования утверждений о причастности к кибератакам необходимо постоянное сотрудничество с негосударственным сектором, занимающимся вопросами обеспечения кибербезопасности.

Ключевые слова: право, цифровизация, безопасность, персональные данные, риск, новации, инновационный, киберпространство, информация, данные.

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16114.

The Improvement of the Legal Regulation of the U.S. Three-Tier Cyber Suppression and Digital Data Protection Doctrine

Tanimov Oleg V., Associate Professor of the Department of Theory of State and Law of the Kutafin Moscow State Law University (MSAL), PhD (Law), Associate Professor, tanimov@mail.ru

Zulfugarzade Teymur E., Associate Professor of the Department of Civil and Legal Disciplines of the Plekhanov Russian University of Economics, PhD (Law), Associate Professor, zulfugarzade.te@rea.ru

Purpose. The article defines as the subject of research strategic directions for the development and improvement of international legal security in the cyber-information environment, based on the current three-level doctrine of cyberspace deterrence, developed by the United States in 2018, the innovative basic model of which provides for the restoration of interstate cooperation, the development and adoption by UN member States of a strategy to deter primarily cyber threats, including the protection of digital data. **The research methodology** is based on identifying shortcomings in the wording of non-mandatory norms of behavior in the cyber-information space and ensuring cybersecurity through international cooperation between all interested subjects of international law, as well as civil society institutions and commercial organizations. **The scientific novelty** of the research is determined by the conclusions according to which, in particular, unilateral decision-making on assigning (in fact, attributing) responsibility for the violation of non-mandatory rules and taking punitive or punitive measures may be at least legally incorrect and, as a result, very problematic; the lack of unambiguity in the requirements of increasing legitimacy increases the negative attitude to the evidentiary process itself, which, in turn, may affect the legality of any action taken as a counter-measure; to substantiate claims of involvement in cyber attacks, it is necessary to constantly cooperate with the non-state sector involved in cybersecurity issues.

Keywords: law, digitalization, security, personal data, risk, innovation, innovative, cyberspace, information, data.