DOI: 10.18572/1813-1190-2018-1-24-30

Уголовно-правовое обеспечение информационной безопасности в России

Гладких В.И., Сухаренко А.Н.*

Цель. *Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования государственных институтов, одновременно порождает новые информационные угрозы. Возможности трансграничного обмена информацией все чаще используются для достижения террористических, экстремистских и иных криминальных целей в ущерб международной безопасности и стратегической стабильности. При этом практика внедрения информационных технологий без надлежащего обеспечения информационной безопасности существенно повышает вероятность проявления информационных угроз. Для минимизации масштабов таких угроз был принят Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», проанализированный в данной статье.* ***Методология:*** *анализ, синтез, формально-юридический метод, метод сравнительного правоведения.* ***Выводы.*** *Состояние информационной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и скоординированности компьютерных атак на объекты критической информационной инфраструктуры. В этой связи основными направлениями обеспечения информационной безопасности являются: повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования; развитие механизмов обнаружения и предупреждения киберугроз и ликвидации последствий их проявления; повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической инфраструктуры; повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям.* ***Научная и практическая значимость.*** *Проведенное исследование дает системный и комплексный анализ организационно-правовых мер, направленных на повышение уровня киберграмотности (осведомленности об угрозах и способах защиты), обязательное раскрытие информации о киберинцидентах, совершенствование международного сотрудничества и национального законодательства о составах преступлений и процедурах расследования. Выводы данного исследования могут быть использованы при создании нормативно-правовых актов, регулирующих вопросы обеспечения информационной безопасности, а также применяться в учебном процессе при подготовке специалистов в данной области.*

Ключевые слова: *информационная безопасность, угроза, киберпреступность, инфраструктура, компьютерные технологии.*

Criminal Law Coverage of Information Security in Russia

Gladkikh V.I., Sukharenko A.N.**

Purpose. *The expansion of the applications of information technology as a factor of development of economy and improvement of the functioning of state institutions, at the same time generates new information threats. Cross-border exchange of information are increasingly being used to achieve the terrorist, extremist and other criminal purposes to the detriment of international security and strategic stability. The practice of introduction of information technology without proper information security significantly increases the probability of information threats. To minimize such threats was adopted the Federal law of July 26, 2017 No. 187-FZ "About the security of critical information infrastructure of the Russian Federation" is analyzed in this article.* ***Methods:*** *analysis, synthesis, formal legal method, method of comparative law.* ***Results.*** *The state of information security is characterized by constant increase in complexity, scale and coordinated cyber attacks on objects of critical information infrastructure. In this regard, the main directions of ensuring information security are: improving the security of critical information infrastructure and the sustainability of its operation; development of mechanisms for detection and prevention of cyber threats and the elimination of the consequences of their manifestation; improving the protection of citizens and territories from consequences of emergencies, caused by the information technology impact on critical infrastructure; improving the efficiency of prevention of offences committed using information technology, and combating such offences.* ***Scientific and practical significance.*** *The conducted study gives a systematic and comprehensive analysis of organizational and legal measures aimed at increasing the level of cyberprotest (awareness about threats and methods of protection), mandatory disclosure of cyber incidents; improve international cooperation and national legislation on offences and investigation procedures. The findings of this study can be used in the creation of normative-legal acts regulating the issues of information security, as well as be used in educational process at training of specialists in this field.*

Keywords: *information security, risk, cybercrime, infrastructure, computer technology.*

* **ГЛАДКИХ ВИКТОР ИВАНОВИЧ,** заведующий кафедрой публичного права и правового обеспечения управления Государственного университета управления, профессор Международного юридического института, доктор юридических наук, профессор, Заслуженный юрист Российской Федерации, *gladkich04@mail.ru*
СУХАРЕНКО АЛЕКСАНДР НИКОЛАЕВИЧ, директор Центра изучения новых вызовов и угроз национальной безопасности Российской Федерации, *sukharenko@mail.ru*

** **GLADKIKH VIKTOR I.,** Head of the Department of Public Law and Legal Support of Management of the State University of Management, Professor of the International Law Institute, Doctor of Law, Professor, Honored Lawyer of the Russian Federation
SUKHARENKO ALEKSANDR N., Director of the Center for Study of New Challenges and Threats to National Security of the Russian Federation