Information for citation:
Pastukhov P. S., Losavio M. Ispol'zovanie informatsionnykh tekhnologiy dlya obespecheniya bezopasnosti lichnosti, obshchestva i gosudarstva [Use of Information Technology to Ensure Security of the Individual, Society and State]. *Vestnik Permskogo Universiteta. Juridicheskie Nauki* – Perm University Herald. Juridical Sciences. 2017. Issue 36. Pp. 231–236. (In Russ.). DOI: 10.17072/1995-4190-2017-36-231-236.

UDC 342
DOI: 10.17072/1995-4190-2017-36-231-236

USE OF INFORMATION TECHNOLOGY TO ENSURE SECURITY OF THE INDIVIDUAL, SOCIETY AND STATE

P. S. Pastukhov

Perm State University
15, Bukireva st., Perm, 614990, Russia
ORCID: 0000-0003-0391-5540
ResearcherID: B-5451-2017
e-mail: pps64@mail.ru

M. Losavio

University of Louisville
Louisville, Kentucky, 40292, USA
ORCID: 0000-0003-0391-5540
ResearcherID: B-5451-2017
e-mail: michael.losavio@louisville.edu

Introduction: *the article analyzes threats to the individual, society and state present in the modern society, and considers the principal directions in the use of modern information technology for ensuring security and increasing efficiency of the state activities and law enforcement.* ***Purpose:*** *based on the study of technical characteristics of computer technologies and software, to identify spheres of the information technology application, to determine the legal regulation of the technology application for providing the efficiency of the state and administrative activities in law enforcement with the aim of creating a safe living environment.* ***Methods:*** *the methodological framework of the research is based on a set of methods of scientific cognition, including general scientific and specific scientific ones, in particular the formal-legal, comparative law, technical-legal methods.* ***Results:*** *the authors state that technical, organizational, administrative and legal aspects of the information technology implementation optimize the activities on ensuring security, but the conditions of the global computerization create new risks for privacy. The article explores the guarantees against the total control to prevent the invasion of privacy. Some specific aspects are analyzed necessary to reach a reasonable balance between the information technology implementation and observance of the constitutional guarantees of privacy.* ***Conclusions:*** *in the modern information society, with the widespread use of the artificial intellect and the increasing number of cybercrimes, the application of information technology in all the spheres of law enforcement, economic and regulatory activities is a necessary, inevitable and the most promising way of development to ensure security of the individual, society and state.*

Keywords: information threats; information technology; geo-information technology; law enforcement; crime investigation; security of the individual; society and state

Information in Russian

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА

П. С. Пастухов

Доктор юридических наук, доцент кафедры уголовного процесса и криминалистики
Пермский государственный национальный исследовательский университет
614990, Россия, г. Пермь, ул. Букирева, 15
ORCID: 0000-0003-0391-5540
ResearcherID: B-5451-2017
e-mail: pps64@mail.ru

М. Лосавио

Профессор
Университет Луисвилля (США)
40292, США, штат Кентукки
ORCID: 0000-0003-4542-8599
ResearcherID: E-3528-2017
e-mail: michael.losavio@louisville.edu

Введение: *в статье анализируются угрозы современного общества для личности, общества и государства, исследуются основные направления использования современных информационных технологий для обеспечения безопасности и повышения эффективности государственной деятельности и правоприменительной практики.* ***Цель:*** *на основе изучения технических характеристик компьютерных технологий, программного обеспечения выявить сферы применения информационных технологий, определить правовое регулирование применения технологий для обеспечения эффективности государственной и управленческой деятельности в правоприменительной практике с целью создания безопасной среды проживания.* ***Методы:*** *методологическую основу данного исследования составляет совокупность методов научного познания. В статье использованы общенаучные и частнонаучные методы исследования, в частности формально-юридический, сравнительно-правовой, технико-юридический.* ***Результаты:*** *авторы утверждают, что технические, организационные, управленческие, правовые аспекты внедрения информационных технологий оптимизируют деятельность по обеспечению безопасности, но в условиях повсеместной информатизации возникают новые риски для частной жизни граждан. В статье исследуются гарантии от тотального контроля для предотвращения вмешательства в частную жизнь человека. Анализируются отдельные аспекты, связанные с необходимостью достижения разумного баланса между внедрением информационных технологий и обеспечением конституционных гарантий неприкосновенности частной жизни.* ***Выводы:*** *в современном информационном обществе, в условиях повсеместного распространения искусственного интеллекта, количественного роста компьютерных преступлений, применение информационных технологий во всех сферах правоохранительной, экономической, регулятивной деятельности является необходимым, неизбежным и самым перспективным направлением развития для обеспечения безопасности личности, общества и государства.*

Ключевые слова: информационные угрозы; информационные технологии; геоинформационные технологии; правоохранительная деятельность; расследование преступлений; безопасность личности, общества и государства

Introduction

The current development of society creates a lot of risks of natural, technology-related, ecological, and conflict character, as well as risks associated with the spread of domestic and international terrorism, deterioration in transport safety, administration risks. In this list, information security threats occupy a special place and include:

– problems in information support for the state power bodies, municipal companies and services;

– interception of the television and radio broadcasts, alert and information system broadcasts;

– unauthorized access to the information covering the activities of the state power bodies, municipal companies and services;

– unauthorized access to managing the information resources;

– deliberate negative information influence on the population via the mass media and the Internet information and telecommunication network;

– incomplete implementation of citizens' rights to obtain and exchange the true information, including manipulation with the public consciousness with the use of the information psychological pressure;

– provoking social, ethnic and religious tension through the activities of the specific (including electronic) mass media;

– increasing abuse in the credit and finance sphere associated with the penetration into computer systems and networks[1] [3].

In the conditions of such threats and risks, citizens need to have the public safety, public order and living environment safety improved, through increasing the efficiency in coordination of the activities of the powers and services responsible for solving these tasks.

Main Part

The tasks on neutralizing threats, minimizing risks and avoiding damage in the conditions of the information-oriented society need to be addressed through the introduction of a complex information system providing forecasting, monitoring, prevention and elimination of the possible threats. Information technology is necessary to control emergencies and offences and take remedial actions, with the integration of the operations of information managing subsystems of the emergency, monitoring and municipal services for their quick cooperation for the convenience of the municipality.

One of the main reasons for the urgent introduction of information technologies into the administrative and the law-enforcement activities is the information and technical character of modern crime. As law enforcement practice shows, every year there is an increase in the number of crimes in the sphere of computerized information and those committed with the use of computer technology, both groups of cries leaving digital footprints. This means that investigation and solution of cyber crimes can only be performed with the use of information technology by law enforcement agencies.

The necessity to develop and introduce information technology is related to the speed of decision-making. In the conditions of the dynamic economy, and with all the human activities [3] being based on information technology, any critical situation requires taking competent managerial decisions in the shortest time possible. Taking balanced decisions needs quick obtaining and analysis of all the information taken from all the sources available, which is impossible without well-developed automatized information search systems, automated data banks, analysis and alert services.

In addition to the mentioned reasons for the information technology implementation, it is necessary to name economic feasibility, the necessity to reduce the bureaucracy, improving the quality of state services, living standards and quality of life.

Both the named and unnamed reasons for the introduction of information technology set a task for law enforcement authorities and state/municipal power bodies to create a communication platform for avoiding and eliminating the risks to the public security and public order, and for creating the safe environment resting on the cooperation between different agencies. For this, it is necessary to determine the potential vulnerable points and to timely react to the threats arising in emergency.

The existing information threats and the necessity to adopt anti-terrorist measures made the Russian legislator to introduce changes into the legislation in July of 2016, which oblige communications service providers and the organizers of the information dissemination on the Internet to keep information of the users and pass it over to the authorized bodies. These changes caused heated

[1] On Approval of the Concept of the Development of the Hardware and Software Package "Safe City": Decree of the Government of the Russian Federation of December 3, 2014 No. 2446-r. *Collection of Legislative Acts of the Russian Federation*. 2014. No. 50. Art. 7220.

discussions in the society. The supporters explained their position by the necessity to struggle against terrorism. The opponents thought that it would lead to the interference with citizens' privacy.

The changed norms of the Russian legislation on countering terrorism[2], on security agencies[3], on communication[4], on information and information technology[5] and others oblige communications service providers to keep in the territory of the Russian Federation any information about the facts of receiving, sending, delivering and / or processing voice data, text messages, images, sounds, video-messages and other messages of the communications service users within 3 years after the completion of such actions.

Communications service providers and organizers of the information dissemination on the Internet are to pass this information over to the state bodies occupied with investigative activities or with ensuring the security of the Russian Federation. For the purpose of the unrestricted receipt of such information, a new investigative procedure was introduced into the legislation on investigation – namely, obtaining of computerized information[6].

In the sphere of law enforcement activities, it is planned to intensively develop the information managing systems, systems of processing and identification of fingerprint, genetic, ballistic and other criminally meaningful information as well as to improve the software and information support for the advanced modern automated management systems, and the information and reference activities for the benefit of the divisions of the Russian Ministry of Internal Affairs[7].

The current efficient information technologies aimed at providing security include video monitoring and video recording, in particular capturing, processing and transferring of the video-stream from cameras showing offenses and emergencies such as damage to utility systems, infrastructure and property. In such cases, analysis of the video- and audio-streams is performed, including automated registration of the events based on the video-stream analysis system, video analysis of the events, real-time video-stream investigation, face identification.

The unique opportunities of applying information technologies in law enforcement activities can be found in the positioning of movable objects (geolocation). Geolocation is determining coordinates of the real geographic location of any object[8]. Determination of the location (latitude and longitude) of an Internet user is performed using the radio signals from the global navigation satellite system GLONASS/GPS, the level signal at Wi-Fi access points, the Cell ID in the mobile service network, the computer IP-address. Geographic information systems are complex information systems created through the integration of the arrays of ordinary (usually factual) information about the objects of interest, with the arrays of geographic information (topographic maps, plans etc.). Geo-information systems of the Ministry of Internal Affairs are complex information systems created through the integration of data bases of ordinary information systems functioning in the divisions of the Ministry with the data bases of the corresponding cartographic information, for the purpose of providing information about specific objects demonstrably and in their spatial location on plans or maps.

The state takes actions to implement satellite tracking technologies for the purpose of developing geolocation and technological infrastructure of the system for the benefit of the state and other information systems which collect and process navigation information received from the vehicles equipped with the satellite navigation

[2] On Combating Terrorism: Federal Law of March 6, 2006 No. 35-FZ (as of July 6, 2016). *Collection of Legislative Acts of the Russian Federation*. 2006. No. 11. Art. 1146.

[3] On the Federal Security Service: Federal Law of April 3, 1995 No. 40-FZ (as of July 6, 2006). *Collection of Legislative Acts of the Russian Federation*. 1995. No. 46. Art. 1269.

[4] On Communication: Federal Law of July 7, 2003 No. 126-FZ (as of July 6, 2006). *Collection of Legislative Acts of the Russian Federation.* 2003. No. 52. Art. 2895.

[5] On Information, Information Technology and Information Protection: Federal Law of July 27, 2006 No. 149-FZ (as of July 6, 2016). *Collection of Legislative Acts of the Russian Federation.* 2006. No. 31. Pt. 1. Art. 3448.

[6] On Amendments to the Federal Law "On Combating Terrorism" and Specific Legislative Acts of the Russian Federation with regard to Establishing Additional Measures of Combating Terrorism and Ensuring Public Safety: Federal Law of July 6, 2016 No. 374-FZ. *Rossiyskaya Gazeta* – Russian Gazette. 2016. 8 July.

[7] On the Arrangement of Scientific Support and Application of Positive Experience in the Internal Affairs Bodies of the Russian Federation and Internal Military Forces of the Ministry of Internal Affairs of Russia: Decree of the Ministry of Internal Affairs of Russia of March 18, 2013 No. 150. Access from the reference legal system KonsultantPlus.

[8] On Approval of the Concept of the Development of the Hardware and Software Package "Safe City": Decree of the Government of the Russian Federation of December 3, 2014 No. 2446-r. *Collection of Legislative Acts of the Russian Federation*. 2014. No. 50. Art. 7220.

devices[9]. For this, there should be a communication platform or a unified information space created with the restricted access to the information of different nature, which will allow for the exchange of information between the participants of all the federal and municipal executive bodies in the sphere of ensuring safety[10].

In modern conditions, information technologies play a key role in the information support for the crime investigation. From the information perspective, information support is a unified system of collecting and receiving information from both external and internal sources, schemes of information streams circulating in the course of the crime investigation and solving, as well as the methodology of using the available databases and creating new ones.

Information support is a process with defined successive stages where the subjects influence the objects (information) in order to achieve specific results (purposes). The process of information support starts with obtaining the forensically meaningful information from its source or potential carrier.

All the potential carriers and sources of information about the crime and the criminal can be divided into three groups: homologous, objective and documentary ones. The group of homologous information sources and carriers includes alive people, dead bodies, parts of dead bodies, body fluid of alive people (blood, saliva, sperm etc.). The objective information carriers are weapons, ammunition and explosives, vehicles, different technical devices, clothes, footwear, everyday items etc. The group of documentary information carriers includes written documents, photos, films, videos, phonograms, graphic images, hardcopies etc. The information contained in these sources is the object of information support. Most of it becomes a basis for forensic and search accounting, and the objects themselves (ammunition, explosives etc.) may complement the prototype collections of expert forensic divisions.

New information technologies have enlarged not only the crime trace pattern but also the list of objects and documents subject to the criminal registration as evidences. Registration and long-term storage of the Internet traffic and all the phone connections, the tight linkage between a subscriber and the base station, as well as the technical capabilities of the modern computer equipment and database management systems allow for a quick processing of the vast amounts of billing and communication information and receiving data which can simplify the crime investigation process.

Modern information technologies and computerized databases make it possible to study personalities of all the individuals committing crimes, to quickly check all the proposed crime scenarios and to take a legitimate decision in the shortest time possible.

With this, one needs to bear in mind that there are several principal problems on the way of introducing information technologies [4]. The first problem is associated with the possibility of total control over a person's behavior. Thus, the legislator is to address this type of new threats and to prevent deterioration of the constitutional guarantees of the personal inviolability. The second problem is connected with the information security, with the possibility of disclosing personal data, theft of commercial, professional, business and state secrets. In the Russian criminal procedure legislation, there is a problem of using digital information as the evidence in criminal cases. This problem is caused by the criminal procedure form, which does not meet the challenges and requirements of the information society. The existing criminal procedure form prescribes the written arrangement of the evidence information in protocols of investigatory actions, which, due to the existing amounts of digital information, makes an investigator to perform laborious work on collecting the evidences. Only in July of 2016, the legislator

[9] On Approval of the Action Plan ("Roadmap") on Creation of the Open Stock Company GLONASS, Development of the State Automated Information System "ERA-GLONASS" and Its Use for the Benefit of Other Information Navigation Complexes and Systems Created by Federal Executive Power Bodies and Organizations: Order of the Government of the Russian Federation of August 9, 2014 No. 1498-r. *Collection of Legislative Acts of the Russian Federation.* 2014. No. 49. Art. 4693.

[10] On the Infrastructure Providing Information and Technological Interaction Between Information Systems Used for Rendering State and Municipal Services and Performing State and Municipal Functions in Digital Format: Regulation of the Government of the Russian Federation of June 8, 2011 No. 451 (as of 05.12.2014). *Collection of Legislative Acts of the Russian Federation.* 2011. No. 1. Art. 3503.

made some efforts (in our opinion, insufficient ones) to modernize the criminal procedural proving[11]. Taking into account the rapid development of information technology and the obsolete criminal procedure form, we have repeatedly highlighted the necessity to modernize the improvement of the criminal procedural proving in the dissertation [1, p. 454] and monograph researches [2, p. 352].

In addition, there are problems of disunity in work of different agencies, underfinancing of procurement and introduction of information technologies. The mentioned problems need to be addressed by all the concerned participants of information technologies, and for this new information legal relations should be established.

Conclusions

Taking into account the above mentioned, we can conclude that in the modern information society, in the conditions of escalating general and information threats, rise of computer-related crimes, and ubiquitous spread of artificial intelligence, the usage of information technologies in all the spheres of law enforcement, economic, and regulatory activities is a necessary, inevitable and most promising area of activity to ensure security of the individual, society and state.

For this, it is necessary to create a unified information environment providing an efficient and immediate cooperation of all the powers and services responsible for public safety and public order. In order to improve the efficiency of investigating and solving crimes, it is necessary to create integrated data banks of forensically meaningful information and to achieve a higher level of law enforcement bodies' computerization. The level of all the preliminary investigation bodies' being equipped with the telecommunications infrastructure and information resources should comply with the modern challenges and technical requirements. When introducing information technologies into all the spheres of the state and law enforcement activities, seeking security of society and the state, it is necessary to avoid excesses and disregard for the constitutional guarantees granted to an individual in the sphere of privacy.

The new structure of the information legal relations should take into account the existing information threats and risks, provide guarantees of a person's right to privacy, and ensure security of society and the state.

References

1. *Pastukhov P. S. Modernizatsiya ugolovno-protsessual'nogo dokazyvaniya v usloviyakh informatsionnogo obshchestva: dis. ... d-ra. yurid. nauk* [Modernization of Criminal Procedure Evidence in the Information Society: Dr. jurid. sci. diss.]. Moscow, 2015. 454 p. (In Russ.).
2. *Pastukhov P. S. Doktrinal'naya model' sovershenstvovaniya ugolovno-protsessual'nogo dokazyvaniya v usloviyakh informatsionnogo obshchestva: monografiya* [Doctrinal Model of Improvement of Criminal Procedure Evidence in the Information Society: monograph; ed. by P. S. Pastukhov]. Moscow, 2015. 352 p. (In Russ.).
3. *Losavio M., Pastukov P. and Polyakova S.* Cyber Black Box/Event Data Recorder: Legal and Ethical Perspectives and Challenges with Digital Forensics. *Journal of Digital Forensics, Security and Law.* 2016. Vol. 10. No. 4. Pp. 43–57. (In Eng.).
4. *Losavio M., Pastukhov P., Polyakova S.* Regulatory Aspects of Cloud Computing in Business Environments. In book: Cloud Technology: Concepts, Methodologies, Tools, and Applications. 2014. No. 1. Pp. 1373–1386. (In Eng.).

References in Russian

1. *Пастухов П. С.* Модернизация уголовно-процессуального доказывания в условиях информационного общества: дис. … д-ра юрид. наук. М., 2015. 454 с.
2. *Пастухов П. С.* Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества: монография. М.: Юрлитинформ, 2015. 352 с.
3. *Losavio M., Pastukhov P., Polyakova S.* Cyber Black Box/Event Data Recorder: Legal and Ethical Perspectives and Challenges with Digital Forensics // Journal of Digital Forensics, Security and Law. 2016. Vol. 10, № 4. P. 43–57.
4. *Losavio M., Pastukhov P., Polyakova S.* Regulatory aspects of cloud computing in business environments // Cloud Technology: Concepts, Methodologies, Tools and Applications. 2014. № 1. P. 1373–1386.

[11] On Amendments to the Federal Law "On Combating Terrorism" and Specific Legislative Acts of the Russian Federation with regard to Establishing Additional Measures of Combating Terrorism and Ensuring Public Safety: Federal Law of July 6, 2016 No. 374-FZ. *Rossiyskaya Gazeta* – Russian Gazette. 2016. 8 July.