National and International Issues of Cyber Security

Ekaterina Dolzhenkova¹*, Dmitriy Mokhorov¹ and Tatiana Baranova¹

¹Peter the Great St. Petersburg Polytechnic University, Saint Petersburg, Russia

*E-mail: skinx@inbox.lv

Abstract. Improving cyber security is the purpose of all states. Military-industrial complex is in need of creating innovative protection systems for their cyber space. A lack of such security systems can lead to the global disaster, using nuclear weapons. Today’s legal regulation of the national personal data still does not provide for legal regulation of user data which can be obtained via gadgets fitted with cameras, speakers, applications. Apart from information leakage as a result of hacker attacks, and accidental cyber leaks, the great problem is related to unlawful leakage and data stolen by company employees. Although the legislation of personal data protection is improving with allowance for precedents in this sphere leading to cybercrimes, an amount of unlawful use of personal data by company employees do not decrease due to a lack of accountability and behavior code in the sphere of personal data processing.

1. Introduction

The dramatic surge of digital technologies and approaches has a great impact on the society in general and every individual in particular. Legal issues caused by the development of digital technologies are covered in works of Voskresenskaya E.V. [1], Mokhorova A.Y. [2]. It is related to changes in the structure of business, healthcare and public sector. This raises the problem of confidentiality and personal data protection. It is worth noting the work by Kosarev S.Y. [3] about electronic signature as an instrument of theft. Patterson N. [4] proposed a model for detection of virtual property theft. In his publication Tebryaev A.A. [5] highlighted current types of terrorism expansion. In the 21st century national and regional security faces new security challenges. Apart from geopolitical problems there is the Umbrella Challenge [6], the hybrid-warfare and cyber-threats, which unites the planet at the moment. It is not enough for every state to have the armed forces and the intelligence service, the state is in need of resources to prevent cyber-threats and to protect its information space.

Information warfare can be considered as a communication technology, the main goal of which is to achieve information superiority in the interests of the national strategy. In addition, the information warfare can be regarded as public relations [7] with unauthorized work in other country’s cyberspace.
If to draw a parallel between geopolitical relations, the information warfare will set off when actors of the international process expect to achieve superiority in the economic, military, political, and other spheres by affecting intensely other cyberspace. The above-stated concepts characterize direction of the information effect. Initially information superiority or information warfare were used for military purpose and were targeted primarily at the military. Today’s world has undergone some changes in the area of digital technologies and approaches. At present information is targeted at the public opinion in this or that country. Digitalization of interaction and development processes requires to ensure complex cyber security.

In the current context information confrontation is considered along with armed struggle, political and diplomatic confrontation, economic competition, interstate rivalry in science and technology, where the targets of the information impact are top political and military Establishment, public opinion, information and telecommunication systems, communication means and systems of rival states, information resources, means of weapon and military equipment informatization, information systems of governmental bodies, banking and economic spheres. These issues are touched upon in the works by Geaza N. [8], Damenu T. [9], Jansen J. [10], Rajivan P. [11], Stewart H. [12], Addae J. [13], Yuryna Connolly L. [14], Schaab P. [15], Ray A. [16], Taheroost H. [17], Alavi R. [18], Pattinson M. [19], Kelley T. [20], Pipiros K. [21], Ilin I.V. [22], Bolsunovskaya M. [23], Kozlov O.A. [24], Qassim Q. [25], Herrmann A. [26], Raban Y. [27], Ani U. [28], Caron F. [29], von Solms B. [30], Renaud K. [31].

2. Methods

Using general scientific methods of analysis and synthesis, the authors study terms and concepts applied by international actors in the area of digital technologies and approaches. Unification of term bases – “information”, “cyber security”, “cyber space” – ensures consolidated understanding how NATO member states and Commonwealth of Independent States perceive their own and other cyber space, how they work in there, and how they interact.

The method of administrative and legal regulation allowed studying contemporary legislative mechanisms of modernizing management decisions in the area of digital technologies and approaches at the national and international levels of cyber space.

Using the method of discretionary protection and personification of information, the authors systematize and actualize particular definitions of security from the area of digital technologies and approaches, i.e. protection of national cyber space, commercial and social cyber space, personal data against leakage, unlawful use, and hacker attacks.

3. Materials

According to the data of NATO Cooperative Cyber Defense Centre of Excellence [32], the main threat in the sphere of international cyber security is usage of communication technologies as information weapons for political and military goals, violation of the international law, violation of national sovereignty, violation of state’s territorial integrity, threats to the global world, security and strategic stability; using information weapons for terrorist purpose, intervention into internal affairs of sovereign states in order to violate public order, to incite national, racial and religious hatred, to disseminate racial and xenophobic ideas, or theories that instigate violence; committing crimes related to unauthorized access to cyber information, to creation and expansion of malware.

Information is defined as any message or knowledge presentation, i.e. facts, data or opinions in the mass media in the text, numerical, graphic, cartographic, descriptive, or audiovisual forms. Relying on the definition given by Oxford university, information is all that can make human mind change opinions about the current state of the real world. In science and technology information is all that contributes to a decrease in uncertainty about the current state of the system.

Information supply provides for measures that protect, uphold information and information systems via ensuring their accessibility, integrity, authenticity, confidentiality and reliability. These measures include facilities for recovering information systems through protection, detection and response.
Cyber security definition accepted in the USA and Russia is the following: cyber security is a capacity of the cyberspace to withstand threats, and also a capacity to respond to threats and to recover. In Russia cyber security is defined as the state of protecting national interests in the cyberspace, determined by the balance between individual, public and national interests.

Cyberspace for both the USA and Russia is represented by any medium with information creation, where data are transmitted, received, stored, processed, or deleted. In Russia cyberspace is regarded as activity related to formation, creation, processing, transmission, usage, storage of information, which affects the information infrastructure, individual and public consciousness.

In the USA and Russian research, information warfare is interpreted as escalation of the information conflict between states, where information operations are implemented by state subjects in support of military and political goals. Russian definition implies that information warfare is confrontation between two or more governments in the cyberspace in order to damage systems, processes and resources essential for the counterparty. In addition, cyber weapons in the UN and the Russian Federation are defined as means and techniques used to damage cyber resources, processes and systems of other country; taking advantage of information to the detriment of other state’s defense, administrative, political, social, economic and other vital systems; using information as a means of mass manipulation in order to destabilize society and the state.

According to Stockholm International Peace Research Institute (SIPRI) [33] Yearbook 2019, there are 9 nuclear-armed countries which have approximately 13,865 nuclear weapons. Figure 1 presents country-wise weapon allocation (Figure 1).

The Information Society Report 2018 of the International Telecommunication Union [34] shows that the nuclear-armed countries which spend most on telecommunication development are the USA and China. There are no available data for Israel and North Korea. Among the nuclear-armed countries with territorial disputes most attention is drawn to India and Pakistan; the latter owns approximately 150 nuclear warheads, whereas India owns 140 nuclear warheads. With such a narrow gap in terms of the number of nuclear weapons, India’s annual spending on telecommunication development is $30 mln since 2014, Pakistan’s annual spending is a little over $4 mln (Figure 2).
Relying on the current legislation on cyber security and protection of cyberspace of the Russian Federation, it is worth noting the draft law known as the “sovereign internet law”, commonly referred to as “On Amendments to the Federal Law ‘On Communications’ and the Federal Law ‘On Information, Information Technology and Information Protection’” [35]. The explanatory note to the draft law mentions that the law reflects the US National Cyber Security Strategy adopted in 2018. In accordance with the US Cyber Security Strategy, Russia, along with some other states, conducted a number of cyber attacks without paying costs and being punished. Responding to the provisions fixed in the USA Cyber Security Strategy, the Russian Government recognize “the urgency of taking protective measures to ensure long-term sustainable operation of the Internet in Russia and improve the trustworthiness of Russian Internet resources”. The draft law claims that “Russia creates an opportunity to minimize dissemination abroad of information being exchanged by users within Russia…The amendments define communication lines crossing the Russian border, and Internet exchange points …Russian telecom firms would also have to install "technical means" to identify the source of the Russian Internet traffic…Russia creates infrastructure that would enable Russian sites to operate in the event that access to servers abroad is cut off or restricted”.

In September 2018, the State Duma approved the draft law, referred to as “On Amendments to Articles 7 and 28.5 of the Federal Law ‘on the Status of Military Servicepeople” [36]. The amendments propose to prohibit soldiers from internet posting any photos; videos; geotags, and other data which would reveal the nature of their activities; the activities of their military units and their position. The explanatory note states that resulting from the study of the Russian military forces, it has been revealed that “military servicemen are of particular interest to the security services of certain countries, terrorist and extremist organizations. Information posted by military servicemen on the Internet or mass media is used for information or psychological influence, as well, in particular cases, to form a biased assessment of the Russian Federation’s state policy”.

In June 2019, a draft law "On Amendments to Article 10-1 of the Federal Law "On Information, Information Technologies and Information Protection" was submitted to the State Duma [37]. In the explanatory note, which stated that in 2019, there was an increase in the number of "false threats of terrorist acts" sent to the e-mail addresses of state authorities. According to the draft law, in order to prevent such violations, "identification of e-mail users is proposed to be carried out using a subscriber number on the basis of an identification agreement concluded by the organizer of an e-mail service with a telecom operator."
Personal data protection is noted in the draft law "On Amendments to the Federal Law "On Information, Information Technologies and Information Protection" and Article 18 of the Federal Law "On Personal Data" [38]. The explanatory note mentions that "in order to protect the personal data of citizens of the Russian Federation the bill establishes the requirement that the technical means and databases of significant information resources should be located on the territory of the Russian Federation". The explanatory note to the draft Federal Law "On Amendments to Article 11 of the Federal Law "On Personal Data" [39] regarding the processing of biometric personal data" refers to biometric information. It is noted that "at present, there is a gap in the legislation of the Russian Federation in terms of protection of information about a person obtained from their biomaterial, which contains genetic information that allows to obtain additional information about them".

In addition to the gaps related to biomaterial, there are other problems that are still unregulated. There is still no legislation regulating user data that is collected by information systems and devices that allow for the identification of geolocation, identity, and social media behavior.

According to statistics from only one state in the United States between 2008 and 2009, 1 million people were affected by the leakage of personal information [40]. In 2010, personal data of 4.5 million people and foreign nationals were stolen in the UK [41]. In the same year, a Spanish bank [42] mistakenly sent the personal data of 35,000 customers to third parties. Vodafone [43] has also allowed the personal data of millions of customers to be leaked.

According to INFOWATCH [44], personal data leaks occur for various reasons. Leakage analysis has shown that leaks can be caused by the loss of a computer or data medium. Such leaks can be both malicious and accidental. The banking and medical sectors have suffered many times because of personal data leaks over the past twenty years. In the UK, a computer with 8.6 million medical records went missing in 2011. Such a situation could provoke blackmail based on available data. In India, there was a situation when the data of 120 thousand individuals who invested in infrastructure bonds of one company was published on the Internet. According to INFOWATCH, the average number of leaks per month in 2011 was about 70, and the average number of leaks per day was more than 2.

States are developing legislation that is capable of protecting personal data on the basis of the experience gained so far. For example, in 2012, South Korea [45] banned Internet companies from collecting and utilizing user passport data as well as telephone numbers and addresses. Restrictions also apply to storing information. Operators were required to delete data older than three years.

Information leakage concerns not only commercial organizations, but security organizations as well. The Pentagon [46] has repeatedly reported the loss and leakage of defense documents, e-mails containing classified information.

In addition to leakage of information to the Internet, there are cases when employees of organizations disclose personal information accidentally. In 2013, the situation in Vladivostok [47], when personal data of insured persons were posted at the Pension Fund as an example for questionnaires, resulted in violations of Law 152-FL "On Personal Data".

There are also cases of hacker attacks, which result in information theft. For example, in 2014, Chinese hackers [48] stole personal information from 4.5 million American patients. Regarding cyber attacks on the military segment, it is necessary to note the 2017 cyber attack [49] on the Ministry of Defense of Singapore. As a result of the cyber-attack, the data of 850 servicemen and civilian employees were stolen.

The analysis of confidential information leaks conducted by INFOWATCH [50] in 2016 showed that the number of leaks in the world increased by 3.4% compared to 2015, while in Russia the increase was 80%. The largest number of leaks were registered through the network channel. Also, the analysis allowed us to conclude that the number of accidental leaks of information when transmitting information over the network and publishing data on the Internet is growing. The USA and Russia shared the first and the second places in terms of information leaks. INFOWATCH also noted that "in countries where personal data in electronic form allow you to quickly and conveniently get public and other services, replace paper documents, there is a high probability that this data will be misused".
Regarding the data that can be obtained from devices equipped with video and audio elements, in 2017, WikiLeaks [51] published documents according to which the CIA can control webcams and microphones, including those connected via wireless network. The CIA itself also claimed in 2016 that it had a vulnerability in its own security system, which could be a source of information leakage.

In 2018, Facebook [52] disclosed that due to a software error, 14 million users' restricted data were made publicly available.

In 2018, the European Union adopted a law establishing principles and requirements for the protection of personal data - General Data Protection Regulation [53]. The law provides for increased liability for failure to comply with the rules of storage and processing of personal information, establishes global standards for data protection and regulates their cross-border transfer.

Cyber criminals also use messengers and mobile applications for manipulation and misinformation. Also, the threat to personal data is caused by employees who, when leaving the company, take away information to which they previously had access.

According to INFOWATCH [54] data for 2018, the main part of information leakage in Russia was personal data - 80.2%. Second place - 8.2% - commercial secret, third place - 6.2% - state secret, fourth place - 5.4% - payment information. General trends of information leakage by data type show that personal data is under threat in the world community. The main culprit is the employee, the second place is taken by an external malefactor.

4. Results and Discussion

National security agencies of states seek to develop the most effective methods to protect the state cyberspace from interference by outside international actors, terrorist groups, hackers, and others. Military action has gone beyond armed conflict. In today's world, success of an operation depends on the ability to conduct cyber warfare in one's own cyberspace, as well as in the cyberspace of one's enemy. In cyberspace, the influence of military personnel's personal information on national security has increased. This has led to the creation of a legal basis that restricts the activities of servicemen on the Internet.

With a single rise in productivity digital modifications are efficient, whereas in a long run it causes instability and ambiguity. Currently, it is rather complicated to estimate the value of introducing digital technologies, as they became in high demand not long ago. This does not allow monitoring dynamics, estimating risks, and making forecasts. The increasing demand for digital technologies leads to the rise in the demand for specialists who are able to work with digital technologies, consequently changing the demand for relevant educational programs. It is essential to integrate new educational programs and to modernize the existing ones in order to supply the labor market with specialists in the digital sphere for various industries.

In the commercial and social sector, the leakage of personal data entails the risk of blackmail and illicit enrichment through the use of personal data. Hacker attacks, which can cause millions of dollars in losses to companies and individuals, are a threat to cyber security and have a cross-border criminal nature. Information leaks related to personal information, such as personal photos, e-mails and medical data, are ethical in nature. Such situations can be detrimental to people's emotional health. Protection of personal data against hacker attacks is possible via improved security of commercial and social cyber space.

When considering threats to the security of all humankind, it is necessary to note the nuclear threat that may arise from the armed conflict of states, but may also arise because of terrorists. There is a risk that terrorist groups may seize a state's nuclear weapons and use them to commit a terrorist act. Armed protection of nuclear weapons cannot fully protect them from unauthorized use. The entire management system, including digital data, needs to be protected.

There is also a risk of an accidental armed collision that could lead to a nuclear war. Russia and the United States have been negotiating for five years to prevent such a situation. There are many factors that can lead to such a situation. But here, we are also talking about the information component of a possible situation. During the Cold War, there was already a situation that could lead to a nuclear war.
between the U.S. and the Soviet Union. In order to prevent the use of nuclear weapons, it is vital to set the UN negotiations targeted at cyber security of nuclear weapon control systems.

Introduction of artificial intelligence technologies into weapon systems, emergence of autonomous weapon systems increase the role of cyberspace and also expand the scope and dependence on digital data. The use of information technology can be regarded as either an advantage or vulnerability. The data sets that are used in the development of machine learning technologies can be subject to unauthorized use both within government agencies and by criminal influences from outside. These trends require simultaneous development of security systems capable of protecting both creation and development of information and protection against unauthorized use of the finished product.

5. Conclusion
Current problems of digital technologies and approaches are not only debatable, but of practical usage. One of the key issues to further development of digitalization processes is the issue of national and international cyber security, which is considered in this paper. Thus, to solve national and international problems in the current geopolitical conditions of the cyber warfare, the outcomes of the presented research urge to undertake the following:
1. to create an innovative technical mechanism of the UN control of a compulsory, rather than optional, type;
2. to improve the system of protecting personal data against hacker attacks and leakage via signing international treaties under the aegis of the UN;
3. to develop and to adopt legal restrictions, national and international liability for subjects of digital relations;
4. to develop artificial intelligence with allowance for the current digitalization reality;
5. to adopt programs of training artificial intelligence aimed at cyber security, and personal data protection;
6. to create a national and international digital learning environment in the framework of higher education, supplementary professional education, and specialized professional education.

References
[1] Voskresenskaya E V, Voronova-Slivinskaya L G and Loiko A N On legal nature of artificial intelligence results Colloquium-journal 5 – 6 7 – 8 (2019)
[2] Mokhorova A Y and Mokhorov D A The role of internet as a means of social communication in disrupting political subjectivity Eurasian Law Journal 3 (118) 364 – 36 (2018)
[3] Kosarev S Y Electronic signature as an instrument of theft Journal of St. Petersburg Law Academy 44 (29) 82 – 87 (2015)
[4] Patterson N, Hobbs M and Zhu T A cyber-threat analytic model for autonomous detection of virtual property theft Information and Computer Security 25 (4) 358 – 381 (2017)
[5] Bairamov S G Ogly, Vasilieva Y S and Tebryaev A A Terrorism threat assessment in today’s world Urgent problems of science and practice 3 (008) 36 – 40 (2017)
[6] Daugulis M The Challenges of Hybrid-Warfare and Cyber-Treats: The Role of Self-Defense in Changing Security Environment Towards Reassurance and Solidarity in the Euro-Atlantic Community 2015 151 – 156 (2015)
[7] Kunakova L N Information war as an object of scientific analysis (concepts and main features of the information war) Academic Journal of Science and Education 6 93 – 96 (2012)
[8] Geaza N, von Solms R, Grober M and van Vuuren J A general morphological analysis: delineating a cyber-security culture Information and Computer Security 25 (3) 259 – 278 (2017)
[9] Damenu T and Beaumont C Analysing information security in a bank using soft systems methodology Information and Computer Security 25 (3) 240 – 258 (2017)
[10] Jansen J and van Schaik P Comparing three models to explain precautionary online behavioural intentions Information and Computer Security 25 (2) 165 – 180 (2017)
[11] Rajivan P, Moriano P, Kelley T and Camp L Factors in an end user security expertise instrument Information and Computer Security 25 (2) 190 – 205 (2017)
[12] Stewart H and Jürjens J Information security management and the human aspect in organizations Information and Computer Security 25 (5) 494 – 534 (2017)
[13] Addae J, Brown M, Sun X, Towey D and Radenkovic M Measuring attitude towards personal data for adaptive cybersecurity Information and Computer Security 25 (5) 560 – 579 (2017)
[14] Yuryna Connolly L, Lang M, Gathegi J and Tygar D Organisational culture, procedural countermeasures, and employee security behaviour Information and Computer Security 25 (2) 118 – 136 (2017)
[15] Schaab P, Beckers K and Pape S Social engineering defence mechanisms and counteracting training strategies Information and Computer Security 25 (2) 206 – 222 (2017)
[16] Ray A and Kaushik A State transgression on electronic expression: is it for real? Information and Computer Security 25 (4) 382 – 401 (2017)
[17] Taherdoost H Understanding of e-service security dimensions and its effect on quality and intention to use Information and Computer Security 25 (5) 535 – 559 (2017)
[18] Alavi R, Islam S and Mouratidis H An information security risk-driven investment model for analysing human factors Information and Computer Security 24 (2) 205 – 227 (2016)
[19] Pattinson M, Parsons K, Butavicius M, McCorma A and Calic D Assessing information security attitudes: a comparison two studies Information and Computer Security 24 (2) 228 – 240 (2016)
[20] Kelley T and Bertenthal B Attention and past behaviour, not security knowledge, modulate users’ decisions to insecure websites Information and Computer Security 24 (2) 164 – 176 (2016)
[21] Pipyros K, Mitrou L, Gritzalis D and Apostolopoulos T Cyberoperations and international humanitarian law Information and Computer Security 24 (1) 38 – 52 (2016)
[22] Ilin I V, Levina A I and Lepekhin A A The complexity of requirements engineering approach as a potential critical-success factor of software project Proceedings of the 30th International Business Information Management Association Conference 2017 2578 – 2590 (2017)
[23] Bolsunovskaya M, Shirokova S, Loginova A and Uspehskij M Developing a procedure for conducting a security audit of a software package for predicting storage system failures MATEC Web of Conferences 245 10007 (2018)
[24] Kozlov O A, Rodionov D G and Guzikova L A Information security problems in educational institutions in conditions of network interaction International Conference on Information Networking 2018 267 – 269 (2018)
[25] Qassim Q, Jamil N, Daud M, Patel A and Ja’affar N A review of security assessment methodologies in industrial control Information and Computer Security 27 (1) 47 – 61 (2019)
[26] Herrmann A, Brenner W and Stadler R Cyber Security and Data privacy Autonomous Driving, Emerald Publishing Limited 2018, 141 – 149 (2018)
[27] Raban Y and Hauptman A Foresight of cyber security threat drivers and affecting technologies Foresight 20 (4) 353 – 363 (2018)
[28] Ani U, He H and Tiwari A Human factor security: evaluating the cyber security capacity of the industrial workforce Journal of Systems and Information Technology 21 (1) 2 – 35 (2019)
[29] Caron F Obtaining reasonable assurance of cyber resilience Managerial Auditing Journal (2019)
[30] von Solms B and von Solms R Cyber security and information security – what goes where? Information and Computer Security 26 (1) 2 – 9 (2018)
[31] Renaud K, Von Solms B and Von Solms R How does intellectual capital align with cyber security? Journal of Intellectual Capital 20 (5) 621 – 641 (2019)
[32] Lorents P, Ottis R and Rikk R Cyber Society and Cooperative Cyber Defence In Internationalization, Design and Global Development. Lecture Notes in Computer Science 5623 180-186 (2009)
[33] Modernization of world nuclear forces continues despite overall decrease in number of warheads: New SIPRI Yearbook out now SIPRI URL: https://www.sipri.org/media/press-
release/2019/modernization-world-nuclear-forces-continues-despite-overall-decrease-number-warheads-new-sipri (2019)
[34] Statistical reports: Measuring the Information Society Report. Volume 1. 2018 ITU URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf (2018)
[35] Draft law No. 608767-7. On Amendments to the Federal Law ‘On Communications’ and the Federal Law ‘On Information, Information Technology and Information Protection’ (2019)
[36] Draft law No. 546450-7. On Amendments to Articles 7 and 28.5 of the Federal Law ‘on the Status of Military Servicepeople’ (2019)
[37] Draft law No. 760029-7. On Amendments to Article 10-1 of the Federal Law "On Information, Information Technologies and Information Protection" (2019)
[38] Draft law No. 763517-7. On Amendments to the Federal Law "On Information, Information Technologies and Information Protection" and Article 18 of the Federal Law "On Personal Data" (2019)
[39] Draft law No. 744029-7. On Amendments to Article 11 of the Federal Law "On Personal Data" regarding the processing of biometric personal data (2019)
[40] Bray H Data breaches affect million state residents boston.com URL: http://archive.boston.com/business/technology/articles/2010/01/03/data_breaches_affect_million_state_residents/ (3 January 2010)
[41] Lewis J and White S For sale: Personal details of millions of Ladbrokes gamblers, offered to the MoS by a mysterious Australian dailymail URL: https://www.dailymail.co.uk/news/article-1245622/For-sale-Pgamblersersonal-details-millions-Ladbrokes-.html (24 January 2010)
[42] Anker G Santander sends thousands of statements to wrong addresses MoneySavingExpert.com URL: https://www.moneysavingexpert.com/news/2010/12/santander-sends-thousands-of-statements-to-wrong-addresses/ (22 December 2010)
[43] O'Brien N Mobile security outrage: private details accessible on net smh URL: https://www.smh.com.au/technology/mobile-security-outrage-private-details-accessible-on-net-20110108-19j9j.html (9 January 2011)
[44] Global data leakage survey 2011 INFOWATCH URL: https://www.infowatch.ru/resources/analytics/reports2583 (21 March 2012)
[45] Korea enacts stricter penalties for data protection violations INFOWATCH URL: https://www.infowatch.ru/resources/analytics/leaks-monitoring2743 (20 August 2012)
[46] Pentagon data leak – half a million Cuban prisoner messages open INFOWATCH URL: https://www.infowatch.ru/resources/analytics/leaks-monitoring3078 (18 April 2013)
[47] The Pension Fund in Vladivostok disclosed personal data ПИА НОВОСТИ URL: https://ria.ru/20131126/979686185.html (26 November 2013)
[48] Chinese hackers stole personal information from 4.5 million American patients INFOWATCH URL: https://www.infowatch.ru/resources/analytics/leaks-monitoring7394 (19 August 2014)
[49] Singapore defense ministry suffers data breach INFOWATCH URL: https://www.infowatch.ru/resources/analytics/leaks-monitoring17465 (16 March 2017)
[50] A study on global data leaks in 2016 INFOWATCH URL: https://www.infowatch.ru/resources/analytics/reports/report2016 (23 March 2017)
[51] WikiLeaks revealed a tracking instrument of CIA INFOWATCH URL: https://www.infowatch.ru/resources/analytics/leaks-monitoring18151 (14 August 2017)
[52] Facebook disclosed private messages of 14 mln subscribers INFOWATCH URL: https://www.infowatch.ru/resources/analytics/leaks-monitoring20473 (08 June 2018)
[53] GDPR EU GDPR.ORG URL: https://eugdpr.org/ (2019)
[54] Data leakage. Russia. 2018. INFOWATCH URL: https://www.infowatch.ru/resources/analytics/reports/russia2018 (30 May 2019)