Revista Jurídica

vol. 01, n°. 73, Curitiba, 2023. pp. 805 - 830

PROBLEMS OF LEGAL REGULATION OF THE RISKS OF USING ROBOTIC AND INFOCOMMUNICATION TECHNOLOGIES FROM THE POINT OF VIEW OF INFORMATION SECURITY

PROBLEMAS DE REGULAÇÃO JURÍDICA DOS RISCOS DO USO DE TECNOLOGIAS DE ROBÓTICA E INFOCOMUNICAÇÃO DO PONTO DE VISTA DA SEGURANÇA DA INFORMAÇÃO

Alexander Gurinovich
Moscow State Institute of International Relations (MGIMO University)
http://orcid.org/0000-0002-9232-3960
gurinovich.a.g@mail.ru

Marina Lapina
Financial University under the Government of the Russian Federation
http://orcid.org/0000-0003-0320-161X
m.a.lapina@bk.ru

Dmitry Kazantsev
Financial University under the Government of the Russian Federation
http://orcid.org/0000-0001-5650-9613
dmitry.a.kazantsev@yandex.ru

Andrey Lapin
Market Economy Institute (MEI RAS)
http://orcid.org/0000-0003-1937-315X
andrey.v.lapin@bk.ru

RESUMO

Objetivo: Este artigo examinou os problemas de regulamentação legal dos riscos decorrentes do uso de sistemas ciberfísicos, inteligência artificial, robôs e objetos robóticos. Atenção especial no artigo foi dada aos aspectos legais e essenciais da aplicação das tecnologias acima do ponto de vista da segurança da informação.

Metodologia: Os autores analisaram, do ponto de vista jurídico, as questões mais significativas relacionadas com a identificação, prevenção e minimização dos riscos decorrentes da utilização de sistemas ciberfísicos, tecnologias de inteligência artificial e robótica em diversas áreas das relações públicas.

Resultados: Os autores examinaram tanto a própria natureza do conceito de "risco" quanto sua interpretação normativa e legal. Também os autores estudaram as abordagens existentes para a classificação de riscos do uso dessas tecnologias do ponto de vista da comunidade científica e especialistas em segurança da informação.

Contribuição: Os autores fundamentaram a necessidade de regulamentação legal dos processos relacionados à identificação, prevenção e minimização dos riscos decorrentes do uso de sistemas ciberfísicos, tecnologias de inteligência artificial e tecnologias robóticas.

Palavras-chave: Regulamentação legal; Inteligência artificial; Sistemas ciber-físicos; Segurança da informação; Tecnologias de informação e infocomunicação.

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

ABSTRACT

Objective: This article examined the problems of legal regulation of risks arising from the use of cyber-physical systems, artificial intelligence, robots and robotics objects. Particular attention in the article was paid to the legal and essential aspects of the application of the above technologies from the point of view of information security.

Methodology: The authors analyzed, from a legal standpoint, the most significant issues related to the identification, prevention and minimization of risks that arise from using cyber-physical systems, artificial intelligence technologies and robotics in various areas of public relations.

Results: Authors examined both the very nature of "risk" as a concept and its regulatory and legal interpretation. Also authors studied the existing approaches to the classification of risks of using these technologies from the standpoint of the scientific community and information security experts.

Contribution: The authors substantiated the need for legal regulation of processes related to the identification, prevention and minimization of the risks that arise from using cyber-physical systems, artificial intelligence technologies and robotics technologies.

Keywords: Legal regulation; Artificial intelligence; Cyber-physical systems; Information security; Information and infocommunication technologies.

1 INTRODUCTION

In Russian legal literature, issues related to the risks of using cyber-physical systems, artificial intelligence, robots and robotics objects are rather poorly covered. In the monograph by P.M. Morhat "Artificial Intelligence: Legal View" the risks associated with the use of artificial intelligence technologies are disclosed most systemically (Morhat, 2017). There are a number of publications by other legal scholars who have touched on the problems of risks arising from operating artificial intelligence, robots and robotics objects in their studies. Among other things, I.V. Ponkin and A.I. Redkina also raised the issue of the main risks and uncertainties associated with artificial intelligence that are essential for legal regulation in the area under consideration (Ponkin, & Redkina, 2018a); in a collective monograph by A.V. Neznamov et al. the current trends of foreign legislation in regards to insuring against risks while operating robots and artificial intelligence technologies are covered.

Today in Russia quite significant changes in the economic structure are taking place due to the integration of multiple achievements in the development of digital technologies. Therefore, it would appear that studies of issues surrounding legal regulation of artificial intelligence, robots and objects of robotics in the Russian Federation are very promising (Ruchkina, 2020).

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

The topic of risks in the use of artificial intelligence and robotics objects has been repeatedly raised in foreign scientific literature, and consideration has been given to both broad theoretical issues of identifying and assessing risks in the process of using artificial intelligence and robots in various spheres of life, as well as more practical and narrow developments that can be in demand in applied activities for the creation and operation of specific robotic objects.

2 LITERATURE REVIEW

To analyze the risks of using modern robotic and infocommunication technologies, it is necessary to determine the conceptual apparatus.

The concepts of "cyber-physical systems" (hereinafter referred to as CPS), "artificial intelligence" (hereinafter referred to as AI) and "robot" have many definitions (for example, the Great Russian Encyclopedia of Artificial Intelligence defines it as “tasks traditionally solved by man” (Osipov, & Velichkovsky, 2022)). The conceptual apparatus is disclosed in most detail in the scientific legal literature in the works of P.M. Morhat (2017; 2018a; 2018b; 2019), as well as in a collective monograph by A.V. Neznamov et al. (2018).

Within the framework of this paper, we will adhere to the following terminology, which has been established in the legislation and in normative and technical documentation:

a) in the Federal Law of 24.04.2020 No. 123-FL "On conducting an experiment to establish special regulation in order to create the necessary conditions for the development and implementation of artificial intelligence technologies in the constituent entity of the Russian Federation – the city of federal significance Moscow and amendments to Articles 6 and 10 of the Federal Law "On Personal Data" "and in the Decree of the President of the Russian Federation of 10.10.2019 No. 490 "On the Development of Artificial Intelligence in the Russian Federation" AI is defined as "a set of technological solutions that are able to simulate human cognitive functions (including self-learning and finding solutions without algorithm) and obtain, when performing specific tasks, results comparable, at least, with the results of human intellectual activity. The complex of technological solutions includes information and communication infrastructure (including information systems, information and telecommunication networks, other technical means of information processing), software (including that which uses machine learning methods), processes and services for data processing and search for solutions";

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

in GOST R 43.0.8-2017 and GOST R 43.0.7-2011, AI is interpreted more succinctly as “simulated (artificially reproduced) intellectual activity of human thinking” (GOST, 2013; 2018);

b) in GOST R 60.0.0.4-2019 / ISO 8373:2012. National standard of the Russian Federation. Robots and robotic devices. Terms and Definitions. a robot is defined very specifically as "an actuator programmed in two or more degrees of mobility, possessing a certain degree of autonomy and capable of moving in the external environment in order to perform tasks as intended" (GOST, 2013). At the same time, in the specified GOST, when interpreting the concept of "robot", a reference is made to ISO / TC 299 "Robotics", according to which a new definition was given in 2018: "a robot is a programmable actuator with a certain level of autonomy for performing movement, manipulation or positioning" (GOST, 2019). In the same standard, the following concept is given: “**Robotics** – science and practice of development, production and application of robots” (GOST, 2019). The concept of "objects of robotics" is not enshrined in legal or technical norms. Based on the above concept of robotics, various classes and categories of robots and robotic systems can be classified as objects of robotics.

The term CPS (Cyber Physical Systems) has not yet been fully normatively or directly defined, but, as a rule, domestic (Chernyak, 2014; Kotenko, Parashchuk, & Saenko, 2017; Vatamanyuk, & Yakovlev, 2019) and foreign (Lee, & Seshia, 2016; Park, Zheng, & Liu, 2012) specialists in the field of information security under CPS mean a unified information technology environment that ensures the integration of computing resources into physical processes. It is a technical system in which computing elements and elements of physical nature are interconnected, serving as sources and consumers of information.

As you can see, these concepts differ significantly. So, on the basis of computer modeling, AI is defined very broadly, CFS combines infocommunication technologies with physical components, and the concept of a robot does not allow for covering a wide range of classes or categories of robots that have significant differences. Based on the above terms – CPS, AI and robots - it can be argued that approaches to identifying and assessing the risks of their use, including taking into account the requirements of information security, can be very different and have certain particular features, depending on the specifics of individual areas of their application.

Consequently, the general risks, taking into account the provision of information security, inherent in all types of CPS, AI, robots and robotics objects, and, accordingly, the possibilities of their legal regulation lie in the plane of regulatory legal acts in this area. The

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

direct risks of using certain types of CPS, AI and robots, for which it is necessary to develop different rules for assessing and managing risks for various classes of devices, should be specified in technical normative acts.

The Resolution of the European Parliament (2017) and the EU Ethics Guidelines for AI (European Commission, 2019) are important documents for the study of the risks of using AI technologies. One of the three basic principles of using AI is “do no harm”. It is these documents that should act as the basic legal foundation for the legal regulation of the risk-oriented approach to the use of modern robotic and infocommunication technologies.

In the Russian Federation, the problems of ensuring information security when using CFS, AI, robots and robotics objects by accounting, assessing and managing risks are reflected both in regulations of various levels (laws, presidential decrees, resolutions of the Government of the Russian Federation, departmental regulations), and in regulatory and technical documents (technical regulations, national standards).

Of course, for the successful functioning of robotic and infocommunication technologies, the risks arising from such activities must be taken into account (Lapina, 2015).

3 THE CONCEPT OF RISK

The etymology of the word "risk" (from French risque – "risk", Italian risico) comes from Old Greek ῥιζικόν – "cliff", Old Greek ῥίζα – “foot of the mountain”; "To take risks" – originally meant "to maneuver between the rocks" (Fasmer, 2022). Legal risk has been defined as “an objectively existing inherent probability in human activity of the subjects of legal relations incurring negative consequences due to the onset of unfavorable events, naturally associated with various prerequisites (risk factors) which, within certain limits, is capable of being assessed and voluntarily regulated” (Tikhomirova, 2018; Avdiyskiy, & Lapina, 2014).

The actively developing relational risk theory should also be noted. A. Boholm and H. Korvellek, revealing its essence, note that this theory deduces risks from located knowledge, which establishes risk relations in the context of certain unforeseen circumstances and a certain causal effect. The strength of relational theory, according to the authors' conception, is that it allows one to interpret the nature of risk; answer questions about what relates to risks and why, and also proposes new approaches to risk

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

management, as it raises the level of awareness of all stakeholders about them (Boholm, & Corvellec, 2011).

So, J.L. Head, considering the theoretical issues of corporate governance of all kinds of risks, focuses on the subjective factors of risk production. Different generations of corporate executives have different views of the same risk. This also applies to single individuals. The subjective views of managers at the corporate level can be critical in organizing the management of the realities of risk. A changing risk management strategy can dramatically change the actions of risk managers (Head, 2004).

Risk in the classical sense in any areas of human activity (without the use of CPS, AI or robots) is of a dual subject-object nature, therefore, the elements of risk are divided into objective (risk factors and situation) and subjective (subject and volitional regulation) "... As a rule, in civil law relations, “legal risk is the current or future risk of loss of income, capital or the occurrence of losses due to violations or non-compliance with internal and external legal norms, such as laws, bylaws of regulators, rules, regulations, prescriptions, constituent documents" (Avdiyskiy, & Lapina, 2014).

In the national standards of Russia, the terminology of risks is disclosed as follows. Clause 1.1 of the National Standard of the Russian Federation GOST R 51897-2011 / ISO Guide 73: 2009 dated 16.11.2011 “Risk management. Terms and definitions" (GOSTб 2012) and clause 3.1 of the National Standard of the Russian Federation GOSTR ISO 31000-2019 “Risk management. Principles and Guidelines” (GOST, 2020), define the concept of risk as “**the consequences of the influence of uncertainty on achieving the set goals**”, also giving the following explanations: “the consequences of the influence of uncertainty must be understood as a deviation from the expected result or event (positive and / or negative). Objectives can vary in content... and purpose (strategic, organizational, project-specific, product-specific, and process-specific). Risk is often characterized by describing a possible event and its consequences, or a combination of both. Risk is often expressed in terms of the consequences of a possible event (including changes in circumstances) and the probability associated with it. Uncertainty is a state of complete or partial absence of information necessary to understand an event, its consequences and their probabilities".

It should be noted that scientific literature conveys the view that the perception of the definition of risk in the context of uncertainty is not correct. In the work of Stephen Lee S. Ward and S. Chapman make the argument that the term "risk" to a greater extent reflects the prospect of a threat, and uncertainty has a broad semantic interpretation. The emphasis on uncertainty, according to the authors, will improve risk management during

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

project implementation, as it will provide an additional management resource for managing opportunities (Li, 2003).

Article 2 of the Federal Law of December 27, 2002 No. 184-FL (current ed.) "On technical regulation" defines the concept of risk as "the likelihood of causing harm to the life or health of citizens, property of individuals or legal entities, state or municipal property, the environment, the life or health of animals and plants, taking into account the severity of this harm."

The relationship between the concepts of risk and safety has been revealed by the authors of the commentary to the law: “even after all safety measures have been taken, some risk, usually referred to as residual, will always be present. This risk is considered acceptable, i.e. acceptable for each specific situation, taking into account existing social values (including economic, political factors, traditions) in a specific country and at a specific time” (Ageshkina, 2018). Of course, in assessing and managing risks when using CPS, AI, robots and robotics objects, the principle of risk tolerance will underlie legal regulation.

All these questions are very important in the context of the problems under consideration in modern conditions (see: (Gurinovich, Lapina, & Lapin, 2020; Aristov, & Kuznetsova, 2018; Ponkin, 2020; Kupriyanovsky, et al., 2020a; 2020b; Ponkin, et al., 2019; Khabrieva, & Chernogor, 2020)).

In the Russian Federation, a number of laws and subordinate normative legal acts contain norms that provide for the analysis, assessment, forecasting and minimization of risks in various areras of public relations.

At the same time, the basic regulatory legal act in terms of state risk management in the Russian Federation is Federal Law No. 172-FL dated June 28, 2014 “On Strategic Planning in the Russian Federation”. In addition to the aforementioned Federal Law, norms providing for the need for risk management can be found, albeit infrequently, in other regulatory legal acts – in the Civil Code of the Russian Federation, in the Criminal Code of the Russian Federation, in Federal Law No. 161-FL of June 27, 2011 “On the National Payment System".

The need to take into account risks in various areas, including strategic planning, is noted in the messages of the President of the Russian Federation (Putin, 2019). In the monograph by A.O. Turganbaev, it was concluded that Russia is technologically lagging behind in the implementation of the latest technologies in strategic planning from the states of the Anglo-Saxon legal system (Australia, Great Britain, Canada, the USA) and some

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

states of the Asia-Pacific region (China, Singapore, Thailand, South Korea, Japan) (Turganbaev, 2019). Only through the use of modern information and infocommunication technologies and artificial intelligence systems in strategic planning is it possible to achieve the main goal of the state - to improve the living conditions of people and increase the comfort of the living environment. However, many risks, challenges and problems, which will arise with the use of these technologies of the future need to be forecasted now.

4 RESULTS AND DISCUSSION

Risks of using cyber-physical systems (CPS)

Domestic scientists V.P. Kupriyanovskiy, D.E. Namiot, S.A. Sinyagov noted that modern CPS "integrate the cybernetic principle, computer hardware and software technologies, qualitatively new executive mechanisms built into their environment and capable of perceiving its changes, react to them, self-learn and adapt" (Kupriyanovskiy, Namiot, & Sinyagov, 2016). At the same time, an integral property of CPS is the connectivity of their physical components through infocommunication technologies (Friedberg, et al., 2017). CPS connect physical production processes or other processes with software and electronic systems (for example, a control system for the distribution of electricity), implemented through continuous control (Wolf, 2009). This is a distinctive feature of CPS and at the same time their weak point. The ability to remotely access physical components (equipment, cars, pacemakers) gives an attacker the opportunity to take control over them. Thus, there is a risk associated with the possibility of unauthorized access, interception and malicious modification of the process of managing the physical component.

For example, in 2009, malware Stuxnet disabled centrifuges at an Iranian uranium enrichment plant. As a result of the attack, the Iranian nuclear industry was pushed back several years. In 2019, Venezuela's energy system was attacked. Attackers gained control of the power management system in the Venezuelan capital and the control system of the Simón Bolivar hydroelectric power plant and remotely shut down the power grid. As a result of the attack, half of the country was left without electricity.

The risk of an intruder entering a cyber-physical system is not limited to damage to the economy and industry of the state. The death of a person can also be a consequence of an attack on the CPS. So, in experiments carried out in laboratory conditions, researchers have demonstrated the possibility of remote access to pacemakers and changing their mode of operation, as a result of which the person with the implant can die.

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

Experiments were also carried out to obtain remote access to the vehicle control system. Marin Ivezic, an information security expert, points to the difficulty of finding traces of such attacks. According to experts, criminologists investigating such incidents "most likely will not pay attention to the few traces left behind and consider the death to be accidental" (Ivezic, 2015).

So, the first criterion for classifying the risks of using CPS can be formulated as the risk of damage from unauthorized access to remote devices (physical components) and their potential malicious compromise.

The second criterion for classifying risks is often three well-known properties of information: confidentiality, integrity, availability (in the English nomenclature – "CIA").

According to the CIA criterion, risks are classified depending on the impact on the above properties of information:

- The risk of breaching the confidentiality of information in cyber-physical systems;
- The risk of violation of the integrity of information in cyber-physical systems;
- The risk of disrupting the availability of information in cyber-physical systems.

At the same time, it is emphasized, not without reason, that in cyber-physical systems the risks the integrity and availability of information pose the greatest danger (State Technical Commission of Russia, 2000; Burenin, & Legkov, 2015). For example, if an attacker gains access to the information contained in a pacemaker, he will be able to find out the rhythm of the heart, possible issues in its work, the daily schedule of a person. Although this information is personal data and is protected by law, the violation of its disclosure is not as dangerous as the violation of the integrity and availability of information in the pacemaker, which can lead to malfunctions in its operation or even to the destruction of the device, which can lead to very tragic consequences for that person. The classification of risks by the properties of information is rather arbitrary, since many threats affect several of the above properties of information at once.

In addition, experts in the field of information security agree that the generally accepted classification of risks by the properties of information is not exhaustive when using CPS. Thus, Hugh Boys, head of the cybersecurity department of the Institute of Engineering and Technology, identifies two more properties that are significant for CPS: manageability / control and utility (Boyes, 2015). In the event of a violation of controllability, the system operator, although able to detect a problem, will no longer be able to correct the situation. In case of violation of control over the system, the operator, even having the opportunity to influence the system, will not receive correct information about its state.

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

Paying attention to utility as a property of the cold air, Hugh Boys cites the loss of a spacecraft, the purpose of which was to collect climatic information about Mars, as an example. During its development, one project team implemented a system using metric units (km / h), while another group used imperial units (miles / h). As a result, the device entered the atmosphere of Mars incorrectly and was destroyed (Boyes, 2015).

The above risks can be confidently applied to robots and robotics objects, because robots are a type of CPS.

Risks of using robots and robotics objects

Despite the fact that robots can act autonomously to a certain extent, they still need communication channels with the operator. The ability of robots to operate completely autonomously may only appear after the AI technologies are integrated in them. But this move could bring even more risks from the use of robots than are currently out there. However, let's move on to considering robots as a type of CPS.

The most common classification of risks of using robots is the above-described **classification of risks when using CPS according to the properties of information**: confidentiality, integrity and availability. Analyzing the types of risks, information security experts and representatives of the scientific community focus on the possibility of losing the confidentiality of conversations and privacy as a result of using robots (ISBuzz Staff, 2017; Pagallo, 2013). Although the problem of information leakage is not the most dangerous for industrial robots and pacemakers, it is quite common for robots used for domestic purposes. In the home use of robots, when the failure of the machine does not lead to anything critical, except for feeling like money had been wasted, it is the risk of violating privacy that may pose the greatest threat. Thus, the president of the prpl Foundation, Art Swift, claims that robot manufacturers, rushing to enter the market with their model, often forget about ensuring the safety of their products, which can result in information leakage (ISBuzz Staff, 2017).

Manufacturers of industrial robots have not gone much further in terms of safety. A report by Trend Micro, a company specializing in information security, presents the results of a study of robots intended for industrial production from a number of well-known manufacturers for their information security (Maggi, et al., 2017). As a result of the study, experts came to the conclusion that all tested robots are vulnerable to external attacks. According to Dan Weber, CTO at Mocana: “One of the most disturbing findings in the Trend Micro report on vulnerabilities in manufacturing robots is how easy it is for hackers, in this

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

case “researchers”, to find unprotected industrial devices online" (Softpedia, 2017). It's alarming because it won’t be hard for perpetrators to access the company’s network, but even find its weak spots.

In addition to the classification of risks by information properties, there is also a **classification of risks by the types of attacks** that are possible with respect to robots:

- *Risk of an intent-modifying attack*. This is an attack aimed at corrupting the messages sent to the robot. It can pursue the goal of both changing the behavior of the robot and disabling it. This type of attack also includes the so-called Denial of Service attack. The point of this attack is that the robot is overloaded with incoming traffic. As a result, it either stops its work, or a delay in reaction to incoming commands

- *Risk of an intent manipulating attack.* This is an attack aimed at modifying messages sent from robots. The purpose of this attack is obvious - to distort information about the state of the machine.

- *Risk of an overhauling attack.* This is an attack in which an attacker completely takes control of the communication between a robot and its operator (Ishaani, 2017).

The above risk classifications have been formed exclusively through the prism of information security. This is justified for CPS and robots, which, according to the concepts given at the beginning of this work, are simply machines (or a set of machines) and pose a danger only in the event of their malfunctioning caused by an internal failure or external interference.

Such risks will be specific and will depend on the specific robotic device or the information and communication technology used in the CPS.

In the Russian Federation, a number of national standards have been adopted to establish requirements for the safety of operation of robots, taking into account the risk assessment of their use. For example, in "GOST R 60.1.2.1-2016 / ISO 10218-1: 2011. National standard of the Russian Federation. Robots and robotic devices. Safety requirements for industrial robots. Part 1. Robots" (GOST, 2016a) in Appendix A there is a table containing a list of significant hazards of robots and their subsystems, consisting of 10 types or groups of hazards (mechanical, electrical, thermal, ergonomic; hazards from noise, vibration, radiation, materials / substances; hazards associated with the environment in which the machine is used; combinations of hazards). To identify any hazards that may arise, a hazard analysis must be performed.

An overall risk assessment shall be performed for all hazards identified during hazard identification.

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

In "GOST R 60.2.2.1-2016 / ISO 13482: 2014. National standard of the Russian Federation. Robots and robotic devices. Safety requirements for robots for personal care" the list of significant dangers of robots intended for personal care contains 85 varieties. This standard provides for a general risk assessment, which includes not only hazard identification in order to identify any hazards that may arise for a particular personal care robot, but also a risk assessment. At the same time, a risk assessment should be performed for all hazards identified during the hazard identification process, “with particular attention to the different situations in which the personal care robot may come into contact with safety-related objects.”

After all structural safety and protection measures have been taken, the residual risk of the personal care robot must be assessed and it must be justified that this risk has been reduced to an acceptable level” (GOST, 2016b).

Thanks to the system of technical regulation (Lapin, 2018), it is possible to regulate the risks of using robots and robotics objects by the state in a timely and flexible manner.

The risks of using artificial intelligence (AI)

AI is a completely new entity, a substance, the mere use of which already raises many ethical, legal and technical problems. Unlike robots and cyber-physical systems, AI is able to independently make decisions and self-learn. The negative consequences of using AI can not only be the result of an outright mistake in its development, but even sometimes independent actions of AI, which the developers could not have predicted. In this regard, the use of AI itself can carry certain threats that should be considered. The need to assess and manage the potential risks of using AI systems, in particular, is stated by the Organization for Economic Cooperation and Development (OECD) (Raab, 2020).

As a rule, the risks of using AI are divided into general ones and those relating to information security.

In a report prepared by researchers at the University of Oxford, edited by Pierluigi Poganini, on the main threats to humanity, AI is among the 12 risks that can potentially destroy the human race (Paganini, 2015).

These risks are classified into 4 groups in the report:

- Current risks;
- External risks;
- Evolving risks;

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

- Global politics risks.

The researchers attributed global warming and the threat of nuclear war to the first. The possibility of a collision of the Earth with an asteroid is second. Researchers understand the risks of global politics as the risks associated with the global government. Developing risks included risks created by humans, such as synthetic biology or AI. In regards to AI, the report maintains the following view: “Artificial intelligence appears to have tremendous potential for purposeful work to destroy the human race. Although synthetic biology and nanotechnology, along with artificial intelligence, can be the answer to many existing problems, if used incorrectly, it can probably be the worst tool against humanity” (Paganini, 2015).

When analyzing the risks of using AI, one should clearly distinguish between the concepts of "strong artificial intelligence" and "weak artificial intelligence". Strong AI is intelligence, which, like a human, can solve various problems, think, adapt to new conditions (ISBuzz Staff, 2017). That is, in fact, intelligence capable of performing all the same functions that human intelligence performs. At the moment, such intelligence does not exist. There is only weak AI – intelligence capable of performing highly specialized tasks (Decree of the President of the Russian Federation of 10.10.2019 N 490).

These issues have already received sufficient coverage in the works of domestic authors (Ponkin, & Redkina, 2018a; 2018b).

According to experts from the Center for the Study of Existential Threats at the University of Cambridge, the creation of a "superintelligence" might be possible as soon as this century (University of Cambridge, 2021). With this in mind, experts of the Center have noted the highest risks associated with such AI. They have divided them into risks associated with accidents (safety risks), and risks associated with the abuse of AI (security risks). The former include the possibility of AI failure with all the ensuing catastrophic consequences (especially if the operation of critical infrastructure depends on the functioning of AI). The second group includes the threat of technology falling into the hands of "bad actors" in the international arena and the threat of a destabilizing arms race in the field of AI (University of Cambridge, 2021).

There is a lot to speculate about in terms of the risks of introducing strong AI, but it makes little practical sense, since these technologies are not currently available. Therefore, let's move on to the risks of using weak AI. Thus, experts talk about the possibility of manipulating public opinion by means of artificial intelligence (Marr, 2018). Media resources have long and successfully used stand-alone algorithms for targeted

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

marketing. But, if the AI knows how to select goods of interest to the user, it can also, using certain personal data, provide them with the necessary information in the form and format which they consider most reliable, thereby manipulating the user's perception.

The risk of manipulating public opinion stems from the risk of an invasion of the user's privacy by AI. The life of a modern person is already under constant supervision by various systems collecting and analyzing data, starting with targeted advertising services and ending with video surveillance cameras with which all major cities are equipped. AI, in turn, is an effective tool for analyzing all the information it collects. By accumulating information from several sources, artificial intelligence can quite accurately form a psychological and behavioral portrait of a person, determine his areas of interest, social circle, and much more. Collecting such information about a person can not only bring internal discomfort, but also certain negative material consequences. For instance, China has already introduced a social credit system, according to which each citizen is assigned a personal score based on their behavior. The system assesses the reliability of Chinese citizens according to various criteria, including whether they walk down the street, whether they buy Chinese goods, what they post on the Internet. People with high scores are eligible to receive discounts on electricity bills or better interest rates on deposits. Citizens with a low rating, on the contrary, are limited in their rights. For example, according to some reports, their access to high-speed Internet may be limited. According to CBS, nearly 11 million Chinese citizens won't be able to use airline services and 4 million – railway services due to this credit rating system. Therefore, this risk of using AI is noted as the **risk of discrimination** (Gianclaudio, & Jędrzej, 2020; Krupiy, 2020).

Experts also note the **risk of inconsistency in the goals of machines and people**. It means that commands in which a person puts a certain meaning can be interpreted in a completely different way by a machine. For example, the command "get me to the airport as quickly as possible" can have extremely negative consequences. If you do not clarify that you need to follow the rules of the road, since human life is more valuable than lost time, then AI can literally fulfill the instruction and leave behind a trail of accidents or collisions (Marr, 2018). When performing a given task, AI is able to cause harm that is not covered by the intent of the people who set the task, due to the fact that the conditions implied by such people by default can be ignored by artificial intelligence if it has been incorrectly trained or does not have special instructions for that particular matter (Čerka, Grigienė, & Sirbikytė, 2015).

AI can harm not only as a result of developers' flaws and misinterpretation of commands, but also as a result of certain external influences. In order to assess the danger

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

of such negative external influence on AI, let us turn to the risks of using AI from the perspective of information security.

At the same time, it is important to emphasize that AI is a tool, a means of achieving certain goals and, accordingly, it, like any other tool, can be used both for socially useful purposes and for criminal purposes. Information security experts expect that AI may appear in the arsenal of cybercriminals in the near future. David Capuano, the commercial director of BluVector, a cybersecurity solutions developer, also talks about this (Press, 2018). The expert warns of the danger of intruders carrying out more powerful and elusive attacks using AI technologies. According to D. Capuano, despite the fact that now technologies for carrying out attacks using AI are in their infancy, they will develop rapidly in the near future. This will be facilitated by the increase in the potential profit as a result of such attacks and the fact that there is a more active exchange of information and innovation between cybercriminals than between those who oppose them. Experts suggest that AI can be used when criminals carry out phishing attacks (that is, attacks aimed at deceiving a user, as a result of which they either transfer confidential information to an attacker or download malicious software onto their device). AI can help automate such attacks or simplify their implementation by, for instance, synthesizing a human voice (Seals, 2018). Attackers can also use AI to search for vulnerabilities and to automatically exploit those vulnerabilities. It is worth emphasizing that even now there are tools automating the above processes, however, in the case of using AI, the process of searching for vulnerabilities and their exploitation will take place on a completely different scale and at a completely different level. In the event of the malicious use of AI technologies, it is possible to spread botnets (computer networks consisting of devices infected with malicious software that allows these devices to be used for their own purposes) without a single control server. The fight against such botnets will become much more complicated, because the commonly used tactic of disabling the command and control server in relation to such botnets will be rendered ineffective. AI can also be used to coordinate the work of conventional botnets in an automatic mode, making it possible to significantly expand the scale of hacker attacks that use these botnets. According to experts in the field of information security, a serious threat is posed by the possibility of artificial intelligence creating new types of malicious software. AI, analyzing the shortcomings of human-created malware, is able to generate more advanced forms of it, making it much more difficult to detect and neutralize such programs (ISBuzz Staff, 2017).

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

In addition, by using AI to develop malware, cybercriminals can make it resistant to scanning by the AI that detects malware (Laurence, 2022).

Danger lies not only in the possibility of using AI technologies by attackers, but also the quite plausible use of AI-enabled software. According to Alex Smith, director of information security solutions at Intermedia, companies will face an increase in random security vulnerabilities and breaches of information security unrelated to hackers as a result of the proliferation of AI-powered products (Press, 2018). In particular, the expert notes that data sets on the basis of which the AI was trained may remain without protection. The disclosure of such information can have negative consequences, both for the company's image and for those whose information is contained in those breaches (especially if the samples are based on data from social networks).

In addition, AI-based software solutions have their own weaknesses and vulnerabilities. For example, researchers note the following highest risks in relation to such software solutions as a result of exploiting certain vulnerabilities in the artificial intelligence algorithm (National Academies of Sciences, Engineering, and Medicine, 2019, pp. 44-53):

1. *The risk of an attack by presenting specially crafted input data to distort the operation of an artificial intelligence algorithm*... The essence of this attack lies in the fact that the attacker, calculating the errors at the output of the algorithm in relation to the input data, can form the input data in order to obtain the result of interest at the output. For example, having formed the code of malicious software in a certain way, an attacker can ensure that the artificial intelligence verifying this code considers it trustworthy. This attack is possible due to the fact that the data sample on the basis of which the algorithm was trained is not comprehensive, and when receiving input data that were not contained in the training sample, the algorithm can produce a random result.

2. *Risk of breaching the confidentiality of training data*... An attacker, observing how the algorithm reacts to certain input data, can calculate the data on the basis of which the algorithm was trained.

3. *The risk of "spoiling" the training data.* In the case of access to data that is used to train artificial intelligence, an attacker can change it in such a way that the algorithm produces the result the attacker needs.

4. *Physical attack risk.* A physical attack means some kind of physical interference with the work of artificial intelligence, changes in the input data. As an example, the researchers cite an experiment where the object detection system had to recognize the "STOP" sign. In one case, the sign was not changed. In the second case, black and white rectangles were glued to the sign. As a result, in the first case, the algorithm easily

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

recognised the sign. In the second case, the system recognized it as a "Speed limit 45" sign. The algorithm was able to correctly identify the sign only when it got close to it – potentially too late to stop and avoid an accident.

5. *Risk of a false positive attack.* The essence of this attack is that the attacker generates a large number of bogus attacks designed to generate a large number of false positives. As a result, the defender will spend a lot of time and resources manually adjusting the system.

There is also the following classification of risks associated with the reliability of solutions that implement artificial intelligence algorithms (Paganini, 2015):

- *Risk of non-compliance*. This risk is associated with the fact that the artificial intelligence system develops during its existence. As a result of this development, the system may no longer meet the original design requirements.

- *Security risk*. It is possible if vulnerabilities in the artificial intelligence algorithm are exploited, as a result of which an attacker is able to manipulate the operation of the algorithm.

- *Risk of misbehavior*. The risk is associated with the fact that a system using artificial intelligence requires constant monitoring of the correct functioning and compliance with the requirements imposed on it at the design stage.

- *The risk of losing control*. It is possible if the mechanisms of human control of the work of the artificial intelligence algorithm are not well thought out or implemented.

- *Risk of reduced reliability*. It is related to the reliability of predictions made by artificial intelligence.

Thus, the risks of using modern robotic and infocommunication technologies have their own specificity, depending on the artificial intelligence technologies used and the robotics object (finished product). For further scientific research of legal regulation, it is important to analyze, take into account and classify the risks of using the above systems and technologies, including taking into account the requirements of information security.

It has been revealed that the highest risks of using CPS and robots from the point of view of information security are associated with the interception of control over them by an attacker or other disruption of their normal functioning. And given the fact that the results of a study of robots intended for industrial production from a number of well-known manufacturers for their information security have shown that all tested robots are vulnerable to an attack from the outside, the risk of control interception becomes even

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

more significant due to the consequences that can have such an interception. At the same time, the problem of information leaks is quite common for robots used for domestic purposes. And the risk of violating privacy in the future, given the rate of proliferation of robots used for domestic purposes, can also pose a serious hazard. Fig. 1 shows a classification scheme for the risks of using cyber-physical systems and the risks of using robots and robotics objects.

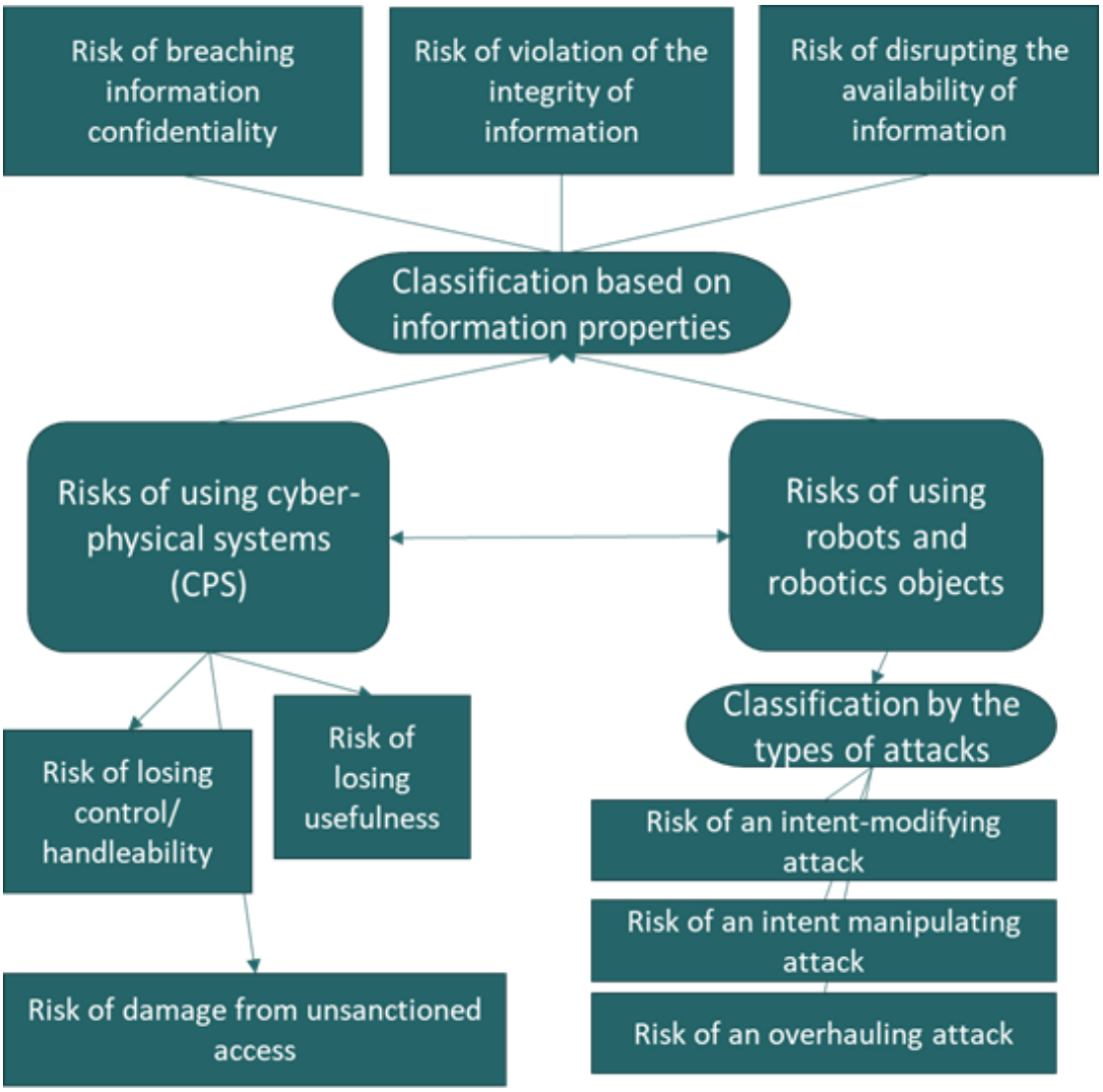

Figure 1. Classification of risks of using cyber-physical systems and risks of using robots and robotics objects

In the case of artificial intelligence, the risk system is somewhat more complex.

First, the risks of using artificial intelligence technologies by attackers are much higher (robots, for example, unmanned aerial vehicles, can also be used by criminals, but the danger from their use is incomparable with the scale of the threat that is possible if artificial intelligence is used for criminal purposes).

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

Secondly, artificial intelligence algorithms have the property of self-learning and modification in the course of their lifecycle, which also creates significant risks from the point of view of cybersecurity. If at the beginning of its work an artificial intelligence algorithm can meet the requirements of information security, then after a while it can move far away from them.

Thirdly, distortion of the work of the artificial intelligence algorithm is possible not only at the design, development and operation stages (as is the case with robots and cyber-physical systems), but also at the training stage, meaning that is another way to compromise a system using artificial intelligence.

Fourthly, additional risks are created by the very fact of training artificial intelligence on real, and often confidential, data that is protected by law, as a result of which there is a threat of their compromise. On the other hand, in the case of artificial intelligence, the risks of impact on the system at the time of its operation (i.e. at the end of development and training) are significantly reduced compared to cyber-physical systems, which greatly complicates attacks on it from the outside.

Fig. 2 shows the classification of the risks of using artificial intelligence.

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

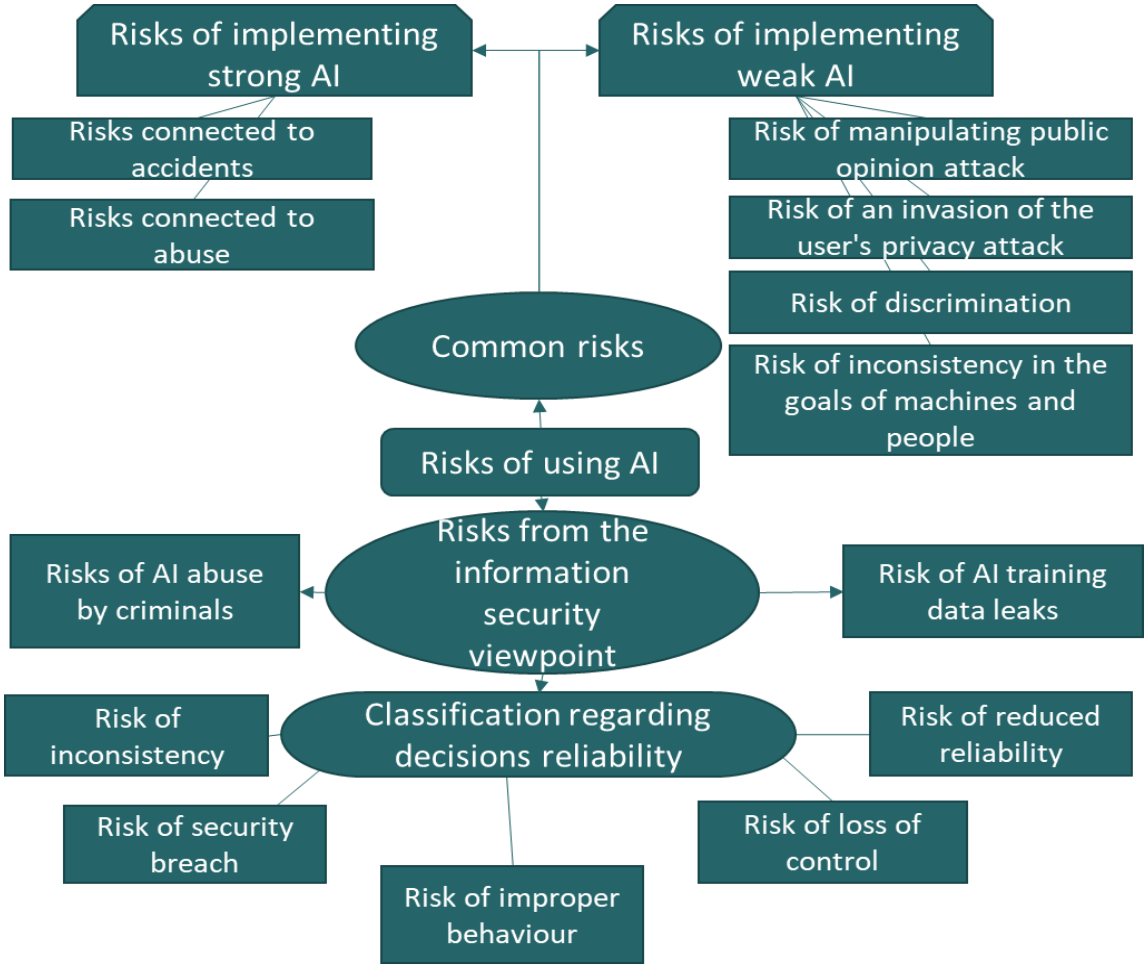

Figure 2. Classification of risks of using artificial intelligence

Summarizing the various types of risks, taking into account the requirements of information security, we propose to classify them from the standpoint of legal regulation, grouping them into general and special ones. A diagram of the types of risks from the standpoint of their legal regulation is shown in Fig. 3.

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

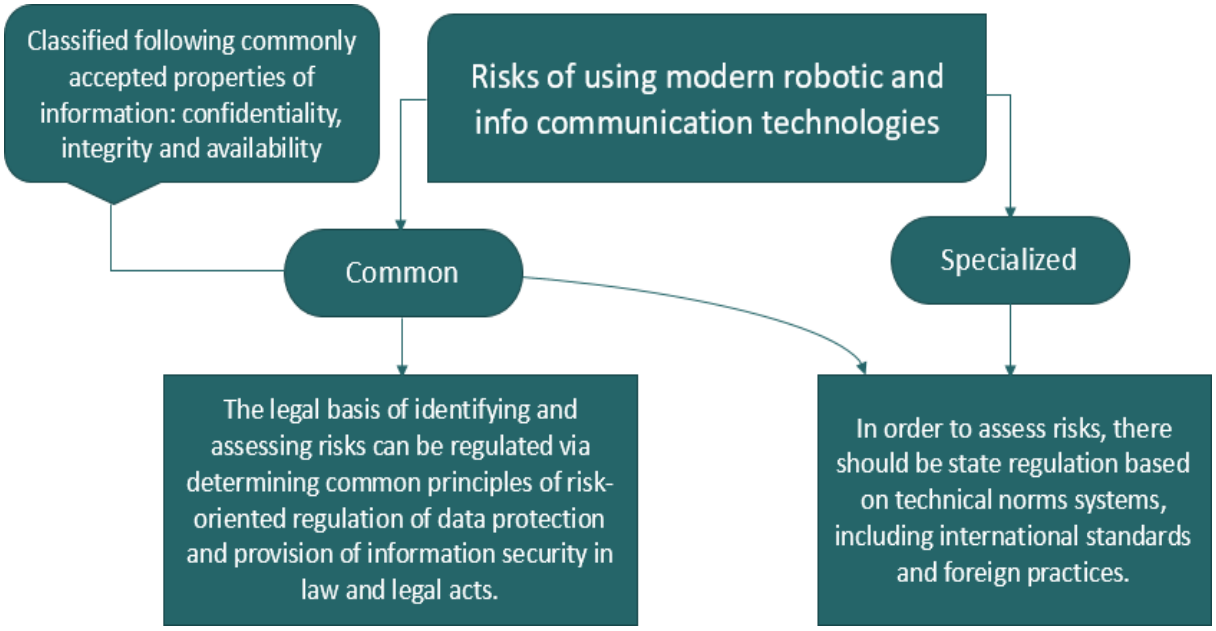

Figure 3. Types of risks of using modern robotic and infocommunication technologies

General risks are classified according to the known and generally accepted properties of information: confidentiality, integrity and availability. The legal basis for their identification, assessment, management and, if necessary, minimization should be contained in legislation and by-laws.

To assess the special risks of using CPS, AI, robots and robotics objects and establish mandatory requirements for their operation, state regulation should be made using a system of technical regulation, including on the basis of international standards and best foreign practices. Thanks to the system of technical regulation, it is possible timely and flexibly regulate the risks of using modern robotic and infocommunication technologies on the part of the state in a timely and flexible manner.

6 CONCLUSION

It has been revealed that conceptual approaches to defining risks are different. The term "risk" should be considered not only as a consequence of the influence of uncertainty on achieving the goal and, accordingly, obtaining a result with a deviation from the expected, but also as an additional resource for managing opportunities.

The risks of using modern robotic and infocommunication technologies have their own specifics, depending on the AI technologies used and the robotics object (finished product). It is proved that in the basis of the legal regulation of risk assessment and

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

management when using robotic and infocommunication technologies should be the principle of risk acceptability, which means for each specific situation an acceptable risk that remains, taking all security measures when using cyber physical systems (CPS), artificial intelligence (AI), robots and objects of robotics.

Authors have proposed a concept for classifying risk into common and specialised ones based on the principle of risk tolerance taking into account information security requirements.

REFERENCES

Ageshkina, N. A. (2018). *Commentary to the Federal Law of December 27, 2002 N 184-FZ "On Technical Regulation" (itemized)*. Saratov: Ay Pi Er Media.

Aristov, E. V., & Kuznetsova, O. A. (2018). On the formation and development of the law of robots (legal regulation of robotics). *Science and education: household and economy; entrepreneurship; law and governance, 8*(99), 58–62.

Avdiyskiy, V. I., & Lapina, M. A. (eds.). (2014). *Legal risks in the public administration system*. Moscow: OT i DO.

Boholm, A., & Corvellec, H. (2011). A relational theory of risk. Journal of Risk Research, 14(2), 175-190. https://doi.org/10.1080/13669877.2010.515313

Boyes, H. (2015, May). *Cyber security attributes for critical infrastructure systems*. Cyber Security Review https://www.cybersecurity-review.com/articles/cyber-security-attributes-for-critical-infrastructure-systems

Burenin, A. N., & Legkov, K. E. (2015). Security issues of infocommunication systems and special-purpose networks: main threats, methods and means of ensuring integrated network security. *Science-intensive technologies in space research of the Earth*, (3), 46–61.

Čerka, P., Grigienė, J., & Sirbikytė, G. (2015). Liability for damages caused by artificial intelligence. *Computer Law & Security Review, 31*(3), 376-389. https://doi.org/10.1016/j.clsr.2015.03.008

Chernyak, L. V. (2014). Cyber-physical systems at the start. *Open systems. DBMS*, (2), 10-11.

European Commission (2019, 08 April). *Ethics guidelines for trustworthy AI*. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

European Parliament (2017, 16 February). *European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL)).* https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html

Fasmer, M. (2022). *Risk*. The etymological online dictionary of the Russian language by Max Fasmer. https://vasmer.lexicography.online/р/риск

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2017). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications, 33*, 183-196.

Gianclaudio, M., & Jędrzej, N. (2020). Vulnerable data subjects. *Computer Law & Security Review, 37*. https://doi.org/10.1016/j.clsr.2020.105415

GOST (2012). *GOST R 51897-2011 / ISO Guide 73: 2009. National standard of the Russian Federation. "Risk management. Terms and definitions"* (approved and put into effect by the Order of Rosstandart dated November 16, 2011 N 548-st). Moscow: Standartinform.

GOST (2013). *GOST R 43.0.7-2011 "Information support for equipment and operator activities. Hybrid-intellectualized human-informational interaction. General Provisions" (*approved and put into effect by Rosstandart Order No. 1242-st of 13.12.2011). Moscow: Standartinform.

GOST (2016a). *GOST R 60.1.2.1-2016 / ISO 10218-1: 2011. National standard of the Russian Federation. Robots and robotic devices. Safety requirements for industrial robots. Part 1: Robots* (approved and put into effect by the Order of Rosstandart dated 08.11.2016 N 1624-st). Moscow: Standartinform.

GOST (2016b). *GOST R 60.2.2.1-2016 / ISO 13482: 2014. National standard of the Russian Federation. Robots and robotic devices. Safety requirements for robots for personal care* (approved and put into effect by Order of Rosstandart dated November 24, 2016 No. 1756-st). Moscow: Standartinform.

GOST (2018). *GOST R 43.0.8-2017. National standard of the Russian Federation. Information support for technology and operator activities. Artificially intellectualized human-informational interaction. General Provisions*. (approved and put into effect by the Order of Rosstandart dated July 27, 2017 No. 757-st). Moscow: Standartinform.

GOST (2019). *GOST R 60.0.0.4-2019 / ISO 8373: 2012. National standard of the Russian Federation. Robots and robotic devices. Terms and definitions*" (approved and put into effect by the Order of Rosstandart dated February 14, 2019 No. 31-st). Moscow: Standartinform.

GOST (2020). *GOST R ISO 31000-2019 "Risk management. Principles and Guidelines"* (approved and put into effect by the Order of the Federal Agency for Technical Regulation and Metrology of 10.12.2019 N 1379-st). Moscow: Standartinform.

Gurinovich, A. G., Lapina, M. A., & Lapin, A. V. (2020). Administrative and legal aspects of management risks in the economic sphere. *Revista Quaestio Iuris, 13*(3), 1325-1347. http://doi.org/10.12957/rqi.2020.55749

Guerra, P. C., Nöth, W., & Knoerr, V. C. de S. (2023). Empowering the Battle Against COVID-19: Exploring the Impact of Artificial Intelligence Solutions. ESG Law Review, 6(1), e01576. Retrieved from https://esglawreview.org/convergencias/article/view/1576

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

Head, G. L. (2004). The duality of risk. *Risk Management, 51*(1), 20.

ISBuzz Staff (2017, 03 March). *Severe Security Vulnerabilities in Home, Business and Industrial Robots*. ISBuzz News. https://www.informationsecuritybuzz.com/articles/severe-security-vulnerabilities-home-business-industrial-robots/

ISBuzz Staff (2017, 21 September). *Artificial Intelligence Can Drive Ransomware Attacks*. ISBuzz News. https://www.informationsecuritybuzz.com/articles/artificial-intelligence-can-drive-ransomware-attacks

Ishaani, P. (2017). Cyber security risks in Robotics. In: *Detecting and Mitigating Robotic Cyber Security Risks* (pp. 333-348) http://doi.org/10.4018/978-1-5225-2154-9.ch022

Ivezic, M. (2015, 31 March). *The World of Cyber-Physical Systems & the Rising Cyber-Kinetic Risks*. 5G.Security. https://5g.security/cyber-kinetic/cyber-kinetic-risks/

Khabrieva, T. Ya., & Chernogor, N. N. (2020). *The future is right. The legacy of academician V.S. Stepin and legal science*. Moscow: Russian Academy of Sciences; Institute of Legislation and Comparative Law under the Government of the Russian Federation; INFRAM.

Kotenko, I., Parashchuk, I. B., & Saenko, I. B. (2017). Information security of cyber-physical systems: the main directions of research. *Proceedings of the III interregional scientific and practical conference «Perspective directions of development of domestic information technologies»* (pp. 63–65). Moscow.

Krupiy, T. (2020). A vulnerability analysis: Theorising the impact of artificial intelligence decision-making processes on individuals, society and human diversity from a social justice perspective. *Computer Law & Security Review, 38*. https://doi.org/10.1016/j.clsr.2020.105429

Kupriyanovskiy, V. P., Namiot, D. E., & Sinyagov, S. A. (2016). Cyber-physical systems as the basis of the digital economy. *International Journal of Open Information Technologies, 4*(2), 18–25.

Kupriyanovsky, V. P., Klimov, A. A., Voropaev, Yu. N., Ponkin, I. V., Pokusaev, O. N., Dobrynin, A. P., & Lysogorskiy, A. A. (2020a). Digital twins based on the development of BIM technologies, connected by ontologies, 5G, IoT and mixed reality for use in infrastructure projects and IFRABIM. *International Journal of Open Information Technologies, 8*(3), 55–74.

Kupriyanovsky, V. P., Ponkin, I. V., Moreva, S. L., & Ponkin, D. I. (2020b). Disruptive technological innovation: concept, meaning and ontology. *International Journal of Open Information Technologies, 8*(8), 60–68.

Lapin, A. V. (2018). Improving the system of technical regulation as a prerequisite for the state industrial policy of growth. *Administrative and municipal law*, (10), 43–51.

Lapina, M. A. (2015). Theoretical and legal aspects of risk management. *State and Law*, (2), 35–44.

Laurence, A. (2022). *The Impact of Artificial Intelligence on Cyber Security*. CPO

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

Magazine. https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/

Lee, E. A., & Seshia, S. A. (2016). *Introduction to embedded systems: A cyber-physical systems approach*. London: MIT Press Publ.

Li, S. (2003). Future trends and challenges of financial risk management in the digital economy. *Managerial Finance, 29*(5-6), 111-125. https://doi.org/10.1108/03074350310768797

Luz, E. H. da, Belli , R. F., & Santos , R. C. dos. (2023). Green management: the sustainability's path of no return in organizations . ESG Law Review, 6(1), e01571. Retrieved from https://esglawreview.org/convergencias/article/view/1574

Maggi, F., Quarta, D., Pogliani, M., Polino, M., Zanchettin, A. M., & di Milano, S. Z. P. (2017). *Rogue Robots: Testing the Limits of an Industrial Robot's Security*. https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf

Marr, B. (2018, 19 November). *Is Artificial Intelligence Dangerous? 6 AI Risks Everyone Should Know About*. Forbes. https://www.forbes.com/sites/bernardmarr/2018/11/19/is-artificial-intelligence-dangerous-6-ai-risks-everyone-should-know-about/

Morhat, P. M. (2017). *Artificial Intelligence: Legal View*. Moscow: Buki Vedi.

Morhat, P. M. (2018a). *Law and Artificial Intelligence*. Moscow: Unity-Dana.

Morhat, P. M. (2018b). *Legal personality of artificial intelligence units*. *Civil law research*. Moscow: Unity-Dana.

Morhat, P. M. (2019). *Law and Artificial Intelligence: Thesaurus*. Moscow: Buki Vedi.

National Academies of Sciences, Engineering, and Medicine (2019). *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*. Washington (DC): The National Academies Press. https://doi.org/10.17226/25488

Neznamov, A.V., Arkhipov, V.V., Bakumenko, V.V., & Volynets, A.D. (2018). *Regulation of robotics: an introduction to "robo-law". Legal aspects of the development of robotics and artificial intelligence technologies*. Moscow: Infotropic Media.

Osipov, G. S., & Velichkovsky, B. M. (2022). *Artificial intelligence*. https://bigenc.ru/mathematics/text/2022537

Pagallo, U. (2013). Robots in the cloud with privacy: A new threat to data protection? *Computer Law & Security Review, 29*(5), 501-508. https://doi.org/10.1016/j.clsr.2013.07.012

Paganini, P. (2015, 24 February). *Cybersecurity and Artificial Intelligence: A Dangerous Mix*. Infosec. https://resources.infosecinstitute.com/cybersecurity-artificial-intelligence-dangerous-mix/

Park, K.-J., Zheng, R., & Liu, X. (2012). Cyber-physical Systems. Milestones and Research Challenges. *Editorial Computer Communications, 36*(1), 1-7. http://doi.org/10.1016/j.comcom.2012.09.006

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

Ponkin, I. V. (2020). The concept of machine-readable and machine-executable law: relevance, purpose, place in RegTech, content, ontology and prospects. *International Journal of Open Information Technologies, 8*(9), 59–69.

Ponkin, I. V., & Redkina, A. I. (2018a). Artificial Intelligence from the Point of View of Law. *RUDN Journal of Law, 22*(1), 91-109. https://doi.org/10.22363/2313-2337-2018-22-1-91-109

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]

Ponkin, I. V., & Redkina, A. I. (2018b). Artificial Intelligence and Intellectual Property Law. *Intellectual Property. Copyright and related rights*, (2), 35–44.

Ponkin, I. V., Kupriyanovskiy, V. P., Redkina, A. I., Semenova, E. M., Ponkin, D. I., & Grinko, O. V. (2019). On the question of the content of the concept and features of the ontology of the energy Internet and its legal and technological images. *International Journal of Open Information Technologies, 7*(8), 87–93.

Press, G. (2018, 03 December). *Cybersecurity Predictions for 2019*. Forbes. https://www.forbes.com/sites/gilpress/2018/12/03/60-cybersecurity-predictions-for-2019/

Putin, V. V. (2019). *Message of the President of the Russian Federation to the Federal Assembly of 02/20/2019*. Rossiyskaya Gazeta, no. 38.

Raab, Ch. D. (2020). Information privacy, impact assessment, and the place of ethics. *Computer Law & Security Review, 37*. https://doi.org/10.1016/j.clsr.2020.105404

Ruchkina, G. F. (2020). Artificial intelligence, robots and robotics objects: on the theory of legal regulation in the Russian Federation. *Banking Law*, (1), 7–18.

Seals, T. (2018, 03 October). *Artificial Intelligence: A Cybersecurity Tool for Good, and Sometimes Bad*. Threatpost. https://threatpost.com/artificial-intelligence-a-cybersecurity-tool-for-good-and-sometimes-bad/137831/

Softpedia (2017, 03 May). *Factory Robots Are Easy to Hack, Researchers Show*. https://news.softpedia.com/news/factory-robots-are-easy-to-hack-researchers-show-515411.shtml

State Technical Commission of Russia (2000). *Protection against unauthorized access to information. Part 1: Information security software. Classification according to the level of control of the absence of undeclared opportunities: Guidance document*. Moscow.

Tikhomirova, Yu. A. (ed.) (2018). *Legal administration in economics*. Moscow: Justice.

Turganbaev, A. O. (2019). *Administrative and legal support and implementation of strategic planning in public administration*. Moscow: Buki Vedi.

University of Cambridge (2021). *Risks from Artificial Intelligence*. https://www.cser.ac.uk/research/risks-from-artificial-intelligence/

Vatamanyuk, I. V., & Yakovlev, R. N. (2019). Generalized theoretical models of cyber-physical systems. *News of the South-West State University, 23*(6), 161-175.

Wolf, W. (2009). Cyber-physical systems. *Computer, 42*(3), 88-89. https://doi.org/10.1109/MC.2009.81

[Received/Recebido: Dezembro 03, 2022; Accepted/Aceito: Fevereiro 09 2023]