Problems of structuring risks and ensuring legal relations in IoT

I. Introduction

Modern advances in information technology, designated as the Internet of Things by popular belief the recommendations formulated so far on global technical and technological development of society, presented, in particular, as the Digital Economy of the Russian Federation and Industry 4.0 programs (Germany) [1,2,3].

The first program initially defined goals and objectives within the framework of 5 basic directions of development of the digital economy in the Russian Federation for the period up to 2024. The basic areas were: regulation, personnel and education, the formation of research competencies and technical reserves, information infrastructure and information security.

At the same time, the dynamism of digital technology changes and their impact on society turned out to be so great that the government had to reconsider in a short time the approaches to the implementation of such a program. First of all, the management system of such a program was restructured [4]. This once again underlines the need for a comprehensive and detailed study of the methods, techniques and solutions of the digital economy. An important role here is played by the risk analysis of the intellectualization of equipment in all areas of its application. Two recent disasters with Boeing 737 MAX aircraft reminded us of this once again [5].

The main areas of the second program are “Integrated Systems Management”, “Resource Efficiency”, “Education and Advanced Training”, “Standardization and the creation of a reference architecture” [2, 3]. In 2015-2017, additional recommendations were published on smart services - Smart Service Welt 2025 and Smart Service Welt II. [6,7].

Representing the undoubted perspective of new technical solutions of this direction, it is necessary to take into account that locally working machines, devices, equipment or their combination perform their functions under the control and control of people who can take control and find an acceptable way out in case of non-standard situations. For this purpose - training, internships, retraining, and advanced training are organized in each professional field (environment). In other
words, there are systems that ensure not only adequate control, but also minimization of equipment activity risks. Obviously, an increase in conglomerates, automatically working and interacting devices, especially self-decision makers, provokes increased risks of possible consequences of using incorrect or inaccurate models, formalization procedures, the presence of algorithmic errors and inaccuracies, programming errors and, accordingly, incorrect functioning of technical devices, processing or data transfer. Disasters with Boeing showed that even the presence of people who understand the unusual situation does not provide a way out of the threatening situation, due to the imperfection of the interfaces between the interaction of software, intellectual equipment and man. It can be said that in this case the first law of Azimov's robotics was unobviously violated.

Thus, errors and inaccuracies, in the first place, of algorithms can significantly affect the correct flow of implemented technological processes, business processes and processes of human existence as a whole.

The basic ideological setup of the Internet of Things is the integration of local devices that perform various actions into some conglomerates with the expansion of sensory, functionality, quality and properties. All this is accompanied by an increase in the volume of data received and the exchange of information both within the conglomerate and with the external environment. Moreover, a corresponding increase in the intelligence of actions and decisions is carried out without or with minimal human participation. Without a doubt, a person’s withdrawal from the sphere of control of actions, decision-making, prediction of consequences, comparison of the results obtained with target values ultimately changes the forms, formats and the very essence of the relationship between a person and the technical means that implement these functions. At the same time, zones of formation and occurrence of risks of different nature and situationality appear and expand, for example, because of possibly different approaches to the intellectualization and interpretation of situations of interaction between the components of an industrial conglomerate and IoT, produced by different suppliers operating in different technological areas. You should also consider the use of initially different knowledge representation systems and algorithms for processing the received data, as well as methods for automatically generating conclusions for making decisions and applying subsequent actions.

Thus, on the one hand, it denotes the task of initially coordinating the set of factors of knowledge representation, building a set of consistent models of functioning and interaction of a conglomerate of devices, as well as intersystem and human-machinery interfaces for aggregate assessment of not just the state of individual objects, but situations involving the actions of sets of devices and people. On the other hand, there are many questions of regulatory and legal regulation of the use of systems and technologies of the Internet of things in the lives of people, things and the industry. Even ethical issues are being discussed. These issues are particularly acute in the Russian Federation, since, at present, the legislative and regulatory framework in this area is at the stage of formation and initial testing.

II. BACKGROUND AND MOTIVATION

It is possible to distinguish in this development several stages, determined by the properties and features of control, management and evaluation of the results of the elements and the total activity, as well as its energy supply performing a retrospective analysis of the development of labor and household activities in human society in terms of its information support and intellectualization. Changes in organizational structures are not considered.

Stage 1. Manual labor. Labor, household and other activities are carried out using manual labor, simple tools and devices [7]. Control and management are carried out by a person using sensory organs (information bio-interfaces) and motor organs (limbs), information processing is provided by the nervous system and the human brain. Source of energy was muscular energy in humans and some animal species. Risks and responsibility for the results of activities fully relate to the person or people group engaged in certain activities.

Stage 2. Mechanization. This stage is characterized by equipment of production with machines and mechanisms; complete or partial replacement of manual labor with machines and mechanisms [8]. It should also be noted the mechanization of household and etc. A variety of activities is carried out with the use of complex tools, devices, machines, equipment. Control and management continue to be the prerogative of the person, information processing is also provided by the nervous system and the human brain. The source of energy was the energy of steam, water, wind and muscle strength of humans and animals. This stage is also characterized by the beginning and development of the use of electricity. Risks and responsibility for the results of activities are beginning to be redistributed between people who directly implement a particular type of activity (operation) and other groups that provide design, development and manufacture of complex tools and equipment. So there are elements of indirect responsibility for the results of activities with the relevant legal relations and law enforcement.

Stage 3. Automation. One of the directions of scientific and technological progress is characterized by using self-regulating technical means and mathematical methods in order to free a person from participation in the processes of obtaining, converting, transferring and using energy, materials, products or information, or significantly reducing the degree of this participation or the complexity of operations [9]. One of the main directions of modern automation is robotics. The main source of energy is electricity. At this stage there is a further alienation of the person from direct participation in production and other types of activity due to the fact that the equipment independently, without (technological) control of the person provides necessary activity and the set production (or other) required result, using the program or a complex of the programs developed by the person.

In other words, when automating the achievement of the result is determined not by the specific physical participation of a person in providing the activity functions of equipment, devices but by mediated information participation.

As a result, there are new types of risks associated with a new property of activity - information support. These risks can appear on the one hand at all stages of the information systems life cycle: planning, design and development, implementation, operation, decommissioning [10]. At these stages an information model of production and other activities is formed and used, starting with models of states and their transformation (model support). Risks can occur when determining the parameters used, formats, descriptions, and sampling the values of data generation,
transmitting, submission, and conversion, as well as the interpretation and algorithmic transformations. These risks arise from inaccurate or erroneous representations or interpretations of actual processes and conditions by developers and operators. But the risks of deliberate interference in the production, information and business processes associated with information globalization are much more dangerous. Currently, these risks have required the formation of a new, dynamically changing subject and production area, defined as information security or information protection. It should be noted that due to the high dynamics of development of information support, regulatory, legal and legislative support often does not correspond to modern realities.

Stage 4. Intellectualization-industry 4.0. The concept of intellectualization and, especially, artificial intellectualization is very multifaceted. This is primarily due to the lack of certainty of the concept of "intelligence" and, especially - "artificial intelligence" [11,12,13,14,15,16].

The following is an understanding of these and related concepts within the subject area of the Internet of things and industry 4.0. In this sense, intellectualization is understood as the organization (implementation) of such (similar, etc.) human activities in all spheres of civilization in which artificially created objects - cyber-physical objects and systems (CPS) participate [17]. At the same time, in our opinion, it will be more accurate to distinguish (differentiate) this activity in three main areas in accordance with their functional characteristics:

- production (industry 4.0) - production of material goods;
- social sphere (Internet of things) - service of a person in his/her environment;
- business processing-intellectualization of business processes.

Further, the problematic issues will be considered only within the direction of "industry 4.0".

III. STRUCTURING RISKS AND THE LEGAL RELATIONS

The main feature and the main problem of CPS participation in activities carried out previously only by man is the transfer of intellectual components of human activity (recognition, definition of goals, planning, defining tasks that are necessary to achieve the goal, execution of actions to achieve the goal, comparison of planned and obtained results, correction of goals and objectives, etc.) on Wednesday CPS with all the ensuing consequences. The risks arising from this and attributable to a variety of different processes are of a different nature, different approaches and methods of their assessment, different consequences and scales. With production and technical activity that is increasingly alienated from a person, reducing the possibility of human intervention in unusual situations, these risks will increase both quantitatively and “qualitatively”. So far this has been minimal, but the entire experience of the development and dissemination of information technology predicts the explosive development of Industry 4.0. To this we must be ready and work ahead of the curve.

In the examples presented as Industry 4.0, the production activity is mainly carried out by one or several CPS complexes. At the same time, artificial objects: production tools, machines, equipment, conveyors, etc., not only realize their own local functions (activities), but also jointly solve the problems of production activities, while possessing the appropriate level of intelligence, which was previously the prerogative of only subjects, then - there are people with their intelligence. It should be noted that human activity is individual by virtue of its origin, and the activity of CPS is of the same type because it is based on the application of algorithms of formal systems. At the same time, many CPS parameters exceed the parameters of human activities. And their actions, and the results of actions, in typical, patterned situations, can also, to a certain extent, be more effective and less subject to risks similar to the risks of human activity. On the other hand, human activity is less algorithmic and more efficient in conditions of uncertain situations. These opposite properties of both management systems must also be taken into account when analyzing risks.

In this regard, it is interesting to look at such an element of the Internet of things as “digital counterpart”. This technology for monitoring the state of technical and other equipment can be a good substitute for human intuition based on the ability of a person to unconsciously record deviations of environmental parameters, including controlled processes, with the human nervous system and translate this unconscious into some emotional coloring. The technology of “doubles” involves the creation of a parametric digital model of the life cycle of CPS. The parameters of the actually working equipment for the corresponding time ranges are compared with this model. The results of the comparison make it possible to determine, on the one hand, the current state of the equipment, and, on the other, to predict its risks during further operation. Such an approach will significantly reduce crash events, which are usually sudden and unpredictable from a human point of view.

A good example of this technology is the S.M.A.R.T. Performing self-testing procedures for disk testing. S.M.A.R.T. can monitor their working status by determining the current values of the parameters. The system software processes the data received. In this case, it is possible to build various models for estimating states, ranging from the simplest warning when values exceed the permissible limits, to statistical analytics of various combinations of parameters. Thanks to this mechanism, users can take corrective measures to prevent data loss and replace suspicious drives to ensure data integrity and minimize the chance of data loss. Thus, the risks of technological properties are reduced and the risks of unforeseen situations that are not calculated during the design increase.

Further, from a legal point of view, the main problem now, when embedding CPS - activity in the human world, is the absence of subjects who were given full responsibility for carrying out any activity and getting the necessary results. Accordingly, all legally significant rules, actions, regulatory and regulatory acts, laws and other elements of legal relations and law enforcement now require a thorough detailed review, adjustment and transformation.

Further, it should be noted the following: one can imagine 2 approaches to reforming the legal framework with respect to CPS:

a) full responsibility of people for all the consequences of human activities in conjunction with cyber-physical systems if it stays in the current legal field. In this case, it is necessary to introduce the concept of indirect responsibility of people for the actions of cyberphysical systems.
b) it is necessary to structure and/or evaluate in any way the actions of cyber-physical systems and the results of these actions (risks, damage, human activities, etc.). Giving certain properties or rights of quasi-subjects of legal relations with the definition of the relevant elements of legal liability to CPS should be in respect of them. For example, limiting the application of any principle of analysis, decision-making, prohibition of any class of CPS or CPS management system with the imposition of certain penalties or restrictive on subjects allowed the development, production or use of CPS of a certain class. As some analogue can lead to the procedure of revocation of cars by manufacturers in the detection of deficiencies in cars, leading to risks to health or life. As some kind of analogue, it is possible to cite the procedures for car recall by manufacturers when identifying deficiencies in cars that lead to risks to the health or life of people.

Before analyzing the issues related to the regulation and formation of legal relations arising from the use and application of cyberphysical systems, it is necessary, first of all, to analyze the risks arising from the fact that CPS without human intervention exercise less control over the static state of objects and processes, and more - control of situations in the environment. At the same time, it makes certain decisions and perform appropriate actions, changing the current situation (or moving from one situation to another possible).

Risk is understood as "a combination of the probability of causing damage and the severity of the damage" according to [18]. Concretizing this definition, it will be considered the probability of causing damage to the probability of this event for a certain period of time, for example, during the existence of an information system. We denote this probability as $v_i$. The significance of the damage can be determined in various metrics, for example, when causing harm to human health, in the cost of treatment plus the cost of the salary paid during treatment. We denote the amount of damage as $z_i$. The combination is defined as the multiplication operation "$\cdot \cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\·
4. At the industrial level, the concept of "industrial Internet of things", "smart enterprise", "industry 4.0" is actively used. Such a complex involves multi-level communication, a large number of objects that are part of an enterprise or organization as a certain property complex, a large amount of data transmitted, several control centers that interact with each other. Since there are a lot of devices for receiving/transmitting data, there are a lot of vulnerabilities and opportunities for their implementation [21].

Often, the complex is subject to one of the most common types of attacks - ddos-attack, when some device is overloaded with information flow and cannot cope with its processing. In addition, it is necessary to take into account the risks of the system itself: coarsening models, algorithmic, interference effects, etc., which arise in situations not provided for in the design of the Internet of things systems.

5. The next level, after smart production, it is necessary to consider the risks arising from the inclusion of smart production in the system that provides smart support for business processes, logistics, operation, logistics of created products, support, technical support and interaction with customers. This level is typical for large commercial organizations, as well as for state and transnational organizations.

The proposed level classification of risks reflects the fact that the change in the level (volume) of participation of CPS objects in the implementation of production activities leads to an increase in their share of participation in achieving the result. At the same time, not only the number of risks of the previous level increases linearly, but also there are types and types of risks of the new level, as well as a combination of risks of different levels. In general, the amount of risk is now defined as the number of combinations

$$C_{\text{risk}} = \frac{N!}{K!(N-K)!},$$

(2)

this means a nonlinear increase in the total (total) risk attributable to the use of CPS and, accordingly, should be taken into account to determine the responsibility and its metrics.

To reduce the number of possible negative situations and their risks, it is already necessary to form a system of state control, management and legal support of the processes of creation and operation of such systems. At the moment, the concepts related to the Internet of things are contained in the state standards [see, for example, GOST R 57100-2016/ISO/IEC/IEEE 42010:2011 System and software engineering. Description of architecture], which are not normative acts; the basic laws in this sphere [22,23] do not contain the concepts of the studied sphere, and the programs "Digital economy" and "Industry 4.0" are based on the entities of the sphere of the Internet of things.

The introduction of the terminology of "unambiguous interpretation" in normative legal acts is an integral part of the creation of successful regulations. Therefore, it is necessary to pay special attention to the conceptual apparatus. Some attempts to define the Internet of things at the legal level are presented in the Open concept "Internet of things: legal aspects (Russian Federation)" [23]. Taking into account that certain defined elements of the Internet of things are present in some normative acts of the Russian Federation, it is necessary to consolidate this definition at the legislative level.

The use of elements of all areas of the Internet of things, according to Russian legislation, is possible both in the relations of individuals and legal entities, and in their interaction with public authorities and local self-government, as well as in the interaction of authorities with each other. Often, legal entities act as independent business structures, representatives of public authorities and local self-government act in civil circulation as, in the direction of the risks of IoT, it makes sense to combine many legal entities and authorities into one group, thus dividing all users at risk of IoT into two groups - individuals and organizations. The division into groups is necessary not only to determine the functionality, volume and quality of the use of IoT (and it is, of course, different), but, first of all, to determine the types and levels of risks of unauthorized situations, as well as the formation of adequate legal support.

In the first case, the object of the threats will be the person using the IoT. Ways of harming can be violation of integrity of work of cyber physical systems which are used by the person directly [25] (personal belongings – IoT), or in the household purposes. In the second case, not individual individuals may be at risk, but industrial enterprises that produce the items, devices, equipment and technologies necessary for the normal functioning and protection of the state and the state institutions themselves.

Thus, in order to form a regulatory and legal framework for regulating the sphere of the Internet of things, it is necessary, primarily at the legislative level, to determine the structure of the Internet of things as a whole and its complex systems, the boundary conditions of such systems (and hence the boundaries of responsibility of manufacturers, operators, users).

Consider the hierarchy of the industrial Internet of things and the possible risks to which the cyberphysical system may be exposed.

The basis of the industrial Internet of things are devices that receive information from the external environment (for example, sensors). The information is then sent to the smart system over a wired or wireless network. The information is analyzed (processed) and then used to make a decision. Information about the further action (inaction) is transmitted to the devices of this or other level, which function depending on the information received. The functions at each level of such a system are different; for example, at the first level it is necessary to obtain the correct source data. it is necessary to prevent the receipt of false data due to forgery, distortion, or incorrect acceptance/reading of information. At the second level, it is necessary to ensure the correct processing of the data in accordance with the models used and the relevant programs. In case of using the software it is necessary to take into account the factor of appearance/manifestation of errors. Since such a complex system, from the point of view of functional and technical, is a multi-component system, it makes sense to allocate the components of the systems in order to possible detail the legal responsibility for the processing, storage and transmission of information of each of these components, resulting from the incorrect operation of the system, as in the processing of information can occur various kinds of errors: failure errors, algorithmization errors, input errors, etc. In view of the fact that operators of separate components of systems can be different divisions of the organization, it is necessary to distinguish areas
of responsibility for the incorrect operation of those or other components of the information system as a whole.

When designing complex information systems, it is necessary to determine the boundaries of parts of the information system, the operation of which is carried out by groups of subjects with different legal status. Control over the performance of duties and the technical component of the work on input, transmission and processing of information is necessary not only for the state, but also for any other information systems.

Unfortunately, at the moment the legal basis for determining legal liability is not sufficient for the above therefore, the relations arising when working with information systems are regulated, first of all, by the norms of the Civil Code of the Russian Federation (Chapter 38 of the civil code) [24], but this is clearly not enough, because it will have to determine any levels of intellectualization of the components of the Internet of things. It is necessary to determine the legal status of both the components themselves and the decisions allowed to be taken by these components.

Even if there are such statuses, it will be difficult to determine who is responsible for the improper performance of work in accordance with article 773 and article 777 of the civil code, since there is no technical and legal differentiation of responsibility arising for the actions of certain entities in connection with the work of certain components of the system.

Thus, it can be concluded that when putting into operation information systems based on the ideology of the Internet of things, it is necessary to provide a means of delineating the areas of responsibility of the components of the IoT. Zones can be temporary – untimely performance of duties by operators, spatial – transfer of information from one legally significant subject to another, functional – the correct processing and storage of data, the correct functioning of the processed data.

Most process control systems are used by subjects of critical information infrastructure. It should be noted that such entities include government or commercial organizations that use automated control systems to perform their functions in the areas of health, transport, energy, nuclear energy, defense and other types of industry. Since, often, such entities are not manufacturers / suppliers of components of the automated process control system, it is necessary to introduce measures to determine compliance with the quality of the components used, which include both components and software, data transmission tools, etc. And the consolidation of such measures should be in the regulations, to which most documents of a recommendatory nature (for example, state standards) do not apply.

Since the automated process control system already allows one to make further decisions based on many input parameters, the next level of decision-making can be considered the intellectual level. And no matter who or what acts on this level. Modern technologies (artificial neural networks, other methods of artificial intelligence) make it possible to make a decision based on the methods used, the features of their implementation and the algorithms used. If the decision is made directly by a person or a group of persons, then decision-making should be excluded if there are subjective factors, or their influence should be minimized.

It is necessary to realize the possibility of negative influence of artificial intelligence on humanity [25], since many actions in industrial cyber-physical systems are carried out on the basis of calculations and conclusions of artificial intelligence systems. Since the artificial intelligence system is implemented by complex software, in this case, the AI is characterized by the same risks as for software development. On the other hand, failures and improper functioning of such systems can lead to serious negative consequences, especially when used for military purposes.

IV. CONCLUSIONS

The introduction of elements of the Internet of things to all levels of human activity entails the responsibility for the creation and production, as well as the operation of such devices. It is necessary to clearly divide the system into logical sections that implement various functions, receive or transmit data in possible ways for further processing. This separation will allow you to accurately detect the cause of the incident for the correct technical and legal assessment of the incident.

The article notes that the Russian legislation does not sufficiently reflect the possibility of regulating the technological processes of industrial enterprises and important facilities (critical infrastructure).

As proposals to substantiate the structuring of the regulatory and legal framework of the Internet of Things and Industry 4.0, a classification of IW components and risks of their exploitation is proposed.

The possible features of the functioning of IW components that are necessary to consider when forming the regulatory legal base of IW are shown.

A level structuring of the functioning of the IW components is proposed and the concept of inter-level interaction, as one of the most vulnerable processes in the entire life activity of the cyber-physical system, is introduced.

Acknowledgement

This research was financially supported by the Russian Foundation for Basic Research in the framework of Project No. 18-29-16014 "The place and role of legal regulation in the development of digital technologies, legal regulation and self-regulation, including taking into account features of branches of law".

References


[3] Industry 4.0: new challenges and labour market opportunities [Online]. Available: https://foresight-journal.hse.ru/data/2017/12/24/1159810745-%D0%9A%D0%B5%D1%80%D0%B3%D1%80%D0%BE%D1%83%D1%87-6-8.pdf
