

LEGAL INITIATIVES IN THE FIELD OF INFORMATION SECURITY (ON THE EXAMPLE OF RUSSIA)

Alexander Redko, PhD¹

Volgograd Academy of the Ministry of the Internal Affairs
of the Russian Federation

The need for an in-depth study of legal initiatives in the field of information security is due to the fact that Russian special legislation in the field of the Internet is at a very early stage of development.

Today the state is in need of new specialists in law enforcement, government and administration. The new reality dictated by a special military operation on the territory of Ukraine and unjustified sanctions against the Russian Federation, with the full support of Russia from the People's Republic of China, can plunge the world into a serious crisis associated with food shortages (Redko, Osipenko, Nasonova, Vekhov, Nikonovich, 2019: 509-515), which will lead to even more crimes. Given that the modern criminal is not particularly eager to leave the house today, it is possible to predict with a high degree of probability an avalanche of Internet crimes.

Criminal communities use all new technologies dictated by rapid scientific development, taking advantage of the lag of middle and older age groups and certain groups of low social status (those suffering from alcohol or gambling addiction, the disabled, partially capable or limited in legal capacity) in computerization and integration of advanced technologies in everyday life. The situation is developing in such a way that each of us (including you, dear reader of this scientific article) repeatedly receives phishing calls from scammers pretending to be bank employees, special voice assistants (bots), and if until recently they needed the necessary knowledge of psychologists, basic skills financial transactions and the charter of the legal entity on behalf of which they are presented, then today their only task is

¹aredko3@mvd.ru

to receive from you the maximum number of voice commands (phrases, theses). This is due to the fact that almost all financial services applications have built-in voice assistants that recognize voice and allow you to make transactions without Face-ID or papillary identification.

While the whole world is considering legislative initiatives on how to counteract these forms of fraud, the Internet information and telecommunications network has been replaced by such a phenomenon as the messenger, which is a symbiosis of clips and short informational texts. In fact, this is a symbiosis of ISQ and YouTube. Efficiency, dynamism, and general accessibility of instant messengers such as WhatsApp, Telegram, and Signal make it possible to effectively influence the life of society, the consciousness of the broadest masses of the population. They can help to arouse public opinion in support of certain goals, a particular political course. At the same time, they can perform integration functions, persuading people to favorably perceive and assimilate the prevailing socio-political values. The leaders of many countries of the world, including Russia, as well as individual leaders of the constituent entities of the Russian Federation, are active users of Facebook, Instagram, WhatsApp, and Telegram. Their position, spread through accounts to millions of people, cannot but be reflected in the formation of public, political and legal consciousness and inspire confidence among citizens who regard these sources as official, which gives enough advantages to commit new types of crimes. In particular, the most common is the collection of funds for the fictitious treatment of children, the disabled, combatants, humanitarian aid for various purposes, etc. Using special programs to cheat the audience, attackers create fictitious accounts for themselves, the photos (avatars) of which display famous people, the account name in one way or another duplicates well-known names, for example: MrMakron__official@gmail.com, and then enter into correspondence with several hundred potential victims at once. There are still no ways to counteract, detect, suppress, disclose, prevent such crimes, and the implementation of the principle of the inevitability of punishment remains at an extremely low level.

At present, there is virtually no experience of legal regulation of this newly emerged sphere of public relations. Unfortunately, this is not only about criminal activity; along with it, Russia's civil law relations, administrative and security, criminal procedure and others are not regulated. The need to develop and implement a scientifically based state strategy in this area is dictated not only by the interests of strengthening democracy, but also by the objective needs of Russian society (the world community as a whole) and the state in protecting the foundations of the constitutional order, morality, and other constitutionally recognized values.

Nowadays the world is developing at such a speed that lawyers are not able to engage in law-making activities on their own due to the fact that they do not have special technical knowledge that allows them to capture and understand the



meaning of the necessary algorithms of behavior in the field of public relations. In today's society, people are more and more dependent on receiving information via the Internet. The United Nations recognized free access to the global network as one of the basic human rights (Rikke, 2013). Obviously, the number of crimes in the virtual environment will increase.

Conventionally, there are two key approaches to the prevention of cybercrime. The first of them relies on preventive measures: moderation, traffic control, blocking of nodes containing "undesirable" information, as well as entire services. A similar practice exists in China (Redko and others, 2019), Iran, Kazakhstan, and a number of other countries. In connection with the popular unrest in Egypt, the Internet was simply turned off. Another approach involves the creation of a monitoring system for the appearance of illegal materials.

At present, the law enforcement and judicial practice of detecting and preventing crimes committed in a virtual environment is still in its infancy: the audience of Internet users is growing, new technical devices are being used and the role and place of certain methods and methods of committing crimes is changing. A vacuum of specialists in the law enforcement sphere who could give a reasonable forensic characterization of a criminal act of this type has formed. It is necessary to recognize at the state level that the middle and older generation of investigators and operational police officers directly or covertly avoid these themes, as they are afraid of demonstrating their incompetence. At the Volgograd Academy of the Ministry of Internal Affairs of Russia, an attempt was made to obtain grant support from the Fund of the President of the Russian Federation for the development of civil society under the Cyber-Policeman project, the essence of which was to carry out preventive measures on an ongoing basis, to prevent the negative impact of prohibited content on Internet users. In case of harm to Internet users affected by illegal actions, the provision of comprehensive assistance aimed at rehabilitation, restoration of rights, freedoms and reputation has been provided. Protection of minors from the negative impact of prohibited content (terrorist, extremist, sexual nature) and measures to prevent and suppress the implementation of illegal actions against them, as well as creating conditions for obtaining reliable information about persons engaged in illegal activities and obtaining information about resources that serve to disseminate illegal information and sending this information to the competent authorities for decision-making in accordance with the law have been provided for (Crystal&Yakushev, 1999: 17).

While using the Internet, citizens constantly receive offers to join extremist organizations, they are subjected to actions aimed at corrupting and inducing suicide, as well as committing various crimes. This is confirmed by the statistics of law enforcement agencies. Frequently, information from instant messengers and information and telecommunication networks is absorbed by adolescents and adults



faster and deeper than face-to-face communication with people. There are entire groups and even communities that openly distribute child pornography, engage in molestation of minors, bullying, sell drugs through digital resources, recruit into extremist organizations, call for participation in illegal rallies, overthrow the state system and commit other illegal actions. Offenders feel their impunity and do not feel controlled by the state and the public. In support of this, it is necessary to cite statistical data that Russia occupies one of the leading places among the countries with the highest number of suicides per 100,000 people in 2020, a significant part of which were pushed to suicide on the Blue Whale Internet platforms, in the form of quest games with tasks and RPG games, as a result of bullying;², among countries with the highest number of sexual offenses committed via the Internet among minors³, the sale of narcotic drugs via the Internet has also increased many times over recently⁴.

The forces and means of law enforcement agencies, in view of the quantitative composition and complexity of detecting such crimes, as well as the lack of relevant legal norms, do not allow taking control of this area. Civil society, represented by public organizations, actively participate in counteracting the commission of these crimes. However, a situation is emerging that public organizations are good at detecting, but cannot fight on their own, and state bodies can fight, but poorly identify and practically do not disclose cyber-offenses. As a rule, law enforcement agencies begin to deal with these types of negative phenomena only when terrible consequences have already occurred, and the system for detecting, preventing and suppressing is not effective. This problem secretly develops like a cancerous tumor, but its consequences can come on suddenly and it will be quite difficult to correct the situation.

Therefore, in the considered social, legal and political problem, a symbiosis of society and law enforcement agencies is necessary. There is a need to develop a state policy of the countries of the world to ensure the protection of human and civil rights and freedoms in the information and telecommunications network, which would include law enforcement, judicial, rule-making, law-educational, propaganda, as well as administrative, managerial, supervisory forms of implementation. First of all, legal initiatives are needed in the legislative environment, since in the course of work law enforcement agencies are faced with new types of crimes, a characteristic feature of which is the almost complete absence of regulatory regulation. For example: the activities of online stores selling nasvaem and snus, school-shooting and bullying groups, the distribution of various kinds of

2 <https://openbase.online/ctatistika-samoubijstv-po-stranam/>, <https://psihomed.com/siniy-kit-zadaniya-kotoryie-ubivayut/?ysclid=l8wy35vc6z196140007>

3 <https://ria.ru/20200529/1572152411.html>; <https://www.gazeta.ru/social/2019/10/16/12758942.shtml>

4 <https://news.ru/society/mvd-chislo-prestupleniya-s-ispolzovaniem-interneta-v-rf-vyroslo-na-91/>



synthetic salts, and much more. Without the capabilities of special subjects, they quickly come up with a legal initiative to resolve the problems that have arisen, develop forensic characteristics and law enforcement practices, criminals will be ahead of law enforcement officers by 5-10 years. Law enforcement agencies simply do not have the opportunity to timely include in their competence the newly emerging negative trends among young people.

Secondly, there is a need for an international exchange of materials of law enforcement and judicial practice on the issue under consideration. It is necessary to conclude a number of international agreements and programs for the exchange of experience and specialists since these crimes are committed all over the world using the same algorithms. For example: cannabis (for narcotic purposes to obtain psychotropic pleasure) is banned in Serbia, but it is allowed in the Netherlands (it is even added to confectionery), so a criminal who sells drugs over the Internet in another country has nothing to fear except extradition (if such a legal institution exists). The Russian Federation today is literally flooded with reports of mining places of mass gathering of people. Despite the fact that this is a serious crime in many countries, we understand that the citizens of Ukraine will not be held accountable for this. Moreover, in most cases the criminals committing an act remotely are in other states and are confident in their own impunity. The Russian Federation today is literally flooded with reports of mining of places of public gathering of citizens⁵. Therefore, without the active work of the Interpol Bureau, Consulates, Ministries of Foreign Affairs, embassies and other international bodies, the effectiveness of prevention, disclosure and investigation will be significantly reduced.

It is also a matter of concern that the Russian Federation has not ratified CETS 185 (the Convention on Cybercrime or the Budapest Convention on Cybercrime) for 20 years. It is obvious that cybercrime is most effectively dealt with within the framework of international law. Because of this, the tendency to expand international cooperation in the field of high technologies is noted in the activities of many international organizations. One of them is the Council of Europe according to which the growth of computer crime requires a coordinated approach by States to develop regulations aimed at combating it. A number of recommendations adopted by the Council are devoted to this problem in which an attempt is made to define the concept and outline the range of crimes related to the use of computer technology⁶. Unfortunately, the advisory nature of these documents did

5 https://gorsite.ru/news/gorod/236-soobshcheniy_o_lozhnykh_minirovaniyakh_poluchili_sluzhby_v_novosibirsk/?utm_source=yxnews&utm_medium=desktop

6 Recommendation No R (89) 9 of the Committee of Ministers of the Council of Europe to member States for the Computer-Related Crime and Final Report of the European Committee on Crime Problems (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies). – Strasbourg, 1990; Recommendation No R (95) 13 of the Committee



not contribute to resolving conflicts and gaps in the sectoral federal laws of modern countries that arise in practice.

Due to these circumstances, the Committee of Ministers of the Council of Europe in February 1997 was tasked to study the legal problems arising in the investigation of computer crimes. Based on the results of its work, it developed a draft Convention on Cybercrime. This is a comprehensive document containing norms designed to have a significant impact on various branches of law: criminal, criminal procedure, copyright, civil, information.

The norms of the Convention are aimed at regulating three main issues:

- convergence of criminal and legal assessment of crimes in the field of computer information;
- convergence of national criminal procedural measures aimed at ensuring the collection of evidence in the investigation of such crimes;
- international cooperation in criminal procedural activities aimed at collecting evidence of the commission of such crimes abroad.

A significant feature for the criminal legal sphere was that it was proposed to be included in the legislation of the countries participating in the Convention uniform norms on criminal liability for cybercrimes, the list of which includes acts directed against computer information (as the subject of criminal encroachment) and using it as a unique instrument of committing a crime, and acts whose subject of encroachment are protected by the law of good. The object of cybercrime, according to the Convention, is a wide range of public relations protected by law that arise during the implementation of information processes regarding the production, collection, processing, accumulation, storage, search, transmission, distribution and consumption of computer information. Among them, legal relations arising in the field of confidentiality, integrity and availability of computer data and systems, the legitimate use of computers and computer information, copyright are emphasized.

The reaction of human rights organizations to the proposed ratification of the Convention in the Russian Federation was quite expected. Human rights organizations argued that it contradicts basic human and civil rights, does not correspond to the natural law theory of law, restricts constitutional permissions, unjustifiably strengthens the powers of national governments, undermines the development of information security methods and reduces the responsibility of the state before the law.

of Ministers of the Council of Europe to member States for the concerning problems of criminal procedural law connected with Information Technology (adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies). – Strasbourg, 1995.



As a result, the number of cybercrimes in Russia in 2021 has risen by a third. In January 2021, this indicator increased by 32% compared to the figures for 2020. In the first month of 2021 alone, 37.2 thousand crimes in the field of information and telecommunication technologies were registered. At the same time, attackers were 39% more likely to use mobile networks to achieve their goals, and the Internet was 51.3% more likely⁷. Over the past seven years, the level of cybercrime has risen 20 times, and the actions of attackers in this area are becoming more aggressive. This was announced by the official representative of the Investigative Committee of Russia: "Today, every seventh crime in Russia is committed with the help of information technology or in cyberspace."⁸

Thirdly, the state, both at the external and internal levels, must include mechanisms for legal education, the formation of legal creation and legal culture. At the same time, the time of wall newspapers and motivational speeches of the boss who was under pressure of a more authoritative boss has passed. This causes extremely negative emotions and a desire to counteract, or at least harm them with inaction or imitation of the fact that they did not understand anything. The state should unobtrusively and covertly influence the consciousness of the population through information messengers, modern bloggers, shows, online streams and RPG games. It is necessary to use the misconception of citizens that state bodies do not care about this area.

Fourthly, the entire branch of the judiciary should be involved in such work. Despite the fact that the Russian system of legislation is attributed to the Romano-Germanic legal family, the judicial precedent is becoming more and more important in modern objective reality. This includes the Plenums of the Supreme Court and various interpretive acts. So, in the case where the regulatory legal framework demonstrates its gaps or conflict of laws, courts of various instances should come to the rescue, which are authorized to eliminate negative factors based on their experience and the use of the analogy method, and law enforcers can focus on them.

Fifthly, an administrative and managerial decision and a political lobbying for serious changes in the structure of law enforcement agencies are needed. In particular, it is proposed to establish the Main Directorate for Combating Cyber Crimes in the system of the Ministry of Internal Affairs of Russia, which will include the following departments:

- a) The department for combating extremist and terrorist activities;
- b) The department for the prevention and detection of crimes of sexual nature;

⁷<https://news.rambler.ru/sociology/45978985-chislo-prestupleniy-v-internete-v-rossii-v-2021-godu-uvlechilos-na-tret/?ysclid=l8y6vn7d7a279380302>
⁸ <https://www.rbc.ru/rbcfreenews/6000f7b39a7947863c0244d2>



- c) The cyber fraud department;
- d) The department for combating bullying, suicidal inclination, shooting and dissemination of deliberately false, defamatory information;
- e) The department for the control of online and RPG games and applications;
- f) The department for the suppression of illegal circulation of digital currency, monetization, mining.

Sixthly, there is a need for sufficient control and oversight of this area of public relations, both on the part of authorized bodies and on the part of public organizations and associations of citizens. The advantages of new means of mass communication and their rapid development provided interested persons with qualitatively different opportunities for manipulating public consciousness and group behavior (Kara-Murza, 2015). The essence of these processes is still little studied, and practice in this area is far ahead of legal theory and legislation. Today, it is necessary to realistically assess the role of these instruments, exercising timely control and supervision.

Currently, there is a rapid growth of the Russian segment of the global information network Internet, both in quantitative and qualitative terms. "Like the legal systems of other countries, including the US and the countries of the European Union, Russian special legislation in the field of the Internet is at a very early stage of development. At the same time, to a large extent, we can talk about the absence of an effectively operating regulatory framework in this area, despite the existence of general norms of constitutional and civil law and a number of other legislative acts. The reasons for this are both the insufficient theoretical study of certain fundamental regulations, and the subjectively wary attitude towards the Internet on the part of law enforcement agencies and persons working in them" (Crystal & Yakushev, 1999).

An analysis of the current legislation that forms the legal foundations of the Internet shows that the rules governing the implementation of its activities may have a different industry affiliation. Currently, the following legal acts are in force on the territory of the Russian Federation that directly or indirectly regulate public relations arising in the Internet environment - the Constitution of the Russian Federation, the Civil Code of the Russian Federation, the Federal Law on Information, Informatization and Information Protection, the Federal Law on Communications, the Federal Law on Mass Media, the Federal Law on Trademarks, Service Marks and Appellations of Origin, Criminal Code of the Russian Federation, the Federal Law on State Secrets, the Federal Law on Advertising, the Federal Law on operational-search activity in the Russian Federation. All of them, one way or another, cover individual features that must be taken into account when investigating crimes and offenses committed in the information and telecommunications



network or by means of instant messengers, but they were not considered in their totality in their conflict and gaps.

Specialized legislation regulating relations in the global network is actively developing all over the world and Russia is no exception. In the criminal and criminal procedural legislative regulation of Internet crimes, several obvious problems associated with objective reality can be identified. Fundamentally new theoretical approaches are needed to the forensic characterization of crimes committed through the information and telecommunications network. We are talking about the formal composition of the crime, we need methods that allow at least elementary to establish the place of the crime and describe the procedural and actual sequences of its conduct, compiling photo tables (possibly using the Print Screen shortcut keys, taking pictures of the screen, etc.), establishing the location of the offender and the effect of this or that legislation in relation to him in accordance with the theory of the distribution of law in space, time and circle of persons. This is the controversial issue of the actual possession and the possibility of disposing of certain funds of the victims, the features of compensation for harm, procedural measures, the difficulty in determining the exact damage, given that the bitcoin or u-money exchange rate is constantly changing. It remains a separate task to determine the persons responsible for the commission of an illegal act, given that the dark web allows them to mirror escape routes and mask VPN devices. Additional difficulties are created by the lack of national borders on the Internet.

Lawyers, scientists, political scientists have been saying for decades that it is necessary to take preventive measures, to prevent or anticipate the appearance of gaps and conflicts in law. Aware of the fact that modern society is dynamically developing and there are more and more social relations that need statutory regulation. At the same time, it is necessary to provide sufficient opportunities for self-regulation and legal initiative to persons who, due to their professional experience, are faced with this kind of crime. Only they are able to streamline the procedural and criminal legislation in such a way that the rule of law corresponds to the real situation of cases in practice, since the legal initiative provided for by legal prescriptions (rules of law) or the possibility of subjects of legal relations arising from their general meaning to cause (initiate) by their lawful actions certain positive changes in the system of current law, various areas of legal practice and individual legal regulation, improve the functions of the state, adjust the work of state bodies, as well as actual activities (behavior) implement this opportunity (Redko, 2021).

Taking into account the specifics of the global network, it should be noted that in some cases, real prevention of violations can only be carried out using the capabilities of providers, i.e. organizations providing communication services. There is an objective need to develop a corrective criminal and criminal procedural legislation of the Federal Law, the structure of which contains both general and special



parts, which would take into account special terminology and specific emerging legal relations, as well as measures of state coercion for non-compliance with prescriptions. Attempts to regulate only some aspects of the legal regulation of the Internet can hardly be considered justified.

The goals of developing Russian criminal substantive and procedural legislation in the field of cybercrime can be:

1. Providing conditions for the participation of the Russian Federation and operators of the Russian segment of the Internet in the development and adoption of international standards governing both technical and technological, as well as organizational and legal aspects of the development of the regulatory legal framework in this area;
2. Consolidation of state guarantees of protection in relations related to the Internet, the rights and legitimate interests of Russian citizens and organizations, public interests, state interests of the Russian Federation, constituent entities of the Russian Federation and municipalities;
3. Development of fundamentally new legislative and other regulations that take into account the specifics of the functioning and development of instant messengers.

According to the results of a sociological study by RBC-online, the share of Internet users aged 12 to 24 in Russia approached 100% and amounted to 97.1% in February-November 2020, following from Mediascope data (available to RBC). In other categories, the number of those who spend time online decreases with increasing age: in the category from 25 to 34 years of age, 95.8% of Russians used the Internet at least once a month, in the category from 35 to 44 years of age - 93.7%, from 45 to 54 years of age - 84.2% and in the category over 55 years of age - almost half (49.7%). In total, from February to November 2020, 78.1% of the country's residents over 12 years of age went online at least once a month. Most often, Russians access the Internet from mobile phones. So, at least once a month, 70.8% of citizens used a smartphone for this purpose, 50.8% used a computer. At the same time, 27.1% of Russians used exclusively a mobile phone to access the Internet in 2020. Most exclusive mobile users in Russia are in the category from 25 to 34 years of age (36.1%)⁹. "Technological tools available to a significant part of Russian society significantly increase the number of available information channels, thereby increasing the level of pluralism and transparency in the functioning of public authorities. The audience of the Internet, as a rule, consists of people who take an active life position, and therefore is quite influential" (Monks, 2003: 55). In addition, all sociologists who have studied the audience of Internet users agree on one

⁹https://www.rbc.ru/technology_and_media/12/01/2021/5ffde01e9a79478eb5230426?ysclid=l4ih2jlicg847763244



thing - every year it will only increase. Thus, it can already be reasonably assumed that the governments of countries that do not pay due attention to the prevention and suppression of crimes in the information and telecommunications network are depriving their citizens of a secure future. Do not forget that today the existence of truly independent media is possible only in the Internet space. Since with the development of political technologies media have become a powerful factor influencing the formation of electoral priorities, their activities are subject to separate regulation. In the implementation of the relevant norms, acute problematic issues arise related to the establishment of a balance between the freedom of the mass media and the freedom of expression of the will of voters. Unfortunately, the normative regulation of relations in this area can hardly be considered sufficient both in terms of volume and quality.

In our opinion, a competent and timely legal initiative will allow correction of the current circumstances, which on the one hand is part of the inalienable right to free will of collective and individual subjects, explicated in the possibility of correcting the rule of conduct that regulates public relations or a group of public relations with the aim of "effective solution in a relatively new way of an urgent socially significant task" (Kharin, Bogdanova, Kaptyugova, 1986: 110). In this case, the initiative is a response to the needs of social development - it expresses the need to resolve contradictions without overcoming the progress of society (Marx, Engels, 1954). The approach to a legal initiative as a law presupposes the presence of a creativity moment, the preservation of a creative position in the process of vigorous activity. The author of the initiative is able to evaluate his actions by socially significant criteria - he must have the ability to search for tasks, problems, new ways of action (Zatonsky, 2006: 15–18). On the other hand, a legal initiative in this sense acts as a form of vigorous activity of subjects in the legal space aimed at protecting the rights and legitimate interests. However, with all the interdependence and interpenetration, the legal initiative is not identical to the legislative initiative and has features inherent only to it, which in the forensic issues under consideration will also be significant advantages:

1. Unlike other types of social initiative (political, economic, scientific, etc.), a legal initiative is regulated (provided for) by the current law, and its implementation is associated with the onset of certain legal consequences. This sign is leading in the sense that it allows a fairly clear line between legal initiative as a specific phenomenon of legal reality and other types of social initiative.
2. The legal initiative demonstrates itself in the legal system of society in the form of two interrelated and interdependent parties: formal-legal (material or static) and active-practical (procedural or dynamic). In the formal legal dimension, a legal initiative appears as a specific right (authority), which is a structural component of the legal status of a collective or individual subject of legal relations.



In this case, it is nothing more than the type and measure of legally guaranteed possible behavior, it belongs to the category of subjective rights or public powers. In the active-practical aspect, a legal initiative is a form of socially active behavior of subjects of legal relations or, in other words, a form of realization of a subjective right (public authority).

3. According to its functional purpose, the legal initiative is aimed at introducing new principles and norms of legal regulation of social relations, forms of legal activity, the emergence of new legal relations, etc. Thus, it is a necessary means of innovative development of the legal system, a way to stimulate and introduce relevant legal changes (innovations).

4. In terms of content, i.e. from the position of ensuring the interests of the individual, society and the state, the legal initiative serves as a means of introducing progressive legal changes. This, of course, does not mean that any initiatives put forward in the legal sphere automatically lead to legal progress. The progressiveness of the legal initiative should be understood in the sense that, according to its purpose in the legal system of society, it is designed to improve, and not worsen, the legal status of citizens, various social groups, society and the state as a whole.

5. From the point of view of its place in the system of modern Russian law, the legal initiative is a complex (inter-sectoral) legal institution that combines the norms of public and private, substantive and procedural law.

6. The implementation of a legal initiative is associated with compliance with the requirements established by law, an agreement or other sources of law regarding the composition and eligibility of the subjects of the corresponding initiative, their number, the subject of the initiative, the time of its submission, form and other parameters. In particular, the Constitution of the Russian Federation (Article 104) defines an exhaustive list of subjects of legislative initiative and limits the subject of the legislative initiative of the Constitutional and Supreme Courts of the Russian Federation only to matters within their jurisdiction. The Labor Code of the Russian Federation (Article 81) does not allow the dismissal of an employee at the initiative of the employer during the period of his temporary disability and vacation. The Family Code of the Russian Federation (Article 17) limits the husband's right to initiate a divorce during the wife's pregnancy and within a year after the birth of the child. The Federal Constitutional Law on the Referendum of the Russian Federation regulates in detail the procedure for implementing the initiative to hold a referendum, which belongs to the citizens of the Russian Federation.

7. Legal initiative is, first of all, the ability of the relevant subjects to exercise their actions granted by the state, international norms or norms of natural law the authority to change, terminate or create mechanisms to protect their rights and le-



gitimate interests. Legal initiative is the most developed form of socially active lawful behavior.

8. Legal initiative is inextricably linked with the realization of the rights and freedoms of man and citizen, manifestations of creativity, social and legal activity, while it is associated with the observance of certain procedural requirements.

9. The legal initiative is a kind of reflection of the level of democratization of society, by the degree of involvement in the legal initiative of collective and individual subjects, as well as by the number of initiatives put forward in the country, one can judge its openness to dialogue with the population, the degree of democracy in political and legal processes, level of development of the legal paradigm as a whole.

Legal initiative is a kind of social initiative and, unlike religious, customary or moral initiatives, must be conditioned by natural law or positive law or authority. A legal initiative cannot exist outside of law, and over time when social, economic, political circumstances arise, its goals and objectives may change.

An initiative is a creative, independent process of comprehension, creation, development, introduction, promulgation and implementation of any socially significant, useful proposals, projects, concepts, technical innovations (inventions), etc., carried out on the basis of free will. Legal initiative is always an active, but at the same time a voluntary process of the relevant subjects, it cannot proceed in the form of compliance or execution, the main form of its implementation is use, except when it comes to legislative initiative, which is the official responsibility of a certain circle of subjects.

The expected results of the development of the institution of legal initiatives are the creation of a permanent mechanism for the prevention of offenses on the Internet among citizens, the provision of comprehensive assistance to victims in rehabilitation, the restoration of their rights, freedoms and reputation, the creation of a platform for operational interaction with law enforcement agencies, the scientific support of this problem and the development of effective methods countering this problem.

Thus, objective reality strongly recommends that we take into account the initiatives of collective and individual subjects of law, for a timely legal response building a human rights system in such a way that it meets the requirements of science and technology.

REFERENCES

- Crystal B.V., Yakushev M.V. (1999) The concept of Russian legislation in the field of the Internet. Project, 17.
- Kara-Murza, S. G. (2015) Manipulation of consciousness. S. G. Kara-Murza. Moscow: TD Algorithm, 563 p.
- Kharin Yu. A., Bogdanova T. P., Kaptyugova E. M. [and others] (1986). Dialectics of social initiative. Minsk: Belarus, 110.
- Marx K., Engels F. (1954). Works: in 30 volumes. M.: Gospolitizdat, Volume 137.
- Monks V.N. (2003). See Mass media and the Internet: problems of legal regulation. Moscow: ECOPRINT, 55.
- Redko A. A. (2021) Legal initiative in modern Russia. Textbook for universities. Moscow: Yurayt Publishing House, 25.
- Redko A.A. Osipenko A.L., Nasonova I.A., Vekhov V.B., Nikonovich S.L. (2019) Agricultural Insurance in china Amazonia Investiga. Skopus journal – Floren- cia, Caqueta: University of the Amazon. 8(24), 509-515.
- Rikke F. J. (2013) Framing the Net. The Internet and Human Rights. MA, US: Edward Elgar Publishing, 262.
- Zatonsky V. A. (2006) Legal initiative is a powerful factor of progress. The right to initiative and its provision. Constitutional and municipal law. M.: Lawyer, (5) 15–18.

