

## IMPROVEMENT OF TYPES OF INFORMATIONAL RISK INSURANCE

***Xolbayev Azamat Yuldashovich***

*Associate Professor of the Tashkent State University of Economics,*

*Doctor of Philosophy*

*email: xolbayev.azamat80@gmail.com*

**Annotation.** In this scientific work, the role of insurance mechanisms in eliminating the types of informational risks and the losses arising from them is analyzed in conditions where modern digital technologies and information systems are rapidly developing. The main focus is on covering the risks of types of informational risk insurance — cybersecurity, data security insurance and information infrastructure.

The work studied the development trends of informational risk insurance systems based on the experience of foreign countries, and developed practical proposals and recommendations for improving insurance services of this type in the conditions of Uzbekistan. Proposals have also been made for informational risk assessment methodologies for insurance companies, the formation of a tariff system and the strengthening of the legal framework.

The results of the study are important in diversifying the insurance market, expanding the possibilities of financially compensating for possible losses in the field of cybersecurity, as well as supporting the digital economy.

**Keywords:** insurance, cybersecurity, financial resource, informational risks, insurance services, insurance premiums, authorized capital, reserve.

**Introduction.** Today, the development of digital technologies and cybersecurity in the global economy and public consciousness is impossible. This may be due to limited access to resources, databases, computer systems, and network infrastructure. At the same time, according to him, such systems can be used to combat cybercrime, information hackers and cybercriminals. This improves the reliability, functionality, reliability, and reliability of the devices.

In such circumstances, it is necessary to use mechanisms to minimize information risks and mitigate their consequences. House, cyber threats, and cybersecurity are the main factors influencing the development of cybersecurity.

Mazur noted that information risks related to cybersecurity should be minimized, and prevention mechanisms such as cybersecurity, cybersecurity, cybersecurity, cybersecurity, and cybersecurity should be expanded.

**Literature review.** Financial and economic aspects of informational risk insurance foreign Economist scientists K.Ruan, Paul Clumpes, Donatella Porrini,

R.Böhme[1], G.Schwartz, H.Narang, A.Sharapov[7], Ye.Baranova, I.Ivanov, V.Nomokonov[2], T.Tropina, S.Smirnov, L.Mamaeva[9], V.Occurs in Larionov studies[3].

Local economist scholars: H.Sobirov, H.Shennaev[10], C.Kushoshev, A.Jo 'raev, S.Umarov, R.Azimov, T.Baymuratov[4], I.Abdurakhmonov[11], G.Halikulova, A.Xolbaev[8], I.Kenjaev, S.Sherov[5], F.Khasanov U.Imamov[6], G.Adilovas in the research of the insurance industry and some issues of informational risk insurance are researched.

**Methodology.** In the process of performing the study, methods of systematic analysis and approach, logical and structural analysis, grouping and generalization, expert assessment and forecasting, mutual and comparative comparison were used.

### **Analysis and results.**

Currently, the main conditions for the formation of informational risk insurance at the level of demand in the national insurance market of our country will be as follows, including:

- In Uzbekistan, the digital economy is developing rapidly, and information occupies the main place in this;
- the issue of comprehensive protection of informational systems for society and the state and other entities is becoming an urgent issue every day;
- day after day, the intensification of cases of violation of informations, theft, destruction, as well as the widespread spread of viruses, the threats to the preservation of their idol are moving;
- to become an urgent issue among the developers of informational systems, the owners of informational and its users the need for Responsibility and the distribution of obligations on the maintenance, distribution and other qualifications of informational.

The main objectives of the creation of modern mechanisms for insurance protection of informational risks due to the above are as follows, namely:

- the progress of crimes related to technology to become an integral part of our lives, the theft, violation, disclosure, loss of informational information as a result of various illegal actions, changes to it, blocking, illegal behavior of persons in order to reduce trends;
- to encourage the creation of infrastructure for themselves, using the investiture capacities of insurance companies and their fundamental functions. In this case, the formation of demand, the optimal establishment of tariffs not only in terms of compensation for losses, but also in terms of earnings;
- to reduce the risks of losing data and making illegal changes to them, as well as to improve their adequate financing in order to effectively carry out preventive work to prevent their harm using the warning function of insurance, in order to effectively

carry out it not only at the expense of insurance companies, but also by attracting state and foreign grants. Such measures will be able to lay the groundwork for reducing their chances of occurrence by several times.

As a result of the occurrence of informational risks in subjects, the following types of financial costs may occur.

Subjects may incur many costs with the aim of preventing the consequences of adverse events that may occur in the future. Some of these costs can be equal to the economic result of the subject's activities. In some cases, they will not be noticeable. In any case, all types of expenses that occur in economic activity have an indirect and direct impact on the financial situation of the economic entity. Based on the above, the entire set of expenses can affect the final financial results of the subject and reduce its financial stability by several times, in some cases it can also lead to bankruptcy.

As a result of the above, it is an important economic issue for insurance companies to develop, provide insurance products on the cooling of measures to reduce the expected costs of the subject, prevent it.

Currently, the risks at which cyber risks, which are a form of informational risks by insurance companies, can be partially or completely insured are the following, namely:

- the risks of appropriation of confidential information by the employees of the subject and their use in ulterior motives;

- the risk of hackers illegally obtaining information about the credit card numbers of the subject's clients or their account sheet data;

- the risk of embezzlement of funds in the accounts of the subject or funds that are in the deposit;

- risk of disclosure of various confidential information of the enterprise;

- risks of accessing a server in a mercenary niche, unauthorized, illegal modification of information there, hacking;

- virtual blackmail (fraud) - risks of stopping a cyber attack or returning stolen information, demanding money for recovery;

- related to the faulty operation of the database;

- risks of loss (theft) of digital media that store and transport data.

Also in advanced insurance markets, the practice of insurance in addition to the insurance of inflationary risks, the following risks and their associated costs are common. As an example, we can cite the following:

- detection of cybercrime, reimbursement of financial costs spent on their prevention;

- costs associated with carrying out various activities to raise the image and image of the subject as a result of the fall of the subject's retainer as a result of the damage caused;

harm of activities related to the protection of the Huquq, which occurs in cases after damage;

to provide reimbursement for the cost of restoring informational systems, etc.

Currently, insurance companies have been creating a variety of products in increasing informational risk insurance coverage. It is common in this to show universal products that jointly include their property, the health of their employees, their material responsibilities before third parties, etc. In this case, we can separately provide liability insurance for third parties. The reason is that it is second only to informational risks due to the fact that it can cause significant damage. By adding such services, the offer embodies the comprehensive protection of the subjects and increases the attractiveness of the insurance product. Currently, such insurance products are widely promoted in foreign countries. It is natural that the use of some of them in the national insurance market also has a good effect. We will cite some of them, including:

types of civil liability insurance of damage to third parties by or without the knowledge of the entities that provide data protection (manufacturers or intermediaries who provide direct services to them) themselves;

insurance policies that provide financial, economic moral liability that can be transmitted to third parties due to errors of electronic platforms (e-purchase, e-auction trading platforms, etc.) and various trading exchanges;

risks such as civil liability insurance of licensed centers operating in data (open data) infrastructure.

Information tools and services provided to subjects are responsible for causing harm to third parties, including in connection with data leakage, data leakage, data leakage, personal data leakage, etc. As a result of the conducted research, it was found that when exposed to harmful substances that cause allergic reactions, side effects may occur in the human body. An amaliyet can be several times the amount of damage caused by their financial resources and assets. As a result of losses caused to a third party, the bankrupt faces bankruptcy. Sub-Zero and Amaliyet were killed, and they were released. If no malware (deception, image) has been found, then it can be used to create malware. Agar sugurta polisi mavjud buladigan bulsa bunda company tomonidan limitlar shirnatili va mizhozlar yzlari etkazishlari mumkin bulgan maximum zararlar paketini tanlab olishadi va sugurta kompaniyalari shu zararlar limiti doirasida mizhozlari tomonidan etkazilgan zararlar mikdorini tilab berishadi yeki sha zararlar mikdori byicha zhavobgarliklarni olib borishadi. Bunda esa ularning maximum kiladigan kharazhatlari shu polislarni sotib olishga ketadigan mikdori tashkent etadi. Yz yzidan bu mikdorlar zararlar mikdoridan bir necha yuz martalab kam mikdori tashkent etadi. Because they couldn't get out of the cave, they turned into zombie monsters. That's what we'd like to do, and that's what we'd like to do.

Information risks associated with human rights violations are associated with

violations of international law and human rights, as well as violations of international law. Do not pay attention to the fact that information risks associated with financial services can be minimized. According to Mikhail Amaliyev, an expert in the field of information security and risk management in the field of consumer protection and human well-being, the implementation of a risk-based approach will reduce information risks and risks associated with consumer rights violations based on the experience of foreign countries. In order to speed up the process, it is necessary to speed up the amalgam. Information risks in these processes are a set of factors that affect the speed of information transfer. In accordance with the legislation of the Russian Federation On Countering Information Risks in the Field of Intellectual property, in accordance with the legislation of the Russian Federation On Countering Information Risks in the Field of Intellectual property, this entity must be represented as an independent entity.

In accordance with the requirements of the law on Countering Information Risks in the securities market, it is necessary to develop its activities, including through the creation of independent and specially authorized bodies. This should be to keep abreast of all the events taking place on the planet.:

The first thing you need to know about cyberspace is how it works. Cybersecurity is a set of risks associated with data leakage, hacker attacks, privacy violations, etc. In our case, this is a cyber threat. The risks associated with this include: hacker attacks, malware, phishing, and DDoS (Distributed Denial of Service). This indicates a reduction in risks. In addition, to protect CTP policies, companies can use, for example, secure CTP servers (this requires specialists who will check CTP policies), the data can be used to assess the risks associated with leakage, leakage or leakage of data, as well as to assess the risks associated with leakage or leakage of data., in case we are unable to track the actions of the attackers, we will be able to track their actions and gain access to files and file systems.

Secondly, there are information risks. The main purpose of this agreement was to convince the parties that they could conclude peace treaties rather than peace treaties. This provides an opportunity for companies that may be interested in raising tariff rates, thus reducing tariff rates and responding appropriately to them. In jurisprudence, Amalasunta is considered as the most likely reason why he was executed.:

The risks associated with the paradox can be divided into: risks related to information and information flows of users, risks related to their activities, and risks that they may pose in the future. The forecast for the number of victims is being clarified.

Information risks and vulnerabilities: Information risks include vulnerabilities (e.g. malware, viruses, and viruses) and malware.

Insurance includes automation of work processes and information programs.



Bunda informationklarning tasirini kamaitirish va oldini olish borasida technologik va mamuriy chora-tadbirlar mazhmualari ishlab chikiladi.

Thirdly, it is the process of exchanging data and information between users. The data that is used in the process of working with data is stored in files stored in the file system and transferred to the server, where it is stored in the file system. Sabbath Systems did not provide the data, but provided them with the information they needed to be able to recover. In this case, the data is stored on one server and then transferred to another: backup copies of the data (archiving) stored on different servers are stored on the same server. If the information cannot be processed to the extent that it is needed, then it can be used in real time to perform certain actions and actions. Bu asosan yuz Berishi Mumkin bulgan risklar guruiga nisbatan ularning salbiy tasirlarini kamaitirishga karatilgan va kam kharazhatlarni amalga oshirish natijasida mamotlarni tiklash bilan boglik kiska muddatli strategialar ishlab chikilishi kerak biladi. Ular orkali tez va kam kharazhat kolaversa kiska vakhtlarda ularni tiklas choralari kirilishi kerakligi anglatadi.

### **Conclusion**

Among the obstacles to informational risk insurance in our country are the lack of experience of insurers in this regard and, accordingly, their lack of qualification to a certain extent. As a result of his research, the problems arise mainly from the fact that the potential insurer does not understand the essence of the main content of IT technology and security provision. In some cases, its original purpose is often incomprehensible to insurers.

Currently, there is no specific approach to assessing informational risks in our country, and there are also no separate insurance tariffs for informational risk insurance, for which the usual methodology for risky types of insurance is used, which slows down the development of this segment in our country.

In place of the conclusion, it can be noted that in our national insurance market, the type of informational risk insurance is going through its stages of development. In this, not only insurance companies and potential insurers, but also the state have shown a number of effective interests. In such conditions, we will be able to emphasize that the prospect of this type of insurance in the near future will show positive circumstances. But this area is much more than what needs to be done. For example, an excellent legislative framework has not yet been created for informational risk insurance, but it will also be appropriate to reflect on the introduction of their socially oriented mandatory manifestations in the initial periods.

### **References:**

1. Kholbaev A.Yu. Information Risk Insurance: Concept and Basic Aspects // International Journal of Trend in Scientific Research and Development, Vol. 6, Issue 1, November-December 2021. – Pp.760-766.

2. Xolbaev A. Y. INSURANCE AS A PROMISING MECHANISM OF INFORMATION PROTECTION //Archive of Conferences.(Dec. 2021). – 2021. – C. 39-40.
3. O‘zbekiston Respublikasi Prezidentining 2023 yil 1 martdagi PQ-108-son “Sug‘urta xizmatlari bozorini yanada rivojlantirishning kompleks chora-tadbirlari to‘g‘risida”gi Qarori.
4. O‘zbekiston Respublikasi Prezidentining 2019 yil 2 avgustdagi PQ-4412-son “O‘zbekiston Respublikasining sug‘urta bozorini isloh qilish va uning jadal rivojlanishini ta’minlash chora-tadbirlari to‘g‘risida”gi Qarori.
5. Xolbaev A.Yu. Страхование информационных рисков (киберстрахование) // «Xalqaro moliya va hisob» ilmiy-elektron jurnali. – Toshkent, 2021. 2-son.
6. Xolbaev A.Yu. Informatsion risklarni sug‘urtalash amaliyoti va muammolari (kiber sug‘urta) // «Logistika va iqtisodiyot» ilmiy-elektron jurnali. – Toshkent. 2021. 3-son. – S.433-439.
7. Kenjaev I.G‘. Sug‘urta tashkilotlarining moliyaviy resurslarini joylashtirish samaradorligini oshirish yo‘llari. I.f.f.d. PhD ilmiy darajasini olish yozilgan dissertatsiya avtoreferati. Toshkent, 2019 yil.
8. Xolbaev A.Yu. O‘zbekistonda informatsion risklarni sug‘urtalash amaliyotini takomillashtirish istiqbollari. I.f.f.d. PhD ilmiy darajasini olish yozilgan dissertatsiya avtoreferati. Toshkent, 2025 yil.
9. Azimov R.S. Iqtisodiyotni modernizatsiyalash sharoitida risklarni sug‘urtalash metodologiyasini takomillashtirish. Iqtisodiyot fanlari doktori (DSc) dissertatsiyasi avtoreferati. – T.: – 2022. – 86 b.
10. Baymuratov T.M. O‘zbekistonda sug‘urta faoliyati va uni soliqqa tortish mexanizmini takomillashtirish. I.f.n. ilmiy darajasini olish uchun yozilgan dissertatsiya avtoreferati. – T.: - 2004. – 22 b.
11. <http://www.napp.uz> – O‘zbekiston Respublikasi Istiqbolli loyihalar milliy agentligining rasmiy sayti ma’lumotlari.