# ЭКОНОМИЧЕСКОЕ РАЗВИТИЯ ФАКТОРОВ, КОТОРЫЕ ВЛИЯЮТ НА ФОРМИРОВАНИЕ УПРАВЛЕНИЕ МЕХАНИЗМА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ НА АНАЛИЗ ДЕЙСТВУЮЩЕЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Мурадов Ботир Хаят**
*Независимый соискатель кафедры промышленный экономика и менеджмент, факультет инженерных технологий, Ташкентскаго государственного технического университета им. И.А. Каримова, г. Ташкент.*

**Аннотация:** *в данной статье анализируется научная литература, связанная с разработкой политики информационной безопасности, обеспечением защиты периметра экономических информаций, а также нормами, стандартами и законами Республики Узбекистан в области информационной безопасности. В то же время была проанализирована работа независимых лабораторий в области информационной безопасности и статистические данные за прошлые годы.*

**Ключевые слова:** *экономика, мотив, механизм, материальные и нематериальные факторы, теории мотивации.*

## ECONOMIC DEVELOPMENT OF FACTORS THAT INFLUENCE THE FORMATION OF THE MANAGEMENT MECHANISM OF INDUSTRIAL ENTERPRISES ON THE ANALYSIS OF THE CURRENT INFORMATION SECURITY POLICY

**Abstract:** *The this article analyzes the scientific literature related to the development of information security policy, ensuring the protection of the perimeter of economic information, as well as norms, standards and laws of the Republic of Uzbekistan in the field of information security. At the same time, the work of independent laboratories in the field of information security and statistical data for the past years were analyzed.*

**Keywords:** *economics, motive, mechanism, material and non-material factors, theories of motivation.*

**B. X. Muradov**
*Tashkent state technical university*

### INTRODUCTION

The great worldwide technological progress in market conditions has radically changed the attitude of information in the economy of industrial industries. Therefore, in order to effectively achieve the goals of the enterprise, the management must control and motivate people to do the work through innovative technologies. If the conditions for self-realization are created at the enterprise, then the work of each employee will be highly effective, and the motives will be effective. Thus, motivating employees means giving them

the opportunity to self-actualize and take into account their desires and interests. That is why the problem of studying motives, incentives, as well as factors that influence the formation of the mechanism of motivation for economic growth remains relevant at the present time. The analysis of information technology and various innovative programs from sources obtained from various works of researchers of different scientists in the world has shown that a significant number of works are devoted to the issues of identifying factors that affect motivation. However, there are different points of view regarding the solution of this issue, and there is no single classification of factors that affect the formation of a mechanism for motivating the use of information from the sphere of economic indicators. The purpose of the article is to develop a classification and systematization of factors influencing the formation of a mechanism of motivation for economic growth in all areas of industries. The functioning of the motivational mechanism of labor activity is carried out under the influence of economic, organizational, socio-psychological conditions that encourage a person to work using new opportunities of electronics and various gadgets. The influence of this mechanism on human behavior depends on many factors. Having studied the meaningful theories of motivation, it is possible to identify the factors of motivation of works classified on the basis of needs.

The processing of electronic documents, as well as the daily work associated with the processing of confidential information, involves many risks to the integrity of the processed information and in the field of economics. As the volume of processed data increases every year, the number of possible risks also increases.

In general, the more confidential information an organization owns, the higher its value. Therefore, any data compromise can cause huge financial losses to an organization that can never be recovered. In today is world, there are many different threats to information security and data integrity. Cybercriminals are constantly changing the ways and means of obtaining the necessary information. From the point of view of cybercriminals, information is a commodity, and the more recent and relevant the information, the higher its price. Currently, cybercrime is not only a remote attack on certain resources, but also the use of social engineering methods for cybercrime.

Social engineering methods are aimed at obtaining the necessary permission to use information in their name, and these methods are based on the specific characteristics of the psychology of the affected person. The use of such techniques creates a type of threat that occurs within the organization, known as "insider attacks," rather than from outside. This type of attack is dangerous because a person or an employee may violate information security without realizing that they are committing an illegal act.

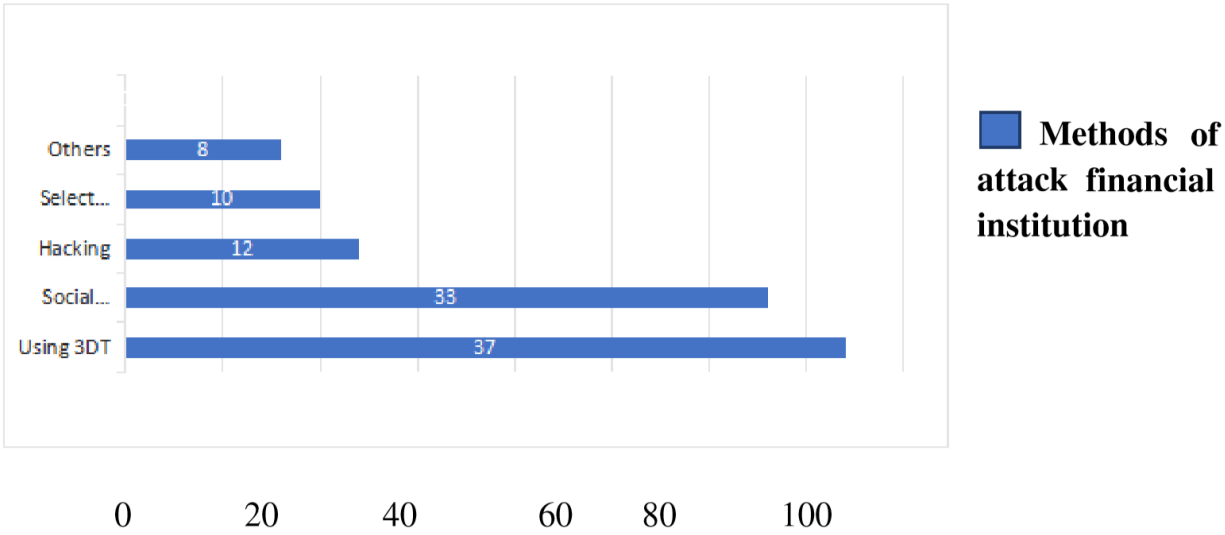
To avoid this, it is necessary to use information security policy. This policy should minimize the possibility of data compromise or corruption.

Therefore, the information security policy covers the possible risks, namely:

• theft of information; • destruction of information; • should provide maximum protection against information corruption.

**MATERIALS AND METHODS**

Information security policy is a set of preventive measures, rules and principles aimed at protecting confidential information and information processes in the enterprise. The security policy includes requirements and regulations for employees, organization leaders and technical services. The information security policy describes the goals and tasks that must be achieved and resolved during the implementation of the information security policy. In most cases, the information security policy is formulated and developed separately for a specific organization, and all employees, without exception, should familiarize themselves with this document.




1-picture. The attack on financial institutions in Q1 2022

Information security policy objectives may fall into one or more of the following categories: • information security - protection of information and the infrastructure that provides it from accidental or intentional effects of natural or artificial nature that can cause unwanted damage to the subjects of information relations; • uthentication the process of determining the authenticity of the user (network subscriber, message sender), program, device or data (information, received message, key); • authorization - giving a certain person or a group of persons the right to perform certain actions; • integrity - the state of information and its carrier, in which it is ensured that the whole and its individual components are not divided and that their unauthorized or intentional destruction, destruction, leakage, theft, forgery are prevented. ; • confidentiality - the state of the information and its carrier, in which prevention of unauthorized familiarization with it or unauthorized documentation (copying) is ensured; • risk - the possibility of using a specific vulnerability of the data processing system in the implementation of a specific threat; • risk assessment - the process of comparison of calculated risk and risk criteria, carried out in order to determine the nature of the risk;

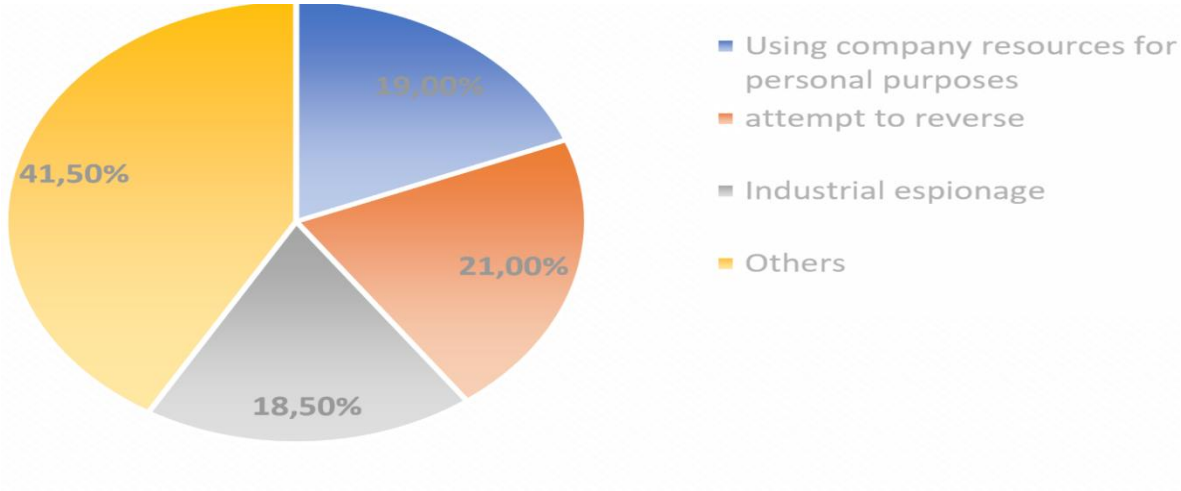
**RESULTS**

In this way, it can be concluded that the information security policy is an integral element of any organization. Applying an information security policy can significantly

increase the level of information protection, which in turn reduces the risk of financial losses and discrediting the company.

Software companies also conduct their own research in the field of information security. These studies are useful for information security professionals to predict the type and nature of threats in advance. According to a report by the Pt security portal, in the first quarter of 2022, methods of attacking financial organizations using ZDT (malware) and social engineering or "phishing" tools are widespread. "Phishing" is aimed at attracting employees of the organization picture- 1 provides a diagram of attack methods against financial institutions.

If security tools are evolving along with threats considering the methods and tools used in cyberattacks are significant it can be assumed that changes will occur. Maybe it's nothing It is possible to carry out an attack with the help of an unsuspecting employee, for example, by running an infected file. This type of attack is called “social engineering" and in everyday life such attacks are "phishing" or are called "insider attacks".




**2 - picture. Threat diagram.**

As you can see from the chart, this type of attack is in order of popularity It is becoming equal to ZDT. The main danger of phishing is that it is difficult to prevent. This type of attack is still the most dangerous for many organizations remains one of the attacks because the threat is carried out with the help of an employee can have serious consequences. Protecting the organization from the inside problem is still a weakness of many organizations.

Antimalware to verify the severity of the internal threat portal conducted a study on the nature of internal threats. This research the result can be observed through the following diagram (Picture-2). Loss of confidential information to choose protection methods it is necessary to consider the reasons. A diagram for this is shown in Picture-3.

Created. Based on the above, in the development of information security policy more attention should be paid to the protection of data from threats originating from within the organization, in which it is necessary to consider the conditions necessary for the formation of an "inside threat".

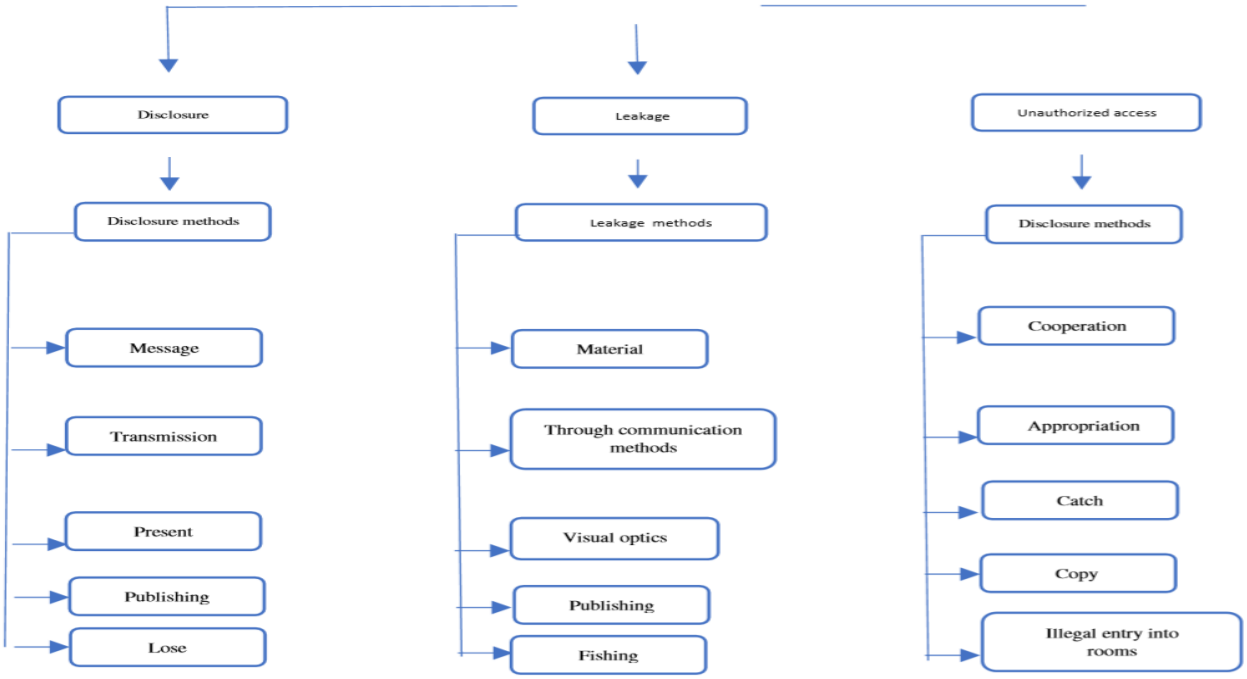
Examples of such conditions include:

• bribery of a responsible person; • excessive talkativeness of the employee, conditions of confidentiality in conversation violation; • non-compliance with the terms of the information security policy in good faith; • low level of computer literacy; • careless handling of confidential information.

**DISCUSSION**

Based on the above information, it is necessary to analyze the current information security policy in the enterprise and define the task of developing a new information security policy. To review the current state of data protection in the enterprise, it is necessary to use the MARION (MARION) method. This method was invented in France by Assemblie Plinihre des Sociitis d'Assurances contre L'Incendie et les Risques Divers (APSAIRD) and improved by Club de la Sicuriti Informatique Frangaise (CLUSIF). The method is the de facto standard for computer risk detection. Designed according to ISO-SC27-WG1 standard. About a thousand security plans of information systems in the world have been calculated according to the MARION method. The essence of the methodology is to formulate basic, basic questions and their answers. Scores from 1 to 4 are used as answers:

1 is a negative rating, that is, a high level of threat; 4 is a positive rating, meaning the threat level is low.




3- picture. Methods of loss of confidential information.

Each criterion (question) has its own "weight", that is, information protection This criterion is determined separately according to the specific characteristics of the organization. The review of the security level consists of 6 sections, in which the main factors are evaluated. The assessment is carried out using the following formula:

Protection Level = Max. Ric - (S. Ric / P. Ric), here Max. Ric is the maximum risk level, 3 is taken as the maximum level.

That is, the gradation of risks looks like this:

• Max. Ric < 1 – low level of threat;

• 1 < Max. Ric < 2 – medium level of threat;

• 2 < Max. Ric < 3 – high level of threat.

S. Ric is the relative value of risks and it is by the following formula is calculated: the criterion value * to its "weight".

P. Ric is the "weighted" sum of the grades.

Analyzing the current information security policy is current in the enterprise it is necessary to review and analyze the developed software. This analysis necessary to review a potential vulnerability in the software being used. See the list of programs used in the enterprise in Table 1. can:

Table 1. List of enterprise information systems and software

| № | Systems and programs |
|---|---|
| 1 | Ijro.gov.uz – inter-departmental executive discipline system |
| 2 | e-qaror.gov.uz – by local government authorities development, agreement and registration of decisions to be made single electronic system of transfer |
| 3 | e-hujjat – local electronic document exchange system |
| 4 | e-tahlil – sector activity control system |
| 5 | collective.uz – effective team management system |
| 6 | exat – e-mail protected |
| 7 | murojaat.fergana.uz – applications portal |

All computers in the enterprise run Windows 10 x64. MMHT software package to transmit electronic documents, including confidential information includes.

Table 2. Comparison of enterprise software

| Name of the software | Protection with a password | From the certificate use | Owning a WEB-interface | Secure connection channel availability | Confidential / private | Software for the organization |
|---|---|---|---|---|---|---|
| Eqaror.gov.uz | + | + | + | + | + | + |
| Ijro.gov.uz | + | - | + | - | + | - |
| Collective.uz | + | + | +- | - | - | - |
| Exat | + | + | +- | - | + | + |
| e-hujjat | + | - | - | - | - | + |
| e-tahlil | + | - | - | - | - | + |
| murojaat.ferghana.uz | + | - | + | - | - | - |

In this regard, data transfer is a secure VPN-type connection through the channel. Authentication in a secure communication channel is carried out using an electronic certificate.

It should be noted that the standard MS Office package is not included in the list in Table 1. Authentication in systems using an electronic certificate PIN code is done using An antivirus is mandatory on every computer software is installed.

As you can see from the table above, 8 out of 5 software products very important for the work of the organization. In other words, if this software in the event that one of the products malfunctions or ceases to function to a significant extent, or can completely disrupt the work of the organization.

Using the interface comes with various risks of information that is expressed. + - is installed both on the WEB-interface and on the local network a software product that supports working in distributed form is defined. Electronic certificates - software for working with electronic documents used in products. Certificate authentication is one-phase, i.e. password (PIN code). In the reviewed aspects of the current state of information security policy to make the following conclusion, taking into account the sum of identified shortcomings possible: currently the enterprise has a vulnerability in the form of internal threats and is current it is necessary to improve the information security policy. In this way, the task of developing an information security policy is correct should be formed.

**CONCLUSION**

The current state of industrial enterprises related to the provision of information security of economic resources is analyzed. The current policy of economic resources of information security of industrial enterprises, the journal in which all important comments are entered, and means of protection (software and engineering tools) were considered. The purpose of this analysis is to disclose or leak confidential information in order to identify shortcomings and weaknesses that may lead to a result. In addition to the review and analysis of the current situation in the field of economic resources of information security, any laws that may lead to data leakage have been corrected, as well as explanations and instructions for elimination have been given. To summarize, review the developed and analyzed current information security policy and identified weaknesses. Information security defines the task of policy development.

**REFERENCES**

1. F.W. Taylor Principles of scientific management/ F.W. Taylor // Controlling. - M. - 1991. - 184 p.

2. J. Stacy Adams «Inequity in Social Exchanges» in Berkowitz, ed. Advances in Experiential Social Psychology. NY: Academic Press, 1965, pp. 267-300.

3. Walter B. Newsome. Motivate, Now, 1992. - P. 458.

4. A.M. Yugay Economic relations and motivation for the development of innovative technologies in agriculture (theory and practice) / A.M. Yugay. – M.: MSHA, 2002. - 582 p.

5. B. X. Muradov. Improvement of organizational and economic mechanisms for the development of coal industry enterprises in a strategic approach. «Industrial Economics and management: problems and solutions».//The on topic of II-collection of materials of international scientific-practical conference. International scientific-practical conference is a collection of articles and abstracts. Department of «Industrial Economics and management of the faculty" engineering technologies». TSTU named after Islam Karimov. T.: 2022. 22.05.144-147 p.

6. B. X. Muradov. Public-private partnership to ensure the current economic stability of the coal industry in educational institutions in the energy sector. «Industrial Economics and management: problems and solutions».// The on topic of II-collection of materials of international scientific-practical conference. International scientific-practical conference is a collection of articles and abstracts. Department of «Industrial Economics and management of the faculty» engineering technologies".TSTU named after Islam Karimov. T.: 2022. 22.05.141-144 p.

7. Б. Х. Мурадов Энергия ишлаб чиқаришда кўмир саноати корхоналарини ривожлантиришнинг замонавий холати ва уларга таьсир этувчи омиллар.// «Инновацион техника ва технологияларнинг қишлоқ хўжалиги озиқ-овқат тармоғидаги муаммо ва истиқболлари».// II-Халқаро анжуман илмий ишлар тўплами. - Тошкент. ТошДТУ, 2022. 22-23 апрель Тошкент. 484-498 вароклар

8. B. X. Muradov. The modern state of development of Kumir industrial enterprises and the factors influencing them.// "The role and significance of digital life and Social Sciences in the upbringing of a harmonious generation: current issues and prospects."// International scientific and practical conference collection of scientific articles and theses. III-IV-subsidiary. Andijan AndMI, 2022. April 12. 2022 Andijan. 292-296 sheets. 5 b.

9. B. X. Muradov. Features of the development of organizational economic mechanisms of modern industrial enterprises.// "The role and significance of digital life and Social Sciences in the upbringing of a harmonious generation: current issues and prospects".// International scientific and practical conference collection of scientific articles and theses. III-IV-subsidiary. Andijan AndMI, 2022. April 12. 2022 Andijan. 296-300 sheets. 5 b.