SCIENTIFIC, METHODICAL AND PRACTICAL ASPECTS OF ACCOUNTING, FINANCIAL, INFORMATION, LANGUAGE AND COMMUNICATIONAL SUPPORT FOR SUSTAINABLE DEVELOPMENT OF AGRARIAN SECTOR

COLLECTIVE MONOGRAPH

DNIPRO
2 0 2 4

6. The Ministry of Finance of Ukraine (2000). Polozhennia (standart) bukhhalterskoho obliku 11 «Zoboviazannia » [Regulation (standard) of accounting 11 «Obligations»]. Available at: https://zakon.rada.gov.ua/laws/show/z0085-00#Text (Accessed 18 Dec 2022).

7. Mizhnarodni standarty finansovoi zvitnosti [International Financial Reporting Standards]. Available at: https://mof.gov.ua/uk/mizhnarodni-standartizvitnosti (Accessed 18 Dec 2022).

8. The Ministry of Finance of Ukraine (1999). Nakaz Ministerstva finansiv Ukrainy «Pro zatverdzhennia planu rakhunkiv bukhhalterskoho obliku ta Instruktsii pro yoho zastosuvannia» [Order of the Ministry of Finance of Ukraine «On approval of the chart of accounts and Instructions for its application»]. Available at: https://zakon.rada.gov.ua/laws/show/z0892-99#Text (Accessed 18 Dec 2022).

9. Hilorme, T. V. and Shachanina, Yu. K. (2018). Udoskonalennia orhanizatsii obliku kredytorskoi zaborhovanosti pidpryiemstv v umovakh nevyznachenosti [Improving the organization of accounting for accounts payable of enterprises in conditions of uncertainty]. *Economics and finance*, vol 1, [Online], pp. 18–24. Available at: https://www.researchgate.net/publication/342850495_udoskonalenna_organizacii_obliku_kreditorskoi_zaborgovanosti_pidpriemstv_v_umovah_neviznacenosti (Accessed 18 Dec 2022).

10. Accounts payable audit. [Automated, 360 audit protection for compliance made easy] [Online]. Available at: https://www.intellichief.com/ accounts-payable-audit (Accessed: 18 Dec 2022).

3.3. INFORMATION SECURITY OF MANAGEMENT OF THE SYSTEM OF ECONOMIC SECURITY OF THE ENTERPRISE AND ITS IMPROVEMENT

Tatiana Machak,
senior teacher of Department of Accounting, Taxation and Management of Financial and Economic Security,
Dnipro State Agrarian and Economic University, Ukraine

Summary. In the modern conditions of information transformation, the need to ensure the protection of information resources of the enterprise appears quite acutely.

Of great importance in the management system of economic security of an agrarian enterprise is information support, which is a set of information, accounting, regulatory sources and methods of assessment and analysis of the level of economic security of the enterprise.

The issue of protection of information sources during the processing, storage and exchange of accounting and management data and the development of a plan to minimize the impact of possible threats and dangers of various origins during the activity of agricultural enterprises require constant attention.

Since threats to the information security of the enterprise can arise under the influence of both internal and external factors, ensuring the appropriate level of information protection is important for the decision-making process of the management and directly affects the state of economic security of the enterprise

Keywords: economic security, security management, information security, ensuring information security, information protection

Modern business conditions encourage businesses to open up new opportunities and make more creative and technical decisions. This process is always accompanied by increased vulnerability of the enterprise, which can worsen the state of its economic activity. Therefore, it is important to focus attention on the issues of creating an effective system for ensuring the economic security of the enterprise.

The relationship between economic security is mostly determined by the multifaceted interpretations and is related to such concepts as "risk" and "danger". This interaction is based on uncertainty, and is a source of potential threats to the company's security. This requires a deeper study of internal and external factors that can affect economic security. Understanding and systematizing different types of threats can allow businesses to respond in time and prevent their occurrence.

Let's consider the concept of "security", which is interpreted from the Greek language as "owning the situation". This category is usually understood as a state of security or a state of absence of threats, in which all the vital interests and needs of a person are preserved and the conditions for its normal functioning are met. Ensuring security includes such aspects as physical, social, informational and economic security and is aimed at ensuring stability and protection from dangers.

At the end of the last century, especially during the rapid development of

economic ties and technological progress, the concept of "economic security" began to be widely used.

Modern business conditions encourage businesses to open up new opportunities and make more creative and technical decisions. This process is always accompanied by increased vulnerability of the enterprise, which can worsen the state of its economic activity. Therefore, it is important to focus attention on the issues of creating an effective system for ensuring the economic security of the enterprise.

The relationship between economic security is mostly determined by the multifaceted interpretations and is related to such concepts as "risk" and "danger". This interaction is based on uncertainty, and is a source of potential threats to the company's security. This requires a deeper study of internal and external factors that can affect economic security. Understanding and systematizing different types of threats can allow businesses to respond in time and prevent their occurrence.

Let's consider the concept of "security", which is interpreted from the Greek language as "owning the situation". This category is usually understood as a state of security or a state of absence of threats, in which all the vital interests and needs of a person are preserved and the conditions for its normal functioning are met. Ensuring security includes such aspects as physical, social, informational and economic security and is aimed at ensuring stability and protection from dangers.

At the end of the last century, especially during the rapid development of economic ties and technological progress, the concept of "economic security" began to be widely used.

In addition, it is equally important to develop and implement effective strategies and policies aimed at preventing negative impacts and ensuring the enterprise's resilience to various economic and financial challenges. Successful management of economic security also involves constant monitoring and updating of security strategies and measures in order to adapt to the changing conditions of the external environment and the constant evolution of market conditions. A key aspect of economic security management is also the involvement and support of personnel involved in the decision-making process and implementation of security strategies. An informed and trained workforce is an important resource for effective risk management and economic challenges. Finally, cooperation with stakeholders such as partners, customers, government authorities and other interested parties plays an important role in ensuring the economic security of the enterprise. Interaction with

stakeholders can facilitate information sharing, joint problem solving, and risk minimization. We will define and analyze the constituent elements of economic security (Fig 1.).

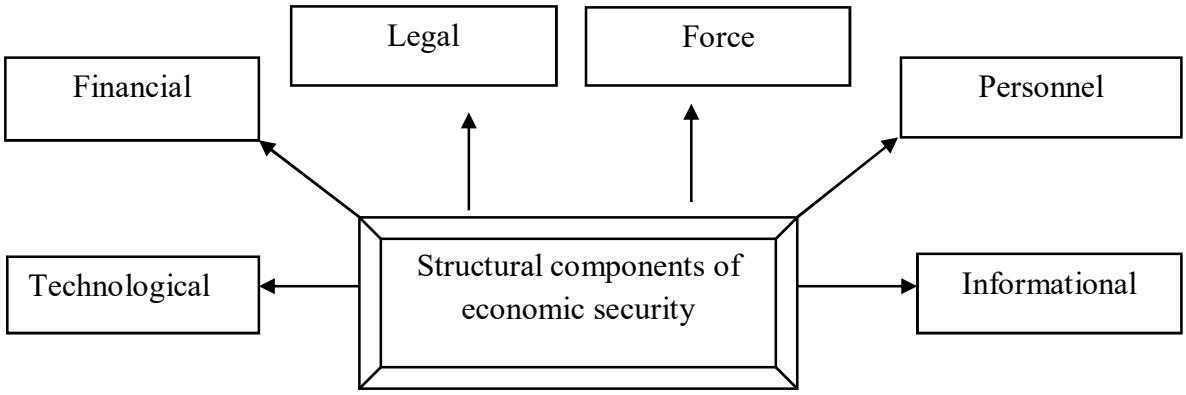

Fig. 1. The general structure of elements of economic security of the enterprise

The structure of elements of economic security is individual for each enterprise and depends on various influencing factors. The specified security elements closely interact with each other and form the foundation for the sustainable development of the enterprise. Considering each component of economic security separately, it can be determined that some of them are aimed at solving internal production aspects. This includes financial security, legal security, environmental security, force security, personnel security - all of them are important, but in our opinion, information security acquires special importance in today's conditions. In the conditions of military aggression against our country, it became obvious how important it is to timely identify and protect information, preserve its confidentiality and integrity.

With the intensive development of private property and telecommunication technologies, information security occupies one of the important places in the structure of economic security of enterprises. Reliable preservation of any information about the enterprise or its employees is crucial for the development and reduction of risks of the enterprise at all stages of its activity.

The information component in the system of financial and economic security acts as an integral part of management and strategic decision-making at the enterprise. It provides management with the necessary basis for analyzing the current financial situation and forecasting future prospects. Information support includes the collection, processing, analysis and interpretation of financial data, which allows you to make informed decisions at different levels of management.The importance of the information component lies in the fact that it contributes to the timely detection of risks, fraud and other potential threats to the financial stability of the enterprise.

Proper management of information flows allows you to effectively respond to changes in the internal and external environment, maintain a competitive advantage and ensure stable development. In addition, proper information support ensures compliance of the company's financial activities with the requirements of legislation and international standards. The informational component also contributes to increasing transparency and trust in the company's activities among stakeholders. Summarizing, information security acts as an important tool for managing financial and economic security, which determines the success and sustainability of the enterprise in the modern business environment. Information security is a multifaceted concept that is considered by modern scientists from different perspectives.

Information security is a key aspect of today's digital environment, defined as the protection of information from unauthorized access, loss, or destruction. Ensuring information security involves the implementation of technical, organizational, and legal measures to ensure confidentiality, integrity, and availability of information. In today's world, information security has become especially important due to the proliferation of cyber threats that threaten both the corporate sector and government systems. The concept of information security covers such aspects as protection against cyber attacks, protection of personal data, security in information systems and networks. The importance of information security lies in the fact that it affects the stability of the economy, the protection of state secrets, the privacy of personal information, as well as the ability to innovate and develop. Inadequate information security measures can lead to serious consequences, including financial loss, breach of trust and breach of privacy. Thus, effective management of information security is an integral component of modern risk management strategies and protection of the interests of organizations and society as a whole.

From a classical point of view, information security is a set of rules and tools that protect sensitive (important, confidential) information from misuse, corruption, unauthorized access or destruction.

Having analyzed various points of view of scientists, we highlight the main concepts of this concept of "information security":

- State of security of the information environment;

- The process of managing risks and dangers aimed at ensuring the sovereignty of Ukraine;

- Protection of the rules established by law, according to which information

processes take place in the state;

- An integral part of political, economic, defense and other components of national security.

Many of the latest technologies are involved in the work of modern enterprises, which actually replaced paper media and facilitated the processing, collection, use and storage of information. At the same time, placing confidential information on digital media significantly increases the risks of theft, distortion, alteration, recording and destruction of information. These threats indicate low protection of the company's information security system.

Let's determine the primary goals and objectives of the information policy, which determine the foundations and formation of the enterprise's security system.The main objectives of the information policy include:

- ensure preservation of confidentiality (sensitivity) of information;

- ensure the completeness and integrity of information data (guaranteeing the inviolability of data);

- compliance with the requirements of legislation, regulations and standards of information security according to which the enterprise is managed;

- ensure the availability of information (maintaining continuous access to information);

- training of employees and their awareness in the field of information awareness;

-monitoring of information systems to identify and timely respond to potential threats;

-destruction of confidential information that has lost relevance for the enterprise, but can be used by third parties;

- ensuring compliance of information processes and systems with data security standards and regulations;

- determination of responsibilities and duties of personnel in the field of information protection, as well as control of their implementation;

- ensuring backup and recovery of information in case of its loss or damage;

-establishment of information protection audit and monitoring mechanisms to assess the effectiveness of security measures;

- development and implementation of incident response procedures for quick and effective resolution of information security breaches;

- ensuring constant improvement of information policy and security measures in accordance with changes in the internal and external environment of the enterprise.

When determining the tasks that precede the formation of information security, it is necessary to conduct research and identify possible threats.

The concept of "threat", in this case, can be interpreted as a violation of the state of information security and encroachment on the appropriation of information. At the same time, such threats can arise both inside the enterprise and from the outside.

Threats to information security are a set of existing and potential factors that pose a threat to the interests of both individuals and society in the information space. These include:

-threats from the influence of unreliable information on the material condition and performance of the enterprise;

-threats from unauthorized and illegal influence of third parties on the company's information assets;

-threats to the company's informational rights (the company's intellectual property rights, the rights to use and transmit information, to disseminate information, etc.).

Informational threats that carry danger can be determined by various factors: natural (natural disasters, fires, earthquakes, floods, etc.) and anthropogenic. Anthropogenic factors include threats of a random nature. These can be errors in the processing and exchange of information and threats made on purpose. Often, such errors occur as a result of mistakes made by the company's employees themselves. Accidental and intentional threats negatively affect both information users and the effectiveness of the enterprise.

Threats to information security should be divided into those that arise inside the enterprise and those that come from outside.Internal threats include:

- irrevocable loss of information as a result of unprofessional actions of employees;
- unintentional or intentional distortion of information;
- negligence of personnel;
- low state of awareness of employees in the field of information security;
- leakage of confidential information to internal employees;
- improper use of technical means.

External threats to information security include:

- leakage of confidential information as a result of inadvertent actions of employees of third-party institutions;

- leakage of confidential information as a result of deliberate actions of employees of third-party institutions;

-malicious software, hacker attacks, spam;

- illegal activity of competitors;

-physical threat to the life and health of an employee, a carrier of confidential information;

- natural phenomena.

The lack of a timely response to such threats can lead to problems in cooperation with partners, damage to the business reputation of the enterprise, damage or complete loss of information resources, as well as financial losses and other negative consequences. A slow or ineffective response to information security threats can also lead to a loss of trust from customers and partners, which can affect the profitability of the enterprise. Inadequate information protection may violate data privacy laws and lead to regulatory sanctions. In addition, information security incidents can cause a loss of competitive advantage because they can become the subject of public criticism and negative feedback. Breach of data confidentiality or integrity may also result in legal action from affected parties or customers. In addition, a negative impact on the company's image can occur due to irresponsible management and the lack of an effective crisis management system. For example, a poor response to security incidents can lead to panic among customers and investors, which can cause a company's stock value to fall. In summary, protecting information security is critical to ensuring the sustainability and success of any organization in the digital world.

The vulnerability of an enterprise to internal and external threats is determined by various factors and is individual for each enterprise.Balanced management decisions aimed at ensuring the economic security of the enterprise affect the reliability of information and make it possible to correctly use information for adaptation to changes and strategic development. Therefore, the main task of information security of the enterprise is to prevent the use of its important information resources by external users, as well as the accumulation of important information by competitors about the internal activities of the enterprise. This means

ensuring that only authorized users have access to critical information, ensuring data integrity and protecting it from unauthorized changes. Preventing the leakage of confidential information outside the enterprise is an important component of information security. This includes protection against malicious actions by external actors such as cybercriminals, spies or competitors. The enterprise must also implement strategies to protect against internal threats, such as employee negligence or abuse of access privileges. Effective management of access to information resources includes the application of the principles of the necessary minimum and the principle of division of duties. Regular inspection and audit of information systems helps to identify possible weaknesses and ensure their correction. The development and implementation of a security policy that covers both technical and organizational aspects is a key element of an effective information security strategy. Staff training on security issues and practical aspects of using information systems also plays an important role in ensuring the security of the enterprise.Summarizing, the information security of the enterprise requires a comprehensive approach and constant improvement of protection strategies and measures.

Therefore, special attention is paid to aspects of interaction and coordination of all departments of the enterprise in the process of collecting, processing and storing important information. All received information can be classified according to the appropriate levels of sensitivity (importance, confidentiality). The degree of sensitivity of the information is decided by the management of the enterprise.

The first level includes "critically important" information - information, the leakage (distribution) of which can lead to significant negative consequences of the operation of the enterprise and poses critical financial and image threats.

The second level includes "important" information - information, the leak (distribution) of which causes material and image damage and significantly affects the efficiency of the enterprise.

The third level includes "useful" information - information, the leak of which causes material damage to the enterprise, but does not affect its effective operation.

The fourth level includes "insignificant" information - information, the leak of which does not cause material damage to the enterprise and does not affect its activities

The information of the first three levels is the most sensitive (it is considered a commercial secret) and is an influential resource of the enterprise. Information

security is an important component of management, ensuring the protection and preservation of valuable information.

To ensure information security, it is necessary to solve a number of tasks to ensure the dynamic and effective development of the enterprise. The development and availability of an effective information security plan will provide an opportunity to take into account possible threats taking into account the specific directions of the enterprise.When developing an information security plan, special attention should be paid to solving the following tasks:

1) provision of management personnel with the necessary information to make balanced management decisions;

2) timely prediction and assessment of threats to the enterprise's activity;

3) prevention and minimization of possible threats to the enterprise;

4) predict the causes of dangers and threats to information resources that affect material damage and disruption of its stable functioning;

5) create a mechanism for rapid response to identified dangers to the company's information sources;

6) develop an information policy and regularly conduct work with the employees of the divisions regarding the issues of ensuring the protection of the confidentiality of the company's information sources;

7) determine the circle of employees who have access to the use of information sources of the enterprise and control to prevent the dissemination of information to persons who do not have access to such information both internally and externally;

8) develop a procedure for destroying confidential information that has lost its relevance for the enterprise, but can be used by third parties.

The main goals of ensuring the information security of the enterprise:

- searching for and obtaining information necessary to ensure the effective development of the enterprise and its security system in the conditions of the occurrence of risks, threats and dangers of the market economy;

- exclusion of the use of unreliable information in the enterprise management system;

- prevention of unauthorized access to information resources of the enterprise;

- prevention of leakage, theft and loss of information;

- prevention of distortion and falsification of information used in enterprise management;

- prevention of unauthorized actions to destroy, copy and block information;
- protection of intellectual property rights at the enterprise.

Information security as an important element of economic security covers all processes of enterprise management, including measures to ensure the completeness, integrity and availability of information sources. Ensuring the completeness of information sources includes measures to preserve all necessary information without loss or distortion. Protecting data integrity involves preventing unauthorized changes or loss of information that could lead to erroneous decision making. Ensuring the availability of information resources is important for ensuring uninterrupted business processes and prompt response to changes in the environment. Information security also includes measures to protect against the leakage of confidential information, which can cause significant losses to the enterprise.Effective information security helps to prevent risks of financial losses, as well as to maintain the trust of customers and partners. Ensuring information security helps to increase the productivity and efficiency of the enterprise. It also helps to reduce the risks of offenses and loss of reputation. The introduction of information security standards contributes to the harmonization of management processes and ensuring security at the level of international standards. Summing up, information security is a necessary condition for the sustainable and successful functioning of any enterprise in the modern digital environment.

An optimally formed information security plan will give the enterprise the opportunity to achieve economic stability and effectively resist threats of various nature, which contributes to the reliable protection of important information and ensuring the smooth functioning of business processes. Optimizing information security helps a business improve its reputation and the trust of its customers, as they can be sure of the security of their data and the confidentiality of the information they provide. In addition, effective information security management can reduce the risks of legal and financial losses related to potential privacy breaches or data loss that may occur as a result of cyber attacks or internal security breaches. In general, an optimally formed information security plan becomes a strategic tool for achieving the stability and success of the enterprise in the conditions of the modern digital environment.

Ensuring legality and compliance with current legislation is an important element in the management and decision-making system at every enterprise. The

legal reflection of information security is a set of legislative norms and standards aimed at regulating the processing, storage and transmission of information in order to prevent unauthorized access, leakage or violation of data confidentiality. This system of measures determines business rules, defines security standards, and establishes responsibility for non-fulfillment of information security requirements.In addition, the legal regulation of information security may include mechanisms for checks and audits to ensure compliance with security standards. Legislation in this area may also determine mandatory requirements for reporting and documenting information security procedures. This helps preserve evidence of compliance with legal requirements and compliance with safety standards. Summing up, the legal regulation of information security establishes the basic principles, requirements and responsibilities necessary to ensure the security and protection of information in the modern digital environment. Legal protection of information sources is determined by a significant amount of regulatory and legislative framework both at the international and state levels. In our country, the main document that defines the security provisions is the Constitution, which indicates that: "a person, his life and health, honor and dignity, inviolability and safety are recognized as the highest social values in Ukraine." There are a number of current regulatory documents on information protection, including: Law of Ukraine "On Information", Law of Ukraine "On Protection of Information in Information and Telecommunications Systems", Law of Ukraine "On State Secrets", Law of Ukraine "On Protection of Personal Data" , Resolution of the Cabinet of Ministers of Ukraine "On the procedure for record-keeping, storage, use and destruction of documents and other media containing official information" and others.

Requirements for the formation of information security must be taken into account at all levels of legislation and cover various aspects of information protection. This approach will contribute to the effective protection of information of various industries at all levels of legislation:

-Constitutional legislation - norms and rules on information protection included in the constitutional legislation (Constitution of Ukraine);

-General legislation - rules on informatization and information protection, laws, codes (on property, on citizens' rights, on citizenship;

-Laws on the organization of management in relation to individual structures of the economy, economy, and state bodies, including issues of regulation and

protection of information;

- Special legislation - a set of legal norms regarding ensuring information security of various sectors of the economy (Law of Ukraine "On Information", Law of Ukraine "On Protection of Information in Automated Systems");

- Law enforcement legislation - provisions and norms of responsibility for violations in the information sphere.

Examining the legislative framework, a separate section can be used to highlight special legislation, which defines the legal foundations of various areas of enterprise activity. Such regulatory documents include the Law of Ukraine "On Information" and "On Protection of Information in Automated Systems". These laws establish the basis of legal definition of important elements of information activity, such as: information and information system; subject of information processes; owners (sources) of information, etc.Therefore, the protection of information of enterprises of various fields at the legislative level is ensured by a complex of different-level legislative acts, starting from the Constitution of Ukraine and ending with internal documentation: agreements, contracts, developed regulations, accounting and management accounting data that are subject to protection.

When forming the information policy at the enterprise, it is necessary to thoroughly work out the sections and articles of the Law of Ukraine "On Information", review and analyze the Resolution of the Cabinet of Ministers of Ukraine "On the procedure for record-keeping, storage, use and destruction of documents and other media containing official information", and as well as the main legal framework related to information security of the enterprise. This guarantees compliance of the information provision of the company's activities with legal norms and will reduce the risks of violations.

When making effective financial decisions, managers must have full information about the financial status of the enterprise.

Information sources provide the necessary information for making strategic decisions, protecting confidential information, and also ensure timely detection and response to threats and incidents in the field of cyber security. Information sources are divided into:

- Internal sources - information that is created, processed and stored within the enterprise itself. These can be databases, financial reports, reports on enterprise activity, event logs, and more. For example, internal customer databases can help

ensure the security of personal data.

- External sources - information that comes from outside the enterprise and can be useful for analyzing the market, competitors, potential threats, etc. This may include predictive analytics reports, cyber threat reports and others. For example, cyber threat reports from external sources can help identify potential risks to information security.

- Expert sources - information that comes from experts in the relevant fields or consultants. This may include consulting with cyber security specialists, legal advisors on data protection compliance, etc. For example, consulting on the implementation of data protection measures can provide a better understanding of potential threats and measures to prevent them.- Specialized information services and software tools - information systems and programs that specialize in collecting, analyzing and monitoring information about cyber security threats. These can be intrusion detection systems, antivirus programs, network monitoring programs, etc. For example, intrusion detection systems may detect abnormal network activity that may be a sign of a cyber attack.

The importance of these sources is that they help businesses collect, analyze and use information to ensure the security of their information and data. They help to respond to threats in a timely manner and effectively manage risks arising in the field of cyber security.

An important category of information sources is accounting information for ensuring the economic and informational security of the enterprise. It includes all information related to financial activities, accounting of resources, financial reports and other financial data of the enterprise

Account information is a key aspect in the information provision of the enterprise's economic security system. In order to make correct and well-founded decisions, the manager needs prompt, high-quality and timely information about the company's activities and financial condition. This can minimize the existing risks and dangers and ensure the sustainable and efficient development of the company. Correctly organized accounting information allows management to obtain a complete and objective picture of the company's financial activity. It includes:

- information about the financial state of the enterprise, such as profit and loss statements, balance sheets, cash flow statements. This information helps to identify financial risks and make financial management decisions;

- detailed information on all operations carried out within the framework of the company's activities. This includes records of purchases, sales, payment transactions, payroll, etc. This information helps detect fraud, internal espionage and other types of financial manipulation;

- information necessary for compliance with tax legislation and reporting to tax authorities.It contains important data about taxable income, expenses, tax obligations;

- generalized information (reports) compiled by independent auditing firms that check the company's financial statements. These reports help confirm the reliability of financial information and identify possible violations or deficiencies in accounting;

- computer systems used to automate financial accounting, including accounting, cost control, inventory management, etc. They help ensure the accuracy, integrity and confidentiality of financial information.

Accounting information is the basis for making financial decisions, as well as an important source for identifying and managing risks in the field of finance and accounting.

In addition, accounting information allows analyzing the efficiency of the use of enterprise resources, identifying potential sources of cost optimization and increasing profitability. This helps the management to make informed decisions regarding investment, development of new projects and strategic planning. Operational and timely accounting information is a key factor in risk management and adaptation to changes in the financial environment. It allows you to quickly react to changes in market conditions, strategically review business plans and, if necessary, adjust them.

Properly organized accounting information is also important for compliance with legal requirements and financial reporting standards. It allows the enterprise to avoid fines and other negative consequences associated with violation of requirements in this area.

Obtaining operational, high-quality and timely accounting information is key for managers in making correct and well-founded financial decisions. This allows them to analyze the financial state of the enterprise, identify trends and predict future results. Knowledge of current financial data allows management to respond in time to changes in the internal and external environment. This helps reduce risks and ensures more accurate management of the company's financial resources. Access to accounting information allows managers to identify effective and ineffective aspects

of operations, which allows to optimize business processes and increase profitability. Account information is also important for internal and external audits, which helps to ensure compliance of the company's activities with legislation and standards. However, insufficient or inaccurate accounting information can lead to incorrect decisions and losses. Therefore, it is important that accounting information is reliable, valid and adequate. Ensuring the accuracy and availability of accounting information may require the development of effective accounting and reporting systems, as well as training of personnel in the proper collection and analysis of financial data.Summing up, accounting information plays an important role in the process of enterprise management, providing management with the necessary data for effective strategic and operational decision-making.

Accounting indicators are important sources of information when carrying out activities at the enterprise. On the basis of these data, it is possible to objectively establish and evaluate the financial condition of the enterprise and the prospect of its development.

Sources of information can be various accounting documents. The presence and movement of cash funds of the enterprise is reflected in income and expenditure orders, journals of registration of documents on the receipt and outflow of cash, generalized information on cash funds is formed in the cash book and registers of synthetic accounting by account. In addition, cash flow information can also be gathered from bank statements, which reflect all financial transactions related to the company's bank account, such as account top-ups, cash withdrawals, payments, interest accruals, etc. Additionally, cash flow information can be stored as part of a company's financial statements, such as a cash flow statement, which shows all cash flow over a period of time, allowing management to analyze financial results and make informed management decisions.

Information about the availability and movement of funds in bank accounts (non-cash settlements) is reflected in the bank statement, which is generated by the bank institution in which the company's current account is opened. The account statement is formed on the basis of such primary documents as a payment order, a payment request of the order. In addition, the bank statement may include information about commission costs, bank interest and other costs related to account transactions. These data are used to monitor the movement of funds in the company's bank account, as well as to prepare financial statements and analyze the company's

financial condition. A bank statement is an important source of information for the company's management when managing financial resources and making strategic decisions

Documents such as an invoice, an expense invoice (recording the fact of receiving goods), a goods transport invoice (contains information on the transportation of goods from the seller to the buyer) are the sources of information on transactions involving the purchase and sale of products. Information, Primary information about the completion of any works and their acceptance by the customer are reflected in the Act of completed works. The accounting certificate is an important source of corrected information after accounting errors have been corrected.

Synthetic and analytical accounting information is the basis for the formation and generalization of financial reporting indicators. In turn, financial reporting is an important source of information that users use to assess the current state of business and make management decisions for the further development of the company.

The founding documents of the enterprise are important sources of information. Such documents include the articles of association, the founding agreement, and the order on the accounting policy.

The charter of the enterprise contains data on: the owners of the enterprise, determining the size of the shares of each of them, the full name of the institution, the form of ownership, types of activities, legal address, defines the subject and goals of the activity, the composition of the property of the enterprise, the terms of termination of activity and other information necessary for the management of the enterprise . The charter of the enterprise is an important tool for the management of the enterprise, as it defines the basic principles and rules according to which the enterprise functions and establishes the framework for making strategic decisions. Its careful implementation is key to ensuring the stability and success of the enterprise

An important source that determines the methods of organization of accounting at the enterprise is the information data of the order on the accounting policy. This document informs about the selected principles and methods of accounting, namely: methods of estimating the disposal of stocks, methods of calculating depreciation of fixed assets, methods of revaluation of non-current assets, the order of payments and distribution of profit, the order and basis of distribution of general production costs and other information that affects indicators financial result of the enterprise. This

document also establishes the bases for the distribution of general production costs, which helps to determine the cost of production and the final cost of products. The information order on the accounting policy is a tool for ensuring internal control over the company's financial activities and compliance with accounting standards. Compliance with the principles and methods established in the order helps to avoid errors and risks when preparing financial statements. An accounting policy order may also include requirements for documenting financial transactions and keeping records. Summarizing, this document is an important element of managing the financial activities of the enterprise, which defines the main accounting principles and rules necessary to ensure the accuracy and reliability of financial reporting.

The provision of information allows the enterprise to monitor, analyze and systematize various areas of its activity in detail, which helps to respond to threats in a timely manner, which ensures the security of the enterprise. An effectively developed accounting system is the foundation of the information support of the enterprise management system. The accounting system, in which financial data appears, is an extremely important component of this process. It not only ensures the accuracy and reliability of financial reporting, but also allows the company's management to identify trends in financial indicators in a timely manner and analyze them. Thanks to the accounting system, it is possible to effectively monitor the movement of funds, control expenses and income, assess the financial situation of the enterprise and identify possible risks and threats in a timely manner. This allows you to avoid financial difficulties and ensure sustainable business development. In addition, the accounting system ensures compliance of financial statements with the requirements of legislation and standards, which is important for the enterprise as a legal entity. This allows you to avoid fines and other negative consequences from the non-compliance of financial reporting with the requirements. The accounting system is the foundation of information support for effective enterprise management, because it ensures the accuracy, reliability and timeliness of financial information necessary for making strategic and operational decisions.

An effective way to form such a system is to divide information sources into appropriate levels:

Level 1. Operational (primary) information - Operational information - current (detailed) accounting information about operations, its collection and registration. The main purpose of forming operational information is to ensure current control and

management, confirm the fact of operations, and also form the basis for analysis and generalization of information at the following levels. An effective accounting system includes the use of modern information technologies to automate accounting processes and data analysis. It allows not only to monitor financial indicators, but also to analyze them dynamically, compare them with previous periods and establish trends, which helps to make informed management decisions. Additionally, it is important to note that the accounting system also plays a significant role in ensuring internal control and compliance with legislation. It helps identify possible financial risks and ways to manage them, reducing the likelihood of financial violations. Effective provision of information, in particular through the accounting system, is a key element for ensuring the security and stability of the enterprise, as it allows timely detection and response to possible threats and risks.

Level 2. Generalized information of financial and management accounting.

Financial information - generalized information about the state of the enterprise, namely, financial statements, balance sheet, cash flow statement, financial results report;

Management information - information aimed at decision-making, namely, strategic development plans, main indicators of efficiency and productivity, enterprise costs. The main goal is to provide generalization of accounting information for planning and timely management decisions, providing information for strategic planning and effective management of enterprise resources, as well as preparation of reports for users.

Level 3. Generalized analytical information - Detailed analysis of accumulated information, assessment of current and strategic tasks of the enterprise. Assessment of possible threats and dangers. The main goal is to ensure management decision-making. Helps in forecasting and prevention of unconditioned risks

Each level of information defines a personal goal in ensuring information security: starting with the preparation of the primary document, which records the fact of the transaction, ending with the formation of financial statements and a general assessment of the financial and economic state of the enterprise.

At the first level, operational information is displayed, which provides detailed information about current operations, allowing accounting and control over them. Such information is usually used by internal users for analysis and further generalization.The second level includes generalized financial and management

information, on the basis of which financial statements are formed, economic indicators of activity are analyzed and important decisions are made for the effective development of the enterprise. The third level contains generalized analytical (detailed) information for evaluating current activities and solving important issues of optimizing the management process and minimizing enterprise risks.

In the conditions of a constantly growing amount of information, it is important to examine all levels of information sources when forming the economic security of an enterprise and ensuring its information security. This will allow the management of the enterprise to make balanced and justified decisions regarding the effective development and minimization of possible threats and dangers in the process of managing the economic security system.

Effective enterprise management is an important element at all stages of business and depends on various factors. Without the formation of a proper state of information support, the enterprise management process becomes extremely vulnerable and ineffective. Therefore, information provision plays a significant role in ensuring the economic security of the enterprise and acts as a special object in the activities of management personnel. The availability of appropriate information support helps to optimize management processes, increases the speed of reaction to changes in the environment and allows effective use of market opportunities. Information support also helps to avoid risks and minimize possible negative consequences in enterprise management. For example, receiving timely information about changes in legislation or the competitive environment allows the enterprise to adapt to new conditions and maintain a competitive advantage. However, ineffective information provision can lead to incorrect strategic decisions and loss of competitiveness. This emphasizes the importance of proper organization and management of information flows in the enterprise. To ensure effective information support, it is necessary to use modern information technologies and develop data processing and analysis systems. Summing up, information provision is an important element of enterprise management, which affects its efficiency, competitiveness and stability in a dynamic business environment.In the business process, various sources of information are used, but accounting data, which reflect the facts of the operations, as well as normative and planning documentation of the process of activity and management of the enterprise, are of great importance. That is, accounting information is a key element in the process of enterprise management before making strategic decisions at various stages of the

production process. The following factors can affect the formation of information support: the quality, completeness and reliability of information sources, the order and form of transmission-received information, an improperly prepared document flow schedule, incompetence of management personnel, etc. All these factors can have both positive and negative consequences on the quality of information on the basis of which, as a rule, important management decisions are made.

Scientists in their research put forward different visions regarding the concept of "information provision". In a general sense, information provision is one of the directions of the management process, the basis of which is the development of various methods of working with information, as well as the organization of an effective system of use, control, storage of information and its exchange between users.

Some scientists interpret the issues of information provision of the enterprise's activity process as: "forms, methods and tools of information resource management, which are necessary for stable functioning", as well as "for the effective implementation of the directions of the enterprise's development."Also, the author expresses his vision for the definition of the concept of information provision from the point of view of management: "it is a combination of all the information used in it, specific methods and means of its processing, as well as the activities of specialists for its effective improvement and use."

That is, the content of information provision consists in an organic combination of scientific knowledge with modern technologies.

The use of modern technologies and the automation of accounting processes allows you to quickly compile documents, ensures the accuracy of processing, the possibility of their use in real time and integration with other software. At the same time, there is an increase in the volume of compilation and use of electronic documents, which leads to the accumulation of large volumes of information and creates an additional danger of data loss. This prompts the creation of new conditions for providing enterprise IS. Therefore, the development of an effective plan to ensure the IS of the enterprise is the best protection against possible threats and the preservation of the business reputation of the enterprise.

The following practices will help to increase the effectiveness of the information security plan:

1) Creating a backup copy of sensitive (confidential) information and a copy of the accounting database in the cloud environment;

2) Encryption of information sources stored in the cloud;

3) Identify persons who may have access to confidential and accounting information;

4) Application of corporate mail for exchanging information and working with documents in shared access;

5) Use of double authentication of identity verification;

6) Use of Skype, Zoom, Google meet platforms for communication during management.

We consider it necessary, as a separate item, to highlight the importance of changing the requirements for company employees, especially accounting employees, when working with information and using modern technical means of its processing.The creation of programs for raising awareness and training employees, aimed at improving the skills of using modern technical support and careful work with information, would give an opportunity for employees to adapt to new technologies and maintain a high level of their competence.

Enterprise management includes a comprehensive approach to ensuring the information needs of the organization, which is based on the interaction of various objects of information provision, namely:

- the legal basis of accounting - defines the norms and principles that should be followed when keeping records and preparing financial statements;

- provisions of the accounting policy - defines specific accounting methods and principles used at the enterprise;

-primary documents - are the basis for recording the facts of business operations and events that are reflected in financial statements. They are a source of primary information for accounting and analysis of financial transactions;

- synthetic and analytical accounting data - used for the formation of financial and management reporting. Synthetic data represent a set of information for a certain period, while analytical data allow a more detailed review of financial indicators and a deeper analysis of the company's financial activities;

- indicators of financial and management reporting - are the basis for making management decisions. improvement and use".

These objects can be used in the formation of an effective system of information support for enterprise management.

Management decisions are made on the basis of a large number of

information sources. In connection with the growing number of information sources and the rapid pace of changes in the modern business environment, effective management of accounting information requires a comprehensive approach. One way to improve the quality of accounting information is to implement an internal control system that includes procedures, policies, and practices aimed at ensuring the accuracy, integrity, and confidentiality of information. These procedures include:

- the introduction of modern software tools for accounting and financial management allows automating many routine processes, reducing the likelihood of errors and increasing the accuracy of accounting information;

- ensuring the availability of accounting information for all interested parties, including management, investors, banks and regulatory bodies, contributes to increasing trust in the company and its financial stability;

- creation of effective internal control systems allows to warn and detect financial risks and errors in accounting, ensuring high accuracy and reliability of accounting information.;

- conducting trainings for accounting and finance personnel contributes to improving their qualifications and awareness of the importance of accuracy and reliability of accounting information;

- the use of recognized international accounting standards (for example, IFRS) contributes to the standardization and comparison of financial reporting, ensuring its quality and objectivity;

- constant analysis of the efficiency and effectiveness of accounting processes allows identifying and correcting possible shortcomings, which increases the quality of accounting information and its trust;

- the involvement of independent auditing firms to check and confirm the company's financial statements is an important stage in improving the quality of accounting information and ensuring its compliance with standards.

This approach allows you to avoid errors and abuses in accounting reporting, which can affect the validity of management decisions. In addition, to ensure the security of accounting information, it is important to implement strategies to ensure the confidentiality, integrity and availability of data. This may include using encryption, installing access control systems, backing up data, and other measures to protect information from unauthorized access and accidental loss. Accounting information security management is an important component of enterprise

management, as it ensures the reliability and validity of data used to make management decisions and helps prevent potential risks and threats to the enterprise. Considering the importance of accounting information, to improve its quality, there is a need to systematize and step-by-step formation of accounting information security management actions: We offer a step-by-step approach to the systematization of accounting information security management actions:

Stage 1. Emergence of an idea - analysis of the previous activity of the enterprise, calculation of existing risks and dangers, identification of needs for increasing the security of accounting information;

Stage 2. Development of the concept - development of a program to improve information security, determination of the main goals of the program, creation of a division of persons responsible for the development and implementation of the program;

Stage 3. Program development - development of targeted measures to increase information security, development of internal information security policy, creation of employee training programs.

Stage 4.Implementation and evaluation of the program - regular evaluation of the effectiveness of programs, support of employees during training.

The formation of successive stages of management of information sources, namely accounting information, contributes to the improvement of its quality at all levels of decision-making. This approach to the organization of enterprise security management will provide a more sensitive response system to the occurrence of potential dangers of various origins, and will also allow timely prevention of threats from both the internal and external environment.

A systematized approach to security management includes the creation of a unified regulatory and management information base, the creation of an enterprise document circulation route taking into account the influence of various factors of information security improvement, the development of an effective program for the protection and preservation of operational and accounting information at various stages of management, which in turn will have a positive effect on the general system of economic security management.

During the conduct of business activities, enterprises use various methods of collecting, processing, summarizing and storing information. At the same time, at each stage of working with information, threats arise that can significantly affect the

integrity, confidentiality and availability of information. Loss of control over the preservation of information can definitely lead to losses and inefficient operation of the enterprise.

Creating a reliable information security system requires solving problems aimed at protecting and preserving formalized and informal information. Formalized information means the process of presenting information in the form of documents or in the form of exchange processes through technical means. The protection of formalized information can be ensured using various methods of information theory by calculating the appropriate indicators of the degree of protection of such an object. If it is impossible to apply calculations using a theoretical approach, expert methods of evaluating indicators are used.

Information security is a critical aspect for today's businesses as they increasingly face threats from the digital world. The combination of different methods based on informal system theory turns out to be an effective approach for modeling effective information protection systems. The use of the theory of random processes, evolutionary modeling, graph theory and other mathematical approaches allows analyzing and forecasting risks related to information security

It is advisable to define the risk of information security as the product of the result of financial losses related to security and the probability of their occurrence. Information can have different forms of existence, but regardless of the way it is displayed, it must be securely protected. For this purpose, it is advisable to systematically assess possible dangers. Information can take many forms, from electronic documents to physical records, so it is important to have a comprehensive protection system that covers all aspects of the existence of information. This includes protection against cyber attacks, physical protection of data and ensuring the confidentiality of information during transport and storage. A systematic assessment of possible dangers allows to identify weak points in the information protection system and to take appropriate measures to eliminate them. It is also important to constantly improve the protection system, taking into account new threats and technological solutions. Awareness and understanding of information security risks allows enterprises to effectively manage these risks and prevent possible threats to the security of their information.

Information security risk assessment is a systematic analysis of information sources that are constantly exposed to threats. Based on the assessment of possible

threats, it is possible to develop measures to reduce the impact and prevent a negative impact on the company's activities in a timely manner.

Sequence of information security risk assessment:

- Determination of information sources, establishing their value;
- Determination of the probability of the occurrence of threats;
- Determination of the vulnerable sector of information sources;
- Calculation of the probability of the occurrence of a threat;
- Calculation of information security risk value.

The assessment of possible threats is determined by an expert method, taking into account the set of threats, their connections and parameters. At the same time, we offer a separate means of protection for each threat. We use the following indicators:

t_i – a set of threats;

ω_{t_i} – the frequency of occurrence of possible threats;

p_{t_i} - the probability of a threat.

The calculation is carried out in several stages:

Let's calculate possible losses from the occurrence of individual threats:

$$R_{t_i} = \sum_{k=1}^{kl} \omega_{t_i} p_{t_i} d_{t_i} c(a_k) \qquad (1);$$

де, Kl – the number of information sources aimed at threat

$t_i, \quad i = 1,2,3 \ldots\ldots, n;$

A_{t_i} – sources of information or assets targeted by the threat t_i;

$c(a_k)$ –cost of information sources, $a_k \in A_{t_i}$.

The coefficient of information $d_{ti} \in [0; 1]$, damage can act as a criterion for selecting those sources of information or assets that are subject to the destructive effect of the threat. It characterizes the general level of the destructive effect of a threat on an information source or asset.

Let's calculate the probable losses from the occurrence of threats that occur one after the other at a certain interval: $M(t_{a,} t_{\beta,})$:

$$R_{M(t_{a,} t_{\beta})} = R\, t_a + \sum_{i=1}^{m} \Sigma_{j=1}^{r} \quad p(t_{i,} t_j) R t_{j,} \qquad (2);$$

де *m, r* – the number of "mother" threats occurring at a specified interval

$M(t_{a,}t_{\beta,})$;

Let's $t_i \in (t_{a,}t_{\beta,})$ calculate the possible costs of providing protection against the onset of threats in the interval $M(t_{a,}t_{\beta,})$:

$$F_{M(t_{a,}t_{\beta})} = \sum_{i=1}^{n} Ft_{i,} \quad (3);$$

де Ft_i – costs incurred to ensure protection against the threat t_i.

At the next stage, the values of the risk value indicators are compared with the costs incurred to ensure information security, and a decision is made regarding the occurrence of this risk. Якщо $R_{t_i} = Ft_i$ - the magnitude of this risk is not significant and the risk can be ignored. In the case when $R_{t_i} \leq Ft_i$,there is an opportunity to optimize costs for ensuring the protection of information sources and company assets. A significant negative impact from risk can be prevented by applying diversification (distribution) of risk or its insurance. If during the calculation we got coefficients in which $R_{t_i} \geq Ft_i$,this indicates the need to apply measures to reduce or minimize the impact of risks on information security objects and to introduce new approaches to ensuring the information security of the enterprise.

The use of this method of expert assessment of the occurrence of possible risks to information security is appropriate for enterprises. Despite the fact that the system of protection of information sources of enterprises is normal, it is advisable to constantly improve and create the most reliable and effective protection system. The use of various methods of risk assessment allows you to find and make optimal decisions when carrying out economic activities, as well as to identify weak points of the enterprise for effective development and minimization of possible losses in the system of information support of economic security management.

The primary condition for the effective management of the enterprise is the improvement of its information support. Information is the basis for effective management. The main part of all enterprise information is accounting data.

- We propose to improve the process of information collection by dividing this procedure into three stages:

- The first stage of management takes place at the initial stage (the collection and formation of information takes place in the production units, warehouses, cash register of the enterprise). Information at this stage is collected on the basis of

primary documents for accounting of receipts and withdrawals of cash, funds in bank accounts, materials, production products, production of employees, etc.

- The second stage of management takes place at the general economic stage (collection and formation of information in auxiliary divisions of the enterprise). Information at this stage is collected on the basis of analytical data of accounting of settlement transactions, receivables and payables, information on the receipt and disposal of fixed assets, materials, etc.).

- The third stage of management is the stage of information processing and generalization (accounting department). At this stage, the accumulated information of the previous stages is grouped and summarized.

- We consider it expedient to use the above-mentioned stages for the formation of a mechanism for collecting accounting sources of information at all structural subdivisions for conducting an analysis of the enterprise's activities, assessing possible risks and making balanced decisions by the management.

- The organization of information support for accounting in the management of the economic security system requires a comprehensive approach and consideration of the features of the structural components of the information system. A close connection with information sources of various accounting and information processing objects is ensured by:

- use of common sources of information for various accounting objects;

-using the formed source information of one accounting object and transferring it as input for another accounting object;

- application of unified forms of information sources in accounting;

- the use of joint economic indicators for information support of various accounting objects.

Therefore, it would be expedient to create a single system of information support at the enterprise, with the help of which it is planned to achieve the following results:

- ensuring completeness, integrity and reliability of sources of accounting information;

- ensuring uninterrupted access to sources of information of management personnel for operational processing of data, analysis and decision-making;

- full and objective reflection of business processes in accounting sources (in accounting accounts, registers of analytical and synthetic accounting);

- ensuring the use of quality sources of information at all stages of enterprise management.

References:

1. Hnatenko V. Information and economic security as a factor of stable development of the state. 2020. No. 5. P. 63–74. URL: http://journals.maup.com.ua/index.php/public-management/article/view/152

2. Grebenyuk A.M. Fundamentals of information security management: training. Manual. Dnipro: Dniprop. state inside affairs, 2020. P.144. URL: https://er.dduvs.in.ua/bitstream/123456789/5717/120OUIB%20.pdf

3. Ignatenko M.M. Information provision of organizational and economic priorities for the development of farms and agricultural enterprises. Efficient economy. 2020 #5 URL: http://www.economy.nayka.com.ua/?op=1&z=7854

4. Oliinyk O.V. Regulatory and legal provision of information security in Ukraine. Law and society. 2012. No. 3. . URL: http://www.pravoisuspilstvo.org.ua/archive/2012/3_2012/28.pdf

5. Information security strategy dated December 28, 2021. URL: https://www.president.gov.ua/documents/6852021-41069

6. Shulga V.I. Modern approaches to the interpretation of the concept of information security. Efficient economy. 2015. No. 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514

3.4. METHODS AND MODELS OF OPTIMIZATION OF PROFITABILITY INDICATORS IN THE SYSTEM OF ENSURING FINANCIAL AND ECONOMIC SECURITY OF THE ENTERPRISE

Oleksandr Tkachenko

PhD in Economics, Associate Professor of the Department of Accounting, Taxation and Managementof Financial and Economic Security, Dnipro State Agrarian and Economic University, Ukraine

Summary. The economic content, types of profit calculation methods and its role in the system of financial and economic security of the enterprise are studied. The factors influencing the profit, which ensure the financial and economic security of the enterprise, have been studied. A comprehensive assessment of the financial and

CONTENT