Ministry of Education and Science of Ukraine
Dnipro State Agrarian and Economic University

ACCOUNTING, FINANCIAL, AND ECONOMIC SUPPORT FOR SUSTAINABLE DEVELOPMENT OF THE AGRICULTURAL SECTOR: THEORETICAL FOUNDATIONS AND PRACTICAL RECOMMENDATIONS

Collective Monograph

DNIPRO
2025

UDC 336 : 338 : 631 : 657
O 17

Reviewers:
Svitlana SHULGA – Doctor of Economic Sciences, Professor, Vice-Rector for Scientific and Financial and Economic Work, National Academy of Statistics, Accounting and Auditing (Kyiv)
Natalia ZDYRKO – Doctor of Economic Sciences, Professor, Director of the Educational and Scientific Institute of Economics, Vinnytsia National Agrarian University (Vinnytsia)
Igor VINICHENKO – Doctor of Economic Sciences, Professor, Head of the Department of Economics, Dnipro State Agrarian and Economic University (Dnipro)

Editors-in-Chief:
Halyna PAVLOVA – Doctor of Economic Sciences, Professor, Dean of the Faculty of Accounting and Finance, Dnipro State Agrarian and Economic University (Dnipro)
Natalia VASYLIEVA – Doctor of Economic Sciences, Professor, Deputy Dean for Research, Dnipro State Agrarian and Economic University (Dnipro)

Recommended by the Academic Council of Dnipro State Agrarian and Economic University (protocol № 7 from 24.04.2025).

Authors:
Halyna PAVLOVA, Oleksandr ATAMAS, Oleksandr TKACHENKO, Liudmyla VOLCHANS'KA, Olha HUBARYK, Olena DUBYNA, Olga CHERNETSKA, Serhii YURCHENKO, Mariya BARDADYM, Lesia VASILIEVA, Olga ODNOSHEVNA, Tatiana MACHAK, Alona MINKOVSKA, Tetiana SAVANCHUK, Svitlana KHALATUR, Svitlana KACHULA, Anna SIRKO, Natalia VASYLIEVA, Iuliia MASIUK, Oksana VODOLAZSKA, Oksana HRABCHUK, Ilona SOLODOVNIKOVA

Accounting, financial, and economic support for sustainable development of the agricultural sector: theoretical foundations and practical recommendations: collective monograph / edited by H. Pavlova and N. Vasylieva. Dnipro: Maksymovska Y.A., 2025. 488 p.

ISBN: 978-617-95342-7-0

The monograph is focused on scientific, methodical and practical aspects of accounting, financial, and economic support for the sustainable development of the agricultural sector in Ukraine. The collective monograph was published within the framework of the state budget research topics "Innovative development of accounting, taxation and control in the system of ensuring the economic stability of enterprises" (state registration number 0121U109731), "Financial support for structural modernization and innovative development of agroindustrial production in Ukraine" (state registration number 0124U000027), "Information technologies and mathematical methods for the development of the agricultural sector of the economy" (state registration number 0120U105338).

The monograph is intended for policymakers and stakeholders in agriculture, accountants, banking and finance specialists, agricultural managers, farmers, researchers and postgraduate students in agricultural economics.

UDC 336 : 338 : 631 : 657

ISBN: 978-617-95342-7-0

CONTENT

PREFACE 5

CHAPTER 1. Accounting and analytical support and financial and economic security in the agricultural sector 9

1.1. Accounting of milk processing processes 9
(Halyna Pavlova)

1.2. Impact of non-financial reporting on investment attractiveness of enterprises in the agricultural sector 31
(Oleksandr Atamas)

1.3. Solvency management in the system of ensuring the financial and economic security of an agricultural enterprise 55
(Oleksandr Tkachenko)

1.4. Peculiarities of accounting and analysis of economic activities of enterprises under martial law 77
(Liudmyla Volchans'ka)

CHAPTER 2. Accounting and economic aspect of enterprise development strategy 98

2.1. International financial reporting and auditing standards as the basis of trust in accounting information in the agricultural Sector 98
(Olha Hubaryk)

2.2. Improvement of accounting and analytical support of payments with consumers in the utility sector 118
(Olena Dubyna)

2.3. Sustainable development monitoring based on an integrated accounting and analytical system 138
(Olga Chernetska)

2.4. Optimization of the accounting and analytical support system and control of the enterprise's accounts receivable 160
(Serhii Yurchenko)

2.5. Accounting provision for management of sales expenses in accordance with the marketing strategy of the enterprise 180
(Mariya Bardadym)

CHAPTER 3. Financial and economic security management 201

3.1. Formation of accounting and analytical support for managing financial and economic security of an agricultural enterprise 201
(Lesia Vasilieva)

3.2. Formation of financial result and its impact on management income of an enterprise as an element of economic security 222
(Olga Odnoshevna)

3.3. Optimization of the information support system for the financial and economic security of the enterprise 243
(Tatiana Machak)
3.4. Personnel selection in the context of ensuring financial and economic security of the enterprise 262
(Alona Minkovska)
3.5. The essence and organization of the economic security system of an enterprise 281
(Tetiana Savanchuk)
CHAPTER 4. Financial and credit support for innovative development of agro-industrial enterprises: modern challenges 303
4.1. Fintech as a driving force for the transformation of traditional banking 303
(Svitlana Khalatur)
4.2. Enhancing financial support for Ukraine's agricultural sector: the interplay between state budget funds and commercial bank lending 327
(Svitlana Kachula)
4.3. Financial risks of innovative activities in the agro-industrial complex: assessment and mitigation strategies 348
(Anna Sirko)
4.4. Contemporary features of agricultural economics modeling 368
(Natalia Vasylieva)
CHAPTER 5. Realities and prospects for the development of insurance and the stock market of Ukraine 387
5.1. The role of insurance in investment protection and developing financial markets 387
(Iuliia Masiuk)
5.2. The mechanism of effective functioning of stock exchanges under the conditions of uncertainty 407
(Oksana Vodolazska)
5.3. Modern trends in the development of the Ukrainian stock market 429
(Oksana Hrabchuk)
5.4. The impact of systemic risks on the development of the Ukrainian stock market under conditions of multidimensional uncertainty 452
(Ilona Solodovnikova)
CONCLUSIONS 472
REFERENCES 476

3.3. OPTIMIZATION OF THE INFORMATION SUPPORT SYSTEM FOR THE FINANCIAL AND ECONOMIC SECURITY OF THE ENTERPRISE

Tatiana Machak,
Senior Lecturer of the Department of Accounting, Taxation and Management of Financial and Economic Security,
Dnipro State Agrarian and Economic University, Dnipro, Ukraine

In the conditions of dynamic development of a market economy and an increase in competition, ensuring the economic security of the enterprise is the basis of its stable functioning and further development. An important tool for achieving such security is an effective information support system, which includes the processes of collecting, processing, storing, analyzing and transmitting information for management decisions.

Modern information support can be considered as a set of methods, tools, resources and technologies that are aimed at meeting the needs of enterprise management. Such a system should cover the full range of management processes - from operational to strategic level, providing access to the necessary, reliable and timely information for risk analysis, planning, control and evaluation of activity efficiency.

In general, information support can be described as an integrated system that includes information resources (internal and external), technological infrastructure (software, computing systems), methodological basis (analytical approaches, models, data processing methods), as well as a regulatory framework. All of these components should interact within the single logic of management, focused on achieving the stability and competitiveness of the enterprise.

Information in this system is not only a passive source of data, but also an active management tool. It allows you to identify threats, identify weaknesses in internal business processes, evaluate the effectiveness of implemented strategies, as well as adapt the activity of the enterprise to external changes-changes in legislation, market trends, competitors' behavior, etc. Accordingly, information support is not only a technical or procedural element, but also a strategic platform.

The information support of the management activity of the enterprise is based on the use of a wide range of sources of information, which are conditionally divided into internal and external. This division is fundamentally important because each category of sources performs its function in the process of forming a complex information base necessary for effective management, strategic planning and decision -making.

Internal sources of information include data that is formed directly within the enterprise in the course of its operational, financial and management activities. First of all, it is an account that is generated in the process of accounting, financial and management accounting. Accounting documents (primary, registers, magazines), financial statements (balance sheet, financial results, cash flow, equity report) reflect the real state of assets, liabilities, income and expenses of the enterprise. Management accounting provides detailed information on internal costs, productivity of units, efficiency of use of resources. In addition, internal sources include the reports of structural

units, service notes, protocols of meetings, which cover operating indicators, the progress of plans, achievement of goals, problems in the organization of production or sales of products. Internal normative documents - accounting policies, regulations, instructions, orders, regulations that form the organizational structure and management culture of the enterprise also play a significant role. Internal sources are characterized by a high degree of detail, regularity and accessibility for internal users. They are indispensable for internal audit, prompt analysis, budget planning, control over the achievement of key performance.

External sources of information, in turn, are formed outside the enterprise and reflect the external environment of its functioning. They cover a wide range of sources: from legislative acts and regulatory documents to economic analytics and market information. In addition, publications in economic and business press, professional analytical reports, markets review, consulting companies research play an important role. Such sources allow to monitor trends in the industry, the actions of competitors, changes in consumer behavior, and to predict changes in demand and prices. External sources include legislative documents - laws, regulations, orders, methodological recommendations that regulate tax, financial, labor policy. They are the basis for building a system of conformity and compliance with legal norms in the activity of the enterprise.

The combination of information from internal and external sources allows you to get a comprehensive picture of the state of the enterprise and its environment, which provides a deep understanding of both internal processes and the impact of external factors, which contributes to the adoption of sound, strategically balanced decisions, increases the flexibility of the enterprise to changes and its ability to adapt.

To date, there is no single established definition of information support system in the scientific environment. However, despite the diversity of interpretations, it can be argued that the effective functioning of this system is based on the availability of certain components, which include: information resources, technological infrastructure, methodology of analysis and regulatory framework. The main purpose of such a system is to ensure a timely, reliable and current information flow necessary for identifying risks, assessing the financial and economic condition of the enterprise and making rational management decisions. At the same time, this system performs an important function in maintaining the financial and economic security of the enterprise, facilitating rapid adaptation to internal and external threats.

Accounting information plays a separate role in the information support system. It is formed in the process of financial, accounting and management accounting, covering data on assets, liabilities, income, expenses, profit, use of resources, budget execution. Such information is the basis for the preparation of financial statements, internal analysis and forecasting. This can not only evaluate the current state, but also model future scenarios, identify risks and form mechanisms of neutralization.

The system of information support of the enterprise is an important component of modern management, which provides access to current, complete and reliable information for making sound management decisions. The effectiveness of its functioning depends

directly on compliance with a number of key requirements that determine the quality of information processes and their compliance with users.

One of the main requirements for the information system is the relevance of information. Data should reflect the real state of affairs at the time of their use so that management decisions are based on the most recent information. Obsolete or unspecified data can lead to a false assessment of the situation and wrong actions. Therefore, the system must ensure constant updating of information according to current changes in the internal and external environment.

The second important requirement is authenticity. All information that is processed and provided by the system must be tested, accurate and free from errors. The high accuracy of the data guarantees the minimization of the risks of improper interpretation of the situation. This is especially important in the financial, legal, management and security fields.

Equally significant is promptness. The information should be available at the moment when it is required to make decisions. Data delays can lead to loss of opportunities, delaying processes or critical situations. Automated information collection and processing tools integrated with other systems are used to achieve efficiency.

The security of information is another fundamental requirement. All data must be securely protected from unauthorized access, loss or damage. This is achieved through the use of modern information security tools: encryption, authorization systems, backup, access audits. Particular attention should be paid to customer personal data and the confidential information of the enterprise. The adaptability of the system lies in its ability to quickly and effectively respond to changes in the external environment, internal structure of the enterprise, changes in legislation, business goals or management methods. The system should be flexible, scaled, with the possibility of modernizing functionality without loss of stability.

The completeness of the information means that the data should contain all the necessary elements for full analysis. Partial or fragmentary information can lead to false conclusions. Fullness is ensured by the coverage of all-important aspects of the enterprise, taking into account internal and external sources.

Availability implies that the data should be accessible to all users who have the appropriate authority. This ensures uninterrupted work of staff, reduces the risk of delay in decision -making and increases the efficiency of interaction between units.

Finally, the economy of the information support system lies in the expediency of its implementation, support and updating. The expenditures associated with the system should be reasonable and should not exceed the value it provides to the enterprise; the cost-benefit ratio should be well substantiated.

The requirements for the effective functioning of the information support system at enterprises are shown in Table 3.3.1. Thus, information support is not only a means of supporting management activities, but also the basis for ensuring the financial and economic security of the enterprise. In the face of constant change of the business environment, it allows managers to adapt strategies, make sound decisions, respond

promptly to potential threats and use available resources as efficiently as possible, at the same time there is an urgent issue of constant improvement of information support system, which involves updating technical means, improvement of information processing, development of information.

Table 3.3.1

Requirements for the functioning of the enterprise information support system

Requirement	Description
Relevance	Information must correspond to the current conditions of the enterprise's operations.
Reliability	Information must be verified and reflect the actual state of affairs.
Timeliness	Information must be available in time to enable quick decision-making.
Security	Information must be protected from unauthorized access.
Adaptability	The information system must easily adapt to any changes in both internal and external environments.
Completeness	Information must be presented in full to allow for comprehensive analysis.
Accessibility	Information must be constantly available to users who are authorized to access it.
Cost-effectiveness	The cost of operating the system must be justified and not exceed the benefits it provides

In today's business environment, enterprises are faced with numerous risks and uncertainty, which can adversely affect their financial and economic security. Usually, risk is considered as the likelihood of events that can have negative consequences for the enterprise, especially in the context of its financial and economic stability. It is known that decision -making in uncertainty is always accompanied by risks that can manifest in both the internal and external environment of the organization. Among the main sources of uncertainty are the rapid development of technologies, lack of awareness of market participants, unpredictability of consumer behavior, variability of economic, political and military conditions, as well as internal instability in management processes. Thus, risks are the natural part of the functioning of each enterprise that arises both as a result of external circumstances (economic, political, military, technological changes), and due to internal shortcomings (management mistakes, inefficient work organization, poor planning).

External risks, as a rule, occur due to unpredictable changes in the environment, while internal - due to decisions and actions within the organization. Both types of risks are interrelated, and poor internal factors can reduce the company's ability to adapt to external changes.

In a separate category, you should bring information about information security. They not only threaten the loss or damage of data, but also restriction as a quality,

accessibility, efficiency and accuracy of information. The causes of such risks may be outdated or poor IT systems, low process automation, data processing errors, or insufficient qualification of employees.

In order to effectively reduce the impact of information risks, reliable information support is required, which contributes to the timely receipt, processing and use of data. Its role is to form the basis for making rational management decisions that protect the interests of the enterprise in the face of uncertainty. Allows you to identify risks in a timely manner, analyze their impact and develop measures for minimizing them. Creating and maintaining an effective information support system allows the enterprise not only to respond to threats in a timely manner, but also to predict possible economic difficulties in the future, which is important for ensuring the sustainability of business in a variable market environment. Collecting information is the first and most important step in the risk management process. It includes both the use of internal data sources and the involvement of external information resources that allow the enterprise to obtain a full idea of the market status, legislative changes, financial indicators and other factors that may affect its activities.

Internal data sources include accounting data as the main source of information about the financial condition of the enterprise. Accounting data provides accurate information about income, expenses, assets, liabilities, cash flow, which allows to identify potential financial problems, such as reducing liquidity or increasing debt. Internal sources also include management accounting data, that is, reports that make up for internal management and allow you to control the key indicators of enterprise efficiency, such as profitability, profitability, cost efficiency, production and sales. Internal sources of information also include an internal audit that is an effective tool for obtaining reliable data. Internal audit provides additional inspection of financial and operating processes, helps to identify deficiencies in the internal control system, in particular on cash flow management, accounting of assets and liabilities, and allows to check the compliance of the enterprise with the requirements of the current legislation.

External data sources include information about market trends, consumer behavior, competition and changes in demand that are necessary to predict possible changes in the financial indicators of the enterprise. This may include an analysis of market trends, demand for products, competitors' analysis and raw materials and materials monitoring. Also, external sources of data include changes in tax, labor, and other types of legislation can significantly affect the financial stability of the enterprise. In particular, changes in tax legislation or rules for regulation of prices may change the costs of the enterprise and its tax liabilities.

Therefore, information security risk management has two important components. The first is to ensure high quality data - their reliability, relevance and integrity. The second component is related to the presence of threats arising from the limited or imperfection of information systems, outdated data processing technologies, as well as insufficient level of professional training of staff. All this can significantly complicate the effective management of information processes in the enterprise. To minimize such risks, the company requires a modern information support system that will provide timely access

to the necessary data, their qualitative analysis and further use to form effective management decisions.

One of the important aspects of such information support system is its integration into the enterprise risk management system, which involves the creation of information infrastructure, which allows you to quickly identify and analyze risks, to form appropriate response and control strategies. In particular, it is important to introduce information and analytical systems that provide automated monitoring of financial indicators, forecasting possible negative scenarios and evaluation of the effectiveness of the decisions made.

Information support also plays an important role in ensuring transparency and accountability of management processes. The availability of reliable information allows the management of the enterprise to detect deviations from the planned indicators in a timely manner, analyze the causes of such deviations and take the necessary measures to eliminate them. In addition, it helps to increase confidence by investors, partners and other stakeholders. The management of the financial and economic security of the enterprise provides a systematic approach to identifying, analyzing and minimizing potential threats. Information support in this context acts as a tool that allows you to identify the risks in the early stages, to evaluate their impact on the activity of the enterprise and to develop effective response strategies. This includes the use of various methods of analysis, such as SWOT analysis, PEST analysis, script analysis, etc.

An important component of information support is accounting information that is formed in the process of accounting, financial and management accounting. This information contains detailed data on business operations, financial status, results of activity and use of enterprise resources. On this basis, financial reports are formed, which serve as a source of information for analyzing and making management decisions.

In addition, information support includes a legal framework that regulates the activity of the enterprise and determines the requirements for reporting, accounting and control. Knowledge and compliance with regulatory requirements is a prerequisite for ensuring financial and economic security and avoiding legal risks.

Effective information support for the management of the risk of financial and economic security of the enterprise also provides for constant monitoring of the environment, which includes the analysis of macroeconomic trends, changes in legislation, behavior of competitors and consumers. Such data allow the company to adapt its strategy to variable conditions and reduce the impact of external risks.

Financial and economic security risk management also requires effective communication between different units of the enterprise, which will facilitate the creation of a single information space where all stakeholders have access to up-to-date and reliable information. This allows to ensure consistency of actions, rapid response to changes and effective decision making. Effective information security management is possible only if purposeful management mechanisms that not only prevent threats, but also reduce their potential influence, contributing to the stability of the financial and economic security of the enterprise.

The mechanisms for managing information risks in the system of financial and economic security of the enterprise cover a set of organizational, technical and management measures aimed at protecting information resources, preventing data leakage, reducing the impact of external and internal threats, as well as ensuring the integrity, confidentiality and availability of data. In today's context, when the information has become a strategic asset of the enterprise, effective information risk management is an integral part of ensuring its financial and economic stability.

The first important step in shaping the information risk management system is to develop information security policy. It aims to establish clear rules and procedures governing the procedure for working with information resources. This policy defines the level of access to data, the responsibility of employees for the processing and storage of information, requirements for the use of technical means of protection, as well as sanctions for violation of the established rules. This policy creates a single standard of conduct for all employees of the enterprise, forming a responsible attitude to processing and preserving information.

Automation of information processes is an important condition for reducing risks. The introduction of modern software solutions and information systems can increase the accuracy of data processing, reduce the impact of the human factor, as well as accelerate the exchange of information between units. Automated accounting, finance, logistics or staff management systems provide centralized access to current information, which allows you to respond promptly to threats and make effective management decisions.

One of the most important technical risk management mechanisms is regular backup. This process involves the creation of copies of critically important information for the purpose of recovery in the event of damage, loss or cyberattack. Backups should be stored on protected media or in restricted cloud services. It is also important to test the recovery system periodically to check its efficiency. Systematic monitoring and auditing of the enterprise information infrastructure contribute to the timely detection of vulnerabilities that can be used by intruders or lead to technical failures. Conducting internal audits allows you to evaluate the state of information security policy, the effectiveness of protective measures, compliance with the regulations of work with information. Monitoring includes both access control and the detection of suspicious activity in the system.

Another critical element is the control of access to information resources. It envisages the introduction of user authentication systems, differentiation of access rights to certain categories of information, depending on employees' job responsibilities, use of multi -level protection for sensitive data. This reduces the risk of unauthorized access and leakage of confidential information. In order to counteract external and internal threats, effective means of technical protection of information. These include antiviral programs, invasion detection systems, files, data encryption, multifactorial authentication technology and more. These tools provide the basic security of the enterprise information systems, preventing most common cyber threats.

However, even state -of -the -art technologies cannot guarantee full safety without the proper level of staff awareness. That is why an important mechanism for managing

information risks is the training and advanced training of employees. Regular trainings and seminars on the rules of working with information, the basics of cybergigiene, the detection of phishing attacks, as well as the prevention of data leakage as a result of careless actions - all this forms a culture of information security in the team and reduces the risks associated with the human factor. The mechanisms of information risks management in the financial and economic security system are Fig. 3.3.1.

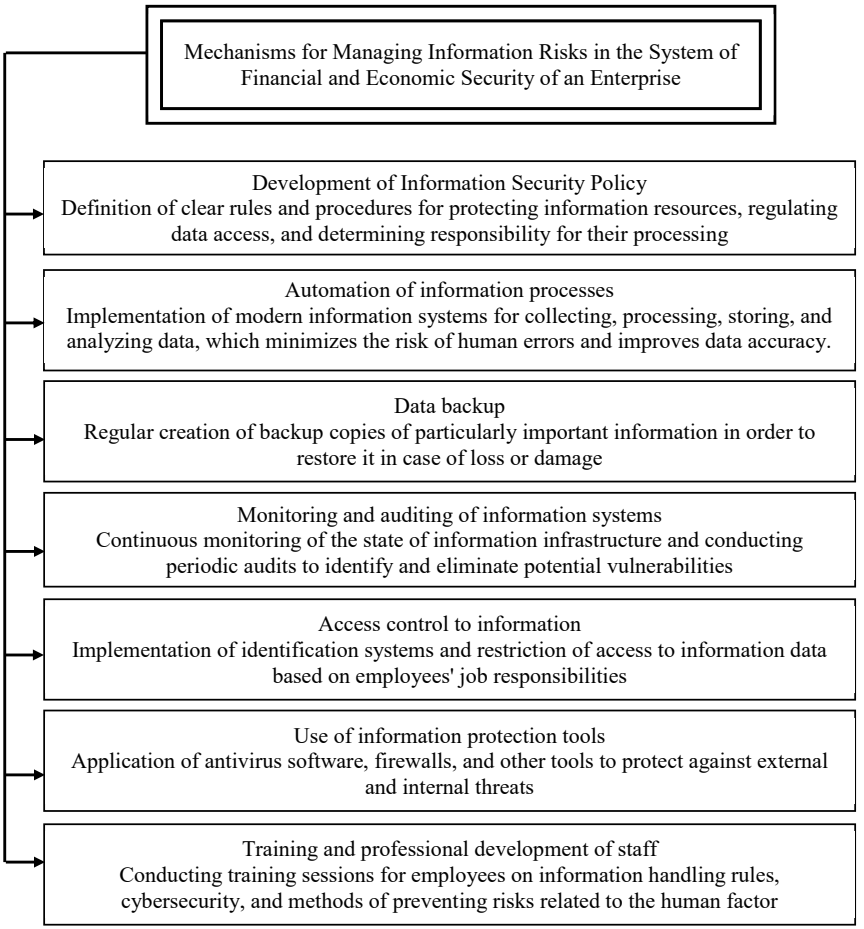

Fig. 3.3.1. Mechanisms for Managing Information Risks in the System of Financial and Economic Security of an Enterprise

Therefore, in order to reduce information risks, it is advisable to introduce a complex mechanism aimed at the timely identification and minimization of potential threats associated with inaccuracy, loss or unauthorized access to information.

Information security risk management is an integral part of general risk management at the enterprise, and it includes two main areas: the first is the provision of high-quality information, and the second is the presence of potential threats that may occur due to shortcomings in information systems, technologies or human factor. The last aspect is especially important for successful information security risk management.

Information security threats can be classified in several directions. First, these are threats associated with technological vulnerability. For example, outdated systems that are no longer supported by suppliers or have known vulnerability can be the object of attacks by malefactors. Such threats can be caused by the use of imperfect software solutions, non -existent operating systems, or even incorrect network settings.

Secondly, the human factor is an important source of threats. The inability or negligent approach of the staff to the performance of safety procedures can lead to leakage or loss of data. These can be intentional actions (fraud, confidential information), and unintentional errors, such as accidental deletion of important files or errors in the security system settings.

Third, external threats, including cybercrime, are a significant problem for businesses. Hacker attacks, harmful software (viruses, Troyans), phishing, and vulnerability in communication networks can be a cause of serious violations in the organization's information security.

Finally, legal threats appear. Failure to comply with the legal requirements concerning information protection can lead to penalties, sanctions or even losses of a license for activity. Changes in legislation, both at national and international levels, require enterprises to monitor and adapt their information systems.

The reliable functioning of the enterprise information system, as well as ensuring its financial and economic security, depends directly on the clear organization of information support, which is based on proper legal regulation. The effectiveness of this process requires a comprehensive analysis of normative legal acts that set requirements for procedures for collecting, processing, storage and use of information within business activities.

The legislative framework of Ukraine in this area is represented by a wide range of regulatory sources. The basis is documents such as the Constitution of Ukraine, the Civil Code of Ukraine, sectoral laws and by -laws, as well as standards that regulate the activities of enterprises. The following laws play a special role: "On information", "On protection of information in information and telecommunication systems", "On accounting and financial reporting in Ukraine", as well as the Tax Code of Ukraine. All these acts form a legal framework within which the information support system of the enterprise operates. Each of the above documents performs a specific function. The Law on Information regulates information relations, defines the rights and obligations of information entities, and establishes the principles of access to data. The Law on

Protection of Information in Information and Telecommunication Systems defines the order of information protection in automated systems, in particular, technical and organizational measures aimed at preventing leakage or distorting data. The Civil Code regulates the ownership of information, as well as the terms of its transfer and responsibility for violation of these rights.

The Law on Accounting and Financial Reporting establishes the procedure for accounting and preparation of financial statements, which is the basis of information support of the economic security of the enterprise. Its provisions determine what data should be recorded, how they should be stored, and in what form - to be transferred to external users, including public authorities.

At the level of the enterprise itself, legal regulation of information processes is implemented through local regulations. In particular, the provisions on accounting policy, which outlines the rules of accounting, formation of primary documentation, and establishes the order of interaction between structural units. This document is an instrument of internal regulation that ensures legal certainty in the functioning of the accounting system.

In order to improve the efficiency of management processes and optimal use of information resources, it is also advisable to develop provisions on information security of the enterprise. This document must state the basic data protection measures, the procedure and conditions of access to information, the requirements for maintaining the confidentiality and integrity of electronic documents. In addition, an electronic communication instruction should be approved, which will set the rules for exchange of electronic information both within the enterprise and with external counterparties.

The development and implementation of such documents will allow to adapt the mechanisms of information interaction to the specific activity of the enterprise, taking into account the requirements of the current legislation and corporate culture. Internal regulations help to increase the level of information security, reduce the likelihood of legal risks and allow you to effectively manage the processes of processing and use of information.

Effective management of an enterprise is an important element at all stages of management 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 support (for the ease of perception we continue to apply reduction with) 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 management uses different sources of information, but credentials are of great importance that reflect the facts of the operations performed, as well as the regulatory and planned documentation of the process of activity and management of the enterprise. That is, accounting information is a key element in the process of managing an enterprise before making strategic decisions at different stages of the production process. The formation of information support can be influenced by the following factors: quality, completeness and reliability of sources of information, order and form of transmission-withdrawal

information, not properly schedule of document management, non-competence of management personnel, other. All these factors can have both positive and negative consequences on the quality of information on the basis of which, as a rule, make important management decisions. Scientists in their studies put forward different visions regarding the concept of "information support". In the general sense, it is one of the directions of the management process, which is based on the development of different 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.

The use of modern technologies and automation of accounting processes allows you to quickly compile documents, provides accuracy of processing, the ability to use them in real time and integration with other software. At the same time, there is an increase in the amount of assembly and use of electronic documents, which leads to the accumulation of large amounts of information and creates an additional danger of data loss. This encourages the creation of new conditions for securing the IB of the enterprise. Therefore, the development of an effective plan for securing an IB enterprise is the best protection against possible threats and maintaining business reputation to the enterprise.

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

1) Creating a backup of sensitive (confidential) information and a copy of the accounting base in the cloud environment. Backup allows you to store important information in the event of failures in the main system, cyberattack or accidental deletion. Cloud storage facilities, such as Google Drive, Dropbox, Microsoft OneDrive, provide not only remote access to information but also automatically backup updates. It is recommended to adjust regular copying of the accounting base (for example, once a day) and divide the archives by access level.

2) encryption of information sources stored in the cloud. For sensitive information stored in the cloud, certified encryption algorithms should be used, and it is important to use data encryption not only in storage, but also when transmitting information. This significantly complicates unauthorized access even in the case of a cloud platform.

3) identify persons who may have access to confidential and accounting information, that is, each employee should only have access to the information that is required to perform its functions. The IT-system administrator must create roles (for example, an accountant, head of the department, analyst) for which different levels of access are established. Keeping access logs allows you to control who, when and what data had access.

4) the use of corporate mail to exchange information and work with documents together. Corporate email (for example, based on Microsoft Outlook or Gmail for Business) provides centralized control over all electronic correspondence of employees. It allows you to limit the use of personal accounts for exchange of service information, protecting it from leakage. Integration with corporate clouds (SharePoint, Google Drive) allows you to work with documents at the same time several users, maintaining control of versions and logging of change.

5)use of double authentication confirmation of person. Two -factor authentication adds an additional level of protection at the entrance to the systems. After entering the password, the user must enter another code that is sent to a mobile phone or generated by a special application (such as Google Authenticator, Microsoft Authenticator). This significantly complicates unauthorized input even if the password has been compromised.

The use of Skype, Zoom, Google Meet platforms for communication during management that will organize virtual meetings, discussions, presentations and trainings, regardless of the geographical location of participants. However, their use requires certain safety rules:

- setting passwords at the conference;
- control of participants of the meeting;
- shutdown of automatic storage of records without permission;
- Use of corporate accounts instead of personal.

We consider it necessary, a separate point to highlight the importance of changing the requirements for employees of the enterprise, especially for employees of accounting, while working with information and using modern technical means of its processing. Training and advanced training of staff on the rules of work with information, cybersecurity and methods of preventing the risks associated with the human factor is an important area in ensuring the information and financial and economic security of the enterprise. The human factor is often the weakest link in the protection system, since even reliable technical solutions cannot protect information resources in case of careless or unconscious violation of the established rules by the employee. That is why systematic training of employees and the formation of a culture of safe behavior with information in them are critical tasks. Employees should understand that information is a strategic resource of an enterprise that needs protection at all stages of the life cycle - from creation and storage to transmission and destruction. They need to give a clear idea of the rules of work with confidential, financial, personal and official information, including restrictions on its distribution, access protection requirements, e -mail rules, storage of documents on physical and digital media.

It is important to systematically the learning process. The information environment is constantly changing, new risks and vulnerability appear, so education should not be a one -time event. Regular trainings, updated online courses, internal newsletters, briefings during hiring and when changing responsibilities should be introduced.

In the process of enterprise management, the main objects of information support are:

- Legislative base of accounting;
- accounting policy provisions;
- primary documents;
- synthetic and analytical accounting data;
- indicators of financial and management reporting.

These objects can be used when forming an effective information support system for enterprise management.

Management decisions are made on the basis of a large number of information sources. Given the importance of accounting information, to improve its quality, there is a need to systematize and gradual formation of account management actions:

The first step is to analyze the previous activity of the enterprise, to evaluate risks and to identify security needs. This stage conducts a thorough study of available processing of accounting information, systems used, documentary flows, level of staff training, as well as, inventory of accounting systems, checks are checked. In parallel, potential risks are calculated: threats of information leakage, accounting errors, technical failures, etc. This makes it possible to formulate an objective picture of the current state of information security.

The second stage is the development of an information security program and defining its strategic goals. Based on the results of the analysis, a program of action is formulated, which should include clearly defined goals: minimizing the risks of data loss, ensuring compliance with legislation, improving the availability of data for authorized users, increasing cyber defense, etc. Particular attention is paid not only to the technical aspects, but also to the organizational - the role of staff, the system of motivation to observe safety policies, the internal culture of information protection.

In the third stage, specific measures and information security policies of the enterprise are developed. This stage provides for the preparation of the list of purposeful measures, which may include: creation of backup databases, encryption of databases, introduction of electronic signatures, installation of modern antivirus and firewall systems, creation of systems of monitoring of user actions. In addition, internal information security policy is developed - a regulatory document that describes access rights, rules for the use of information systems, the order of response to incidents, and the responsibility of employees for violation of the established standards.

In the final fourth stage, the effectiveness of the implemented program and organizational support of staff are evaluated. After implementing the program, it is necessary to monitor its efficiency, including auditing information processes, analysis of security incidents, assessment of protection of protection systems, as well as collecting feedback from users. It is important not only to identify technical disadvantages, but also to evaluate how well the staff adhere to the politician and whether additional training needs. For this purpose, seminars, trainings, instruction and practical simulations are organized, which allow to maintain a high level of awareness among employees and increase their readiness for action in crisis situations.

Information is an important resource for managerial decision-making and allows you to respond in a timely manner to changes in both the external and internal environment, so an important issue is the optimization of the information support system of financial and economic security. Optimization not only improves the effectiveness of existing practices, but also ensure continuous improvement of the system at all levels of management. It includes viewing existing tools and procedures, integration of the latest technologies to increase the protection of accounting information, as well as adaptation to changes in the legislative environment and foreign economic conditions.

Today, there are a large number of effective risk assessment tools that play a key role in shaping the information support system for the enterprise's financial and economic security. It is through information support that the collection, processing, analysis and submission of relevant data needed to make sound management decisions on identification and minimization of risks. Qualitative, reliable and operational information creates the basis for the use of modern risk assessment tools, providing a systematic approach to the management of threats and strengthening the economic stability of the enterprise.

One of the effective tools of information modeling tools is SWOT analysis that reveals the strengths and weaknesses of the enterprise, as well as opportunities and threats from the environment. As part of information support, this method is based on a wide range of internal and external data, which allow not only to see potential risks, but also to establish relationships between the internal resources of the enterprise and the conditions of its functioning on the market. For example, a weak place may be a low level of digital security found in the process of internal reports analysis, while the threat is the activation of cyberattacks in the industry, confirmed by analytical reviews and sectoral reports.

Another effective method is PEST analysis that evaluates the impact of political, economic, social and technological factors on the activity of the enterprise. Within the framework of information support, such analysis is based on the collection of data from official sources, analytical publications, legislative acts and forecasts of economic development. This allows you to identify the risks associated with changes in tax regulation, macroeconomic instability, or technological innovations that can both threaten and open new opportunities for the enterprise. For example, information on changes in the legislation on the protection of personal data may be the basis for reviewing the security policies at the enterprise.

A special role in the information support system is played by the analysis of financial indicators, in particular liquidity, profitability, solvency and business activity. This analysis is based on accounting and reporting information, which is one of the main components of information support. Financial analysis can not only evaluate the current state of the enterprise, but also identify potential points of financial vulnerability. For example, reducing the current liquidity ratio may indicate future difficulties in fulfilling financial obligations, which requires immediate intervention and development of anti - crisis measures.

Information support is also necessary to fully evaluate the financial and economic security of the enterprise. Risk assessment methods are based on a deep analysis of both internal and external data and allow you to identify threats in a timely manner and minimize them. For example, a script analysis is a tool that allows you to predict changes in the financial condition of the enterprise depending on different economic conditions. Reliable information support allows you to model several variants of events, taking into account macroeconomic, sectoral and internal factors.

Monte Carlo's statistical method - uses random values to forecast financial results. It requires a large amount of accurate data from accounting, financial and analytical sources, and allows you to assess the likelihood of risks in various scenarios.

Credit analysis - provides an assessment of the solvency of the enterprise, which uses financial statements, liquidity ratios, profitability and capital structure. An important element is the forecasting of cash flows, which is possible only if you fully and accurately account.

The method of monitoring financial and economic threats is based on the systematic collection of information on changes in the external environment (economy, legislation, market) and internal environment (indicators of activity, financial results). This allows you to respond timely to potential threats and adapt a strategy.

An effective tool for assessing the risk of insolvency and bankruptcy forecasting is the method of multifactorial discriminant analysis, which allows to take into account the impact of different financial indicators and their relationship, combining them into a single integral indicator that allows to determine the degree of influence of each of them on the probability of bankruptcy. One of the most famous models of this method is Altman Z-Score, based on five financial ratios: liquidity, accumulated profit, asset profitability, market value of equity to liabilities and assets. The results of this analysis allow you to classify enterprises by bankruptcy risk. The Springate S-Score Model, developed on the basis of the Altman model, includes four indicators: working capital for assets, payments to taxes and interest on assets, tax profit in short-term liabilities and assets. It allows to determine the threat of financial instability. Another common model is the Taffler model, which includes tax payments on short -term liabilities, ratio of current assets to liabilities, short -term liabilities to total assets and assets. It was specially adapted for British enterprises and has proven itself well in unstable markets. It is worth noting the forest model, which, like the previous ones, is based on a combination of financial ratios, but focuses on the assessment of the enterprise's ability to generate cash flow to cover liabilities and the efficiency of assets. All of these models are an important part of the information support system of the enterprise's financial and economic security, as they allow to draw reasonable conclusions about risks and to take precautionary measures in a timely manner.

In today's context, the digitalization of business processes has become a prerequisite for ensuring the effective financial and economic security of enterprises. The use of information technologies and automated security management solutions allows you to optimize the processes of collection, processing and analysis of financial data, which significantly improves decision -making and reduces the risks associated with insufficient information and human factor.

One of the main tools for ensuring the integrity of the financial and economic security of the enterprise is the introduction of ERP systems (Enterprise Resource Planning). These systems allow to process all financial and operational data of enterprises centrally, which significantly increases the efficiency of financial, accounting and control management. ERP systems, such as SAP, Oracle, 1C or Microsoft Dynamics, provide businesses to manage all aspects of their activities, including finances, purchases, supply, sales, production and human resources. With this centralized approach, businesses can reduce the likelihood of errors in accounts, increase transparency of transactions, and reduce the

risks of unauthorized access to critical information. ERP systems automatically integrate data from different departments, which allows for a timely detection of deviations in financial indicators, misconduct or inefficient use of resources. In addition, ERP systems provide compliance with the legislation through the automatic updating of the regulatory framework, which allows businesses to be sure of the relevance of their accounting and financial data, which is an important element in ensuring financial and economic security.

Another important element of modern information support system is the use of Big Data - large ranges of data that allow you to carry out an in -depth analysis of the economic and financial processes of the enterprise. Large data processing technologies provide real -time monitoring, which helps to identify potential threats in a timely manner and adjust the enterprise strategy to minimize risks. Thanks to Big Data, businesses can analyze data not only about their own financial indicators, but also about the market situation, the behavior of competitors, changes in legislation and other factors that directly affect the business environment. This allows you to respond to existing threats and predict possible economic crisis and adapt a strategy to change.

As a result of the introduction of Big Data, businesses can make a more accurate forecast of income, expenses, as well as to predict possible changes in the cost of resources and goods, which allows to make more sound management decisions on financial security.

It is important to use Business Intelligence (BI) to effectively manage financial and economic security. Platforms, such as Power Bi, Tableau, Qlik, allow you to visualize key financial and security indicators in a convenient and intuitive format. Thanks to these tools, the management of the enterprise can quickly receive the necessary information and make effective decisions to ensure financial security. Bi systems use a variety of data analysis methods, including forecasting, trend analysis and comparative estimates, which allows to monitor the current state of the enterprise's finances and to predict their development in the future, which allows to identify potential problems or threats to financial and economic safety, such as reduction of liquidity, deterioration of solidity or increase in credit.

GRC systems (Governance, Risk Management, and Compliance) is an important tool for integrating risk-oriented approach into the operating activity of the enterprise. These systems allow the management of the enterprise to receive all the necessary information for effective management of corporate risks, compliance with regulatory requirements and ensuring proper internal management policy. GRC systems help businesses monitoring real-time risks, automatically evaluate the level of compliance with politicians and standards, as well as identify violations in a timely manner and organize control measures. They also allow you to integrate all stages of risk management from identification to respond to them, which provides more efficient activity of the enterprise and reduces financial threats.

In real time, the use of artificial intelligence (AI) and machine learning (ML) is very urgent, which opens up new opportunities for forecasting and identification of financial risks. With these technologies, businesses can automatically analyze large amounts of data, identify anomalies and develop forecasts to increase financial security. Artificial

intelligence allows you to identify hidden patterns in market behavior, to predict changes in the value of assets, costs and income based on historical data and current economic trends. This allows companies not only to respond to real -time changes, but also to predict possible crisis situations before their occurrence.

Recently, special attention has been paid to cybersecurity of enterprises, since the leaks of financial information or attacks on accounting systems can seriously threaten the financial and economic security of the company. The introduction of modern antiviral systems, fireworks, data encryption and multifactorial authentication of users are necessary measures to prevent unauthorized access to important financial information.

Regular updating of software and security tools, as well as monitoring of real -time systems allow you to respond in a timely manner to potential cyber threats. Consideration of such factors in the information support system allows to reduce the risks of data leakage and to ensure high reliability of financial and economic security of the enterprise.

In the process of economic activity of the enterprise, various approaches to the collection, processing, generalization and storage of information are actively used. At each stage of information, there is a risk of threats that can seriously affect its integrity, confidentiality and accessibility. Loss control over information flows can lead to significant financial losses and reducing management efficiency.

Formation of an effective information security system involves solving a set of tasks related to the security of both structured and unstructured information. Structured (formalized) information is usually understood to be the data presented in the form of documents or in the form transmitted through technical means of communication. Protection of such information is possible through the use of information theory methods that allow you to calculate the level of security of individual objects. In cases where theoretical approaches do not allow to ensure accuracy of evaluation, expert methods are used. Practice testifies to the widespread use of methods based on informal systemic theory. The comprehensive application of different approaches, including the theory of random processes, evolutionary modeling, graph theory, etc., allows you to effectively model the information security system, taking into account its complexity and dynamism.

Information risks should be evaluated as a product of the probability of an incident on the potential financial loss that may cause information security. Regardless of the form of existence, the information should be properly protected, so it is necessary to constantly monitor potential threats and vulnerabilities.

The risk assessment procedure in information security is a systematic analysis of all information resources that can be exposed to threats. As a result of this analysis, it becomes possible to determine the prevention of preventive measures that reduce the likelihood of threats and minimize their negative consequences for the enterprise.

A typical sequence of information security assessment includes the following steps: identification of information assets and determination of their value; assessing the likelihood of potential threats; identification of vulnerable places in the information support system; calculation of probability of specific threats; determining the integral risk level, taking into account the likelihood, vulnerability and potential losses.

Potential threats are evaluated by an expert approach, which involves taking into account the set of threats, their relationships and appropriate characteristics. At the same time, for each specific threat, an individual protection means that allows you to increase the efficiency of response to it. The following main indicators are used in the analysis process:

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:

$$R_{t_i} = \sum_{k=1}^{kl} \omega_{t_i} p_{t_i} d_{t_i} c(a_k) \quad (3.3.1);$$

where, *kl* – the number of information sources aimed at threat $t_i,\ i = 1,2,3 \ldots\ldots, n;$

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 influence $d_{ti} \in [0; 1]$ can act as a key criterion in determining the sources of information or assets that are most prone to destructive influence of a certain threat. This indicator reflects the overall level of potential damage or negative impact that can be caused by a specific information object or asset.

Consider the possibility of calculating likely losses that can be caused by a consistent act of threats with a certain time interval between their occurrence. Such losses can be expressed mathematically in the form of the expected value of $M(t_{a,} t_{\beta,})$:

$$R_{M(t_{a,}\, t_{\beta})} = R\, t_a + \sum_{i=1}^{m} \sum_{j=1}^{r} p(t_{i,}\, t_j) R t_j, \quad (3.3.2);$$

where *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 $M(t_{a,} t_{\beta,})$:

$$F_{M(t_{a,}\, t_{\beta})} = \sum_{i=1}^{n} F t_i, \quad (3.3.3);$$

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

In the next stage of the analysis, the values of the estimated risk costs with the actual costs incurred to ensuring information security are compared. This allows you to make a reasonable decision on the nature and level of acceptability of a particular risk. In cases where the risk value of $R_{t_i} = Ft_i$ is equal to or less than a certain financial threshold $R_{t_i} \leq Ft_i$, such a risk is considered insignificant and may be left without additional response. At the same time, if it is observed that $R_{t_i} \geq Ft_i$, this indicates the need to revise approaches to protection: analysis of the effectiveness of already implemented measures and optimization of safety costs.

In case of significant potential threats, it is advisable to use strategies such as risks or insurance diversification, which allows to reduce the financial burden on the enterprise in the event of negative scenarios.

The method of expert assessment of risks concerning information security is appropriate and effective in the practice of economic activity of economic entities. Despite the presence of a formally organized system of protection of information resources, businesses need to constantly improve this system, striving for maximum reliability and efficiency. The comprehensive application of different methods of risk analysis allows not only to increase the level of information security, but also to make sound management decisions, to identify vulnerable places in the functioning of the enterprise, as well as to minimize potential losses that may arise in the system of information support for economic security management in a timely manner. The prerequisite for effective management of a modern enterprise is to improve the mechanisms of information support of management processes, because the information is the basis for decision -making. The main part of all information about economic activity is credentials that must be collected, processed and analyzed in a timely manner.

To optimize the information collection process, the structure of the information collection process is offered, which covers three main stages:

1. The initial stage - the formation of primary information occurs directly in production, warehouses, as well as in the cash desk of the enterprise. Primary data is collected on the basis of accounting documents, reflecting the receipts and expenses of funds, transactions with bank accounts, movement of materials, products produced, accounting of labor, etc.

2. Analytical stage - information is formed in the auxiliary units of the enterprise. At this stage, analytical information on regulated transactions, counterparties' debts, the movement of fixed assets and material resources are collected, which allows you to form a complete economic picture.

3. The final stage - data processing and generalization is carried out in the accounting service of the enterprise. Here, information from the previous stages is consolidated, grouped and reflected in the accounting registers, which allows to carry out a full analysis of financial and economic activity.

Consistent implementation of these stages allows to improve the quality of management information, to identify risks in a timely manner and to ensure rational decisions. Formation of effective accounting information support system in the context of economic security provides: creation of a single source of reliable information; ensuring communication between all accounting facilities; unification of forms of information presentation; use of common economic indicators in different accounting processes.

As a result of the introduction of a unified information support system, the following goals are achieved: completeness, accuracy and reliability of accounting information; prompt access to data; objective display of economic processes; increasing the overall quality of management decisions at all levels. Therefore, optimization of risk assessment methods with improving the information infrastructure of the enterprise generates a solid basis for ensuring stable financial and economic security and effective management.

SCIENTIFIC EDITION

ACCOUNTING, FINANCIAL, AND ECONOMIC SUPPORT FOR SUSTAINABLE DEVELOPMENT OF THE AGRICULTURAL SECTOR: THEORETICAL FOUNDATIONS AND PRACTICAL RECOMMENDATIONS

COLLECTIVE MONOGRAPH
In English

Responsible for the issue is Natalia Vasylieva

The materials are printed in the author's edition.
The views expressed in the publications are solely the position of the authors.
Authors are responsible for the scientific level of publications, the validity of conclusions, the reliability of results, and the presence of plagiarism.

Підписано до друку 30.04.2025 р. Формат 60 х 841/16. Папір офсетний. Друк цифровий. Обл.-вид. арк. 35. Ум.-друк. арк. 35. Тираж 100 прим. Зам. № 95

Видавець ФОП Максимовська Ю. А.
Свідоцтво держ. реєстрації серія ДК № 7589 від 07.02.2022

Надруковано у ТОВ "Україна-Принт"
Вул. Архитектора Олега Петрова, 25, Дніпро, тел. 067 165 74 75

Автори:
Галина ПАВЛОВА, Олександр АТАМАС, Олександр ТКАЧЕНКО, Людмила ВОЛЧАНСЬКА, Ольга ГУБАРИК, Олена ДУБИНА, Ольга ЧЕРНЕЦЬКА, Сергій ЮРЧЕНКО, Марія БАРДАДИМ, Леся ВАСІЛЬЄВА, Ольга ОДНОШЕВНА, Тетяна МАЧАК, Альона МІНЬКОВСЬКА, Тетяна САВАНЧУК, Світлана ХАЛАТУР, Світлана КАЧУЛА, Анна СІРКО, Наталя ВАСИЛЬЄВА, Юлія МАСЮК, Оксана ВОДОЛАЗСЬКА, Оксана ГРАБЧУК, Ілона СОЛОДОВНИКОВА

О17 Облікове, фінансове та економічне забезпечення сталого розвитку аграрного сектору: теоретичні основи та практичні рекомендації: колективна монографія. Англійською мовою. Дніпро: ФОП Максимовська Ю. А., 2025. 488 с.

ISBN: 978-617-95342-7-0

UDC 336 : 338 : 631 : 657