UDC 657

S.I. Vasylishyn, Dr. Sci. (Econ.), Prof., CAPA *(ALC «Institute of Accounting and Finance» of NAAS; NSC «Institute of Agrarian Economics», Kyiv; State Biotechnological University, Kharkiv)*
Yu. S. Bezdushna, Dr. Sci. (Econ.), Prof., CIPA, DiplFR *(NSC «Institute of Agrarian Economics», Kyiv)*

COMPONENTS AND STAGES OF ENSURING CYBERSECURITY OF AGRARIAN ENTERPRISE ACCOUNTING DATA

The digitalisation of the economy has contributed to the emergence of the latest integrated systems for processing and storing financial information, so traditional forms of accounting have been replaced by automated accounting based on the use of a software package that automates up to 90% of all manual operations of an accountant. In the process of managing the economic security of business structures and its accounting and analytical support in the digitalised world, cybersecurity of the information environment plays an important role. Cybersecurity in the modern world is a crucial tool for business development and its strategic growth, as the losses of global companies from cybercrime are increasing every year.

The most common types of cyberattacks have been and remain “Spear Phishing” and “Watering Holes”, the main feature of which is the infection of a specific target group of network users. A fraudster planning a targeted phishing attack can create a fake employee email address and use it to write to several employees, requesting information about the company. Thinking that they are communicating with a colleague, employees may provide this information without any suspicion. In the case of a “Watering Holes” attack strategy, hackers place malware in the code of websites that are most likely to be visited by employees of the targeted company. If an employee accesses such a site from a company computer, the entire network can be exposed to a data-stealing virus.

The results of our expert survey of practicing accountants show that 33% of the digitalisation risks of enterprises are associated with physical failure of equipment, 27% with disclosure of trade secrets, and 20% with unauthorised information leakage as a result of cyber attacks. Automation of accounting is a way to minimise the impact of the human factor on the implementation of accounting functions and management decision-making. The human factor is associated with a high probability of intentional distortion of conclusions and accounting information, the occurrence of accidental technical errors, personal gain or enrichment through fraudulent transactions with the assets and liabilities of the enterprise [1]. The consequences of automation are the need to form technical, software, information, personnel and organisational components of information security (Table 1).

In view of this, the impact of cyber threats on the economic security of agricultural enterprises should be considered in terms of four components: network, software, information and database, and personnel. The unity of actions to prevent the impact of cyber threats, taking into account these components, allows achieving a

synergistic effect of measures to cyber defend the information shell of business structures.

Table 1 - **Components of enterprise information security**

Component name	Characteristics
Technical	Complex of computer equipment: processors, monitors, modems, cables, printers, other communication channels
Software	A set of software and its modules; operating systems and their add-ons
Information	A set of accounting information stored electronically on internal and external memory media
Staffing	Staff of accounting services and departments that have access to accounting information and its protection
Organisational	Unit or employee responsible for keeping trade secrets and protecting accounting information

Source: developed by the author.

According to Jeff Smith, the modern era of digital transformation of outdated infrastructure optimised for legacy applications increases the level of competitive, budgetary and financial risk. In his opinion, only a true enterprise cloud - hyperconvertible, on-premises and hybrid - will ensure security, reliability and flexibility, as well as accelerate innovation and reduce risk [2]. We believe that full automation of the modern accounting network and the use of cloud-based information storage technologies will allow us to build reliable information links within the accounting department and between the accounting department and other structural units of the enterprise. At the same time, the level of security and the development of the necessary levers to avoid digitalisation risks, including the organisation of information security by creating a separate unit (expert group within the unit) or engaging professional audit or consulting companies, require the necessary attention of owners and employees.

The main stages in the process of organising the protection of accounting information are as follows [3]:

1) identification of threats to information security;

2) identification and control of risks and features of information support for their management;

3) building a model of risk management and its information support;

4) formation of a system of measures to counteract threats to information security;

5) development of organisational regulations for the protection of accounting information;

6) control of information security and assessment of measures to ensure it.

As a rule, all cybercrimes have a single sequence of cybercriminals' actions, which necessitates a phased management of digitalisation risks

In particular, the purpose of the preventive stage is to assess (reconnaissance) the possible impact of cyber risks. At the stages of actual penetration of cybercriminals into the information environment, the reactionary stage of immediate blocking of a cyber-incident (or cyber-attack) is necessary, while the protective stage involves preserving the available amount of information to the maximum extent possible and transferring it to other media or cloud storage. The purpose of the prognostic and monitoring stage is to continuously monitor known and potential digitalisation risks and forecast scenarios of their impact on the information and, as a result, economic security of enterprises.

As a result of the preventive, reactive, defensive, prognostic and monitoring stages of cyber defence, it is possible to progressively plan and implement restoration measures as a result of the impact of cyber-attacks on economic security in the short, medium and long term.

Information sources

1. Automation. *Visnyk Zaporizkoho natsionalnoho universytetu*, no. 2, pp. 65–71.
2. Jeff Smith. Re–thinking «risk» from digital disruption. Business acumen magazine. 2018. URL: https://www.businessacumen.biz/index.php/innovation-leaders/news-better-business-technology/3292-re-thinking-risk-from-digital-disruption (Accessed November 1, 2024).
3. Vasylishyn S. (2021). Improving the Levers of Digitalization Risks Management of Economic Security and Formation of Cybersecurity of the Accounting System. *Herald of Economics*, no. 1 (99), pp. 97–110, https://doi.org/10.35774/visnyk2021.01.097

УДК 657:33

Н.С.Акімова, канд. екон. наук, проф. *(ДБТУ, Харків)*
Н.В. Новицька, канд. екон. наук, доц. *(ХНУМГ ім.О.М. Бекетова, Харків)*

ФУНКЦІОНУВАННЯ ОБЛІКОВО-АНАЛІТИЧНОЇ СИСТЕМИ В УМОВАХ СТАЛОГО РОЗВИТКУ

Розвиток ринкових відносин в Україні, що супроводжується її інтеграцією у світове співтовариство, викликає необхідність перегляду існуючих та розробки нових методів управління та контролю.

Стабільність та конкурентні переваги суб’єктів господарювання в умовах ринку багато в чому залежать від ступеня оперативного подання та достовірності інформації, на основі якої проводиться економічний аналіз, формуються та реалізуються управлінські рішення.

Для відповідності ринковим відносинам у трансформаційній економіці України необхідно сформувати адекватну обліково-аналітичну систему.

Забезпечення концепції сталого розвитку та діджиталізація суспільства призводять до ускладнення внутрішніх та зовнішніх зв’язків у системі, що обумовлює трансформацію до гнучких активно-адаптивних обліково-аналітичних систем [1, с. 85]. Активність гнучких систем обліково-