UDC 343.72
JEL Classification: F52 H83
DOI: http://doi.org/10.31617/visnik.knute.2021(135)03

NEZHYVA Mariia,
PhD in Economics, Associate Professor
of the Department of Financial Analysis and Audit
Kyiv National University
of Trade and Economics
Ukraine, 02156, Kyiv, 19, Kyoto str.

E-mail: m.nezhyva@knute.edu.ua
ORCID ID: 0000-0002-3008-5338

MYSIUK Viktoriia,
PhD in Economics, senior lecturer
of the Department of Financial Analysis and Audit
Kyiv National University
of Trade and Economics
Ukraine, 02156, Kyiv, 19, Kyoto str.

E-mail: mysuk091@ukr.net
ORCID ID: 0000-0001-8931-733

ASP STRUCTURE: PREVENTION OF ECONOMIC FRAUD

Measures to detect fraud and fraudsters have been developed in the article, including the definition of common "red flags" for a person who commits typical and accidental abuse. The main organizational control structures used to prevent fraud are identified. Evidence was analyzed in both paper and electronic formats, including big data, to form a classification of fraudsters and fraudulent activities. Possible solutions for effective fraud management and its prevention within the company by the help of ASP approach were developed.

Keyworlds: fraud, economic fraud, fraudster, bribery, forensic, ASP, ACFE.

Background. An important element of stability and efficiency of financial and economic activity of enterprises is their economic security in an open economy. In the course of financial and economic activities, very often companies are faced with various types of fraud, including: financial fraud, employee misconduct, fraud and other risks that diminish the financial result. According to the Prosecutor General's Office of Ukraine, the number of criminal offenses in the financial and credit sector (banking, foreign trade, privatization) committed by organized criminal groups, the pre-trial investigation of which in 2018 amounted to 175 measures [1]. It is often not enough to use standard audit techniques to identify the risk nature, as fraud is often a pre-planned and thought-out process that is accompanied by inventive measures to cover it.

In the case of an improper control system, all of the above features can create the basis for various types of fraud, in particular, allowing employees to distort data when displaying business transactions and reporting. Therefore, there is a need to introduce new techniques to detect fraud within the enterprise, and to strengthen the system for detecting and ending financial crimes by counterparties. Today, organizations, in addition to standard auditing methods, need to use alternative business protection methods, which include a forensic or forensic-audit.

Analysis of recent researches and publications. Financial investigations are the subject of research by many scientists such as K. Nazarova, O. Zaremba, A. Kovbel, R. Deb, A. Shelupanov and A. Smolina, A. Enofe [2–9]

and others. For example, V. Suits et al. [10] investigated the theoretical basics of forensics, the nature and types of fraud, the stages and basics of the technique of forensics, its basic methods, as well as practical issues of its conduct. M. Dubinina et al. [11] pay attention to theoretical and organizational and methodological principles of forensic audit development in Ukraine. M. Horodylov et al. [12] considered the concept of "forensic" in order to introduce the term into scientific circulation and to properly understand its meaning. G. Solomina [13] substantiates the ways of using and implementting the services of forensics in ensuring the economic activity of the enterprise, determining the priorities of the targeted areas of financial investigations. Particularly, researches of state financial audit with an opportunity to transform it into forensic were examined by R. Deb [14], who allocated corruption risks of accounting and essential influence on the process of state audit. A. Semenets [15] proposes to introduce into the accounting theory the concept of "forensic audit", which should be understood as the process of studying company's reporting and economic operations in order to develop measures to respond, manage and prevent fraud on the basis of expert judgement. A. Enofe et al. [9] examined the impact of forensic audit on corporate fraud. At the same time, market development is constantly generating new demands for research, and therefore the recommendations previously developed by the scientists need to be improved and adapted to current market changes.

The **aim** of the article is to study the trends of economic fraud in the world and to establish methods for preventing and minimizing the risks of fraud in the enterprise.

Materials and methods. The research was carried out using the following methods: monographic – to generalize the theoretical and methodological foundations of the formation of costs for marketing communications of enterprises; analysis and synthesis, induction and deduction – to pose the problem of research, detailing and clarification of its subject); system analysis – to clarify the essence of concepts; classification-analytical – for the classification of costs; graphic – for visual and schematic representation of theoretical and practical results of research and questionnaires. The information base of the study is monographic literature, regulations of Ukraine, materials of periodicals, as well as information from the Internet.

Results. Cybersecurity incidents have begun to occur more frequently and are regularly covered by news headlines, which is of increasing concern to consumers and business executives. Despite the close attention that has been drawn in recent years, it is still difficult for most organizations around the world to grasp and manage emerging cyber risks in an increasingly complex digital environment. Recognizing that the digital environment is becoming more complex every day and our dependence on data and networking is growing, the development of cyber-resilience, a large-scale, devastating, cascading event, has never been so important. Despite the growing awareness and publicity of the events and consequences of cyberattacks,

many companies are still unprepared for real threats. If the world does not create a real effective cyber defense system, as early as 2021, the business could suffer $ 6 trillion in cyberattacks [16].

Achieving higher levels of cyber resilience within individual businesses or across society requires greater effort to identify and manage new risks in current technologies. Organizations need the proper guidance and procedures for implementing information security measures that need digital progress. When conducting digital transformation, particular attention should be paid to protecting the technologies and processes being implemented, and in some cases incorporating cybersecurity transformation.

Over the past two years, 48 % of Ukrainian organizations have suffered from economic crime and fraud, including through modern information technology. Bribery and corruption (73 %) are the leaders among economic crimes that have been plagued by organizations over the past two years. The top 5 also include: property misappropriation (46 %), procurement fraud (33 %), personnel management fraud (33 %) and cybercrime (31 %). Ukrainian respondents expect bribery and corruption to be the most significant economic crime for their organizations in the next two years [17].

Forensic service is a relatively new phenomenon even in the countries with developed market economies. The first consulting and audit firms to provide such a service have appeared in Ukraine relatively recently. Forensic cannot be equated with the common concept of "audit" in our country, because this service is much broader than audit. Forensic involves the involvement of specialists in various specialties, which help the company to resolve conflict situations related to fraud. Forensic is often described as a financial investigation. An essential part of the forensics service is corporate intelligence and computer investigations.

There are different views on the essence of forensics. Domestic experts believe that forensics is the detection and reduction of fraud risks, illegal actions and unethical behavior in the field of economic activity. Moreover, financial losses resulting from misappropriation of assets that are unfavorable to the company's purchases and sales, as well as other financial abuses – by contractors, management or employees that have a direct negative impact on the entity's income and expenses. At the corporate level, financial investigations have a clear purpose to detect fraud among both contractors and employees of the organization, as they can cause significant financial losses, damage the company's reputation and violate the entity's economic security. Many Western firms, among other things, audit computer systems and provide information security during financial investigations.

Financial investigations can be conducted by both authorized public bodies and private organizations. In other words, the subjects of financial investigations are both representatives of public authorities and subjects of the private sector of the economy, in particular consulting companies.

Financial investigations are extremely complex type of research. *Firstly*, their implementation requires many years of experience in the financial sector. *Secondly*, no agency is able to capture on its own the wide range of information needed to track all financial transactions. *Thirdly*, the scale, diversity and variability of the financial sector complicate financial investigations. The subject of financial investigations as a special type of analysis is the financial component of criminal activity. It is the study of the financial component on the basis of appropriate methodology, technology and organization of work can significantly help investigators in identifying and investigating virtually any crime related to the movement of financial resources and traces in the form of financial information.

Taking into account the complexity, dynamism and great variety of manifestations of financial fraud, among a number of reasons that lead to its existence, it is appropriate to distinguish the following main groups:

economic reasons: rapid growth of financial transactions in today's globalized world; extremely high incomes of financial fraudsters compared to much smaller probable financial penalties; the presence of personal financial problems and low living standards of a large part of the population; the disappearance of borders for free movement of money, goods and services that provoke the growth of transnational financial crime;

reasons of moral and psychological nature: desire for quick profit; lack of respect for the owner and someone's property; low level of financial literacy of persons who are primarily targeted by fraud; psychological propensity of individuals to risky actions and various scams;

reasons of regulatory nature: imperfection of domestic legislation to combat financial fraud; lack of a clear list of transactions directly related to the probable fraudulent misappropriation of funds; low probability and insignificant penalties for fraud;

reasons of infrastructural and organizational nature: increase in the volume of out-of-person contactless transactions, online trade, online auctions, etc.;

reasons of institutional nature: reducing the confidentiality of personal data; rapid development of technologies used by cybercriminals; lack of proper organization of the fight against financial fraud by the authorities and the imperfection of their personnel policy; high level of latency of fraudulent crimes; a small percentage of disclosed registered crimes related to financial fraud (on average, law enforcement officers disclose every fifth crime); lack of preventive measures and effective control over the spread of fraudulent schemes; lack of transparent information for ordinary citizens about the activities of financial institutions in Ukraine and possible manifestations of fraud in financial market, etc.).

Forensic is also defined as an independent economic investigation, which is usually conducted in the interests of company owners. Economic investigation allows to determine the amount of damages at the conclusion of the contract or violation of its terms, in case of non-performance of warranty

obligations. It is used to prevent possible disputes, to assess insolvency risks, bankruptcy and reorganization, to assess the business as a whole. Corporate fraud is widespread in modern business, the forms and motivations of which have different consequences for the company's activities.

An important area of activity in the provision of forensic services is computer investigations. The so-called IT forensics is "data analysis in electronic form, including analysis of e-mail and documents, including deleted letters and files on hard drives, mail and file servers, automation of the comparison of large amounts of corporate data, digital evidence and providing data to the court. Summarizing the above definitions, we can draw the following conclusions. In general, the term "forensic" is used to describe the independent initiative to investigate, examine, analyze, assess, resolve situations and develop procedures to combat fraud, corruption, commercial bribery, withdrawal and misappropriation of funds and other assets, illegal actions, assessment of contractual activities, settlement of differences between the parties on financial and business issues. Such activities can be initiated by the owners or the company's board of directors.

Also, the term "forensic" is an activity to provide services on financial, economic, legal, commercial and other issues that involve significant economic risks, or to identify actions of employees or organizations that do not comply with laws, regulations, standards, principles.

There is an opinion that "forensic" is a set of independent initiative services provided by audit, consulting and specialized companies for owners, board of directors of companies of various organizational and legal forms. These services include the following *works*:

- financial investigations;
- fraud risk management;
- corporate (business) intelligence;
- extrajudicial, pre-trial expertise, as well as assistance in court proceedings;
- investigation of fraud using information technology;
- counteraction to legalization of illegal income;
- protection of intellectual property;
- verification of contractual obligations and reliability of business partners;
- prevention of financial and reputational damage;
- checking messages on the hotline;
- detection and analysis of hidden commercial risks;
- settlement of differences between the parties to the conflict on financial and business issues;
- development of procedures aimed at combating fraud, corruption, withdrawal of funds, misappropriation of assets;
- compliance investigation;
- financial examination of documents.

In practice, forensics includes other services related to the prevention of various thefts, fraud, as well as the collection of evidence on the facts that have already occurred.

Representatives of various specialties take part in activity in the field of forensics: accountants, auditors, experts in financial investigations, experts in the field of information technologies (project managers, experts in the organization of processes, software developers, database administrators), lawyers, security specialists, journalists, political scientists, specialists in the field of structural analysis and mathematical modeling.

Substantiating the *interdisciplinary nature of financial research*, they include the following aspects:

economic – detection and study of the economic mechanism of violations; assessment of the damage caused by a specific violation; development of recommendations to eliminate the economic causes of violations;

legal – qualification of a specific violation; study of legislation to avoid liability for violations, development of recommendations for their elimination;

forensic – the process of collecting, consolidating and studying materials (evidence of violation); methodology and methods of collecting, consolidating and studying materials (evidence of violation);

criminological and psychological – identification of psychological characteristics of persons who have committed violations in the financial sphere; measures to prevent violations in the financial sector.

This comprehensive approach is more in line with the subject of financial investigations – the use of knowledge of criminology, accounting, financial control, analysis, audit in combating crime.

The possibility of financial fraud is primarily due to the favorable conditions for fraud, the possibility of access to available financial resources, inadequate corporate culture and weak control (or lack thereof) over the actions of a potential fraudster.

The motivation of fraudulent actions can be due to the presence of certain financial problems in such a person (difficult financial situation and the need to improve it, propensity to risky and risky acts) and external pressure from others, lack of strict financial control over the activities of potential fraudsters and the probability of obtaining very high incomes by financial fraudsters.

Rational justification of potential fraud involves justifying a person's wrongdoing ("no one will notice it", "it will not hurt anyone", "it is less evil", "others do it too", etc.). But the rationality also lies in the fact that fraud is often committed by people who are prepared and competent, morally consistent with such an act. Such individuals are endowed with sufficient experience, intelligence, cunning and flexibility, understanding the sequence of their actions and predict the appropriate reaction of the enemy, they use any weaknesses in the organization for their own purposes.

It should be emphasized that the last component (justification of fraud) is the most problematic in terms of fraud prevention, as it largely contains (and difficult to control from the outside) moral and ethical component.

Thousands of businesses are affacted by fraud around the world everyday. Fraud examination and forensic accounting provide tools and techniques for preventing, deterring, detecting, investigating and remediating bad acts grounded in financial gain.

According to the Association of Certified Fraud Examiners (ACFE), "average losses from fraud are about 5 % of total gross domestic product or GDP. When that 5 % is applied to actual economic production, total losses from fraud may be as high as 3.5 trillion worldwide. In the United States losses have a trillion dollars total" [18]. Based on ACFE reporting, we can distinguish *three popular fraud categories* (*figure 1*).

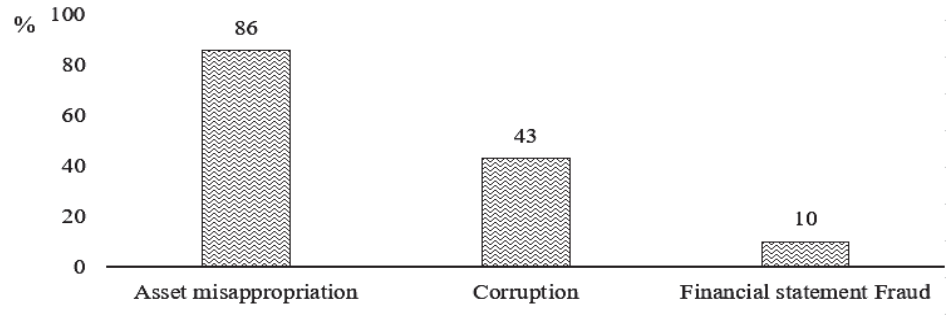

Figure 1. How is occupational fraud committed?

Source: [18].

Depending on each company fraud investigation process, we can distinguish them into *different groups*: which do not care about fraud investigation, which have a really well developed anti-fraud system, which know about fraud cases and do not want to have any measures to uncover them. Companies' management knows about fraud status (*figure 2*).

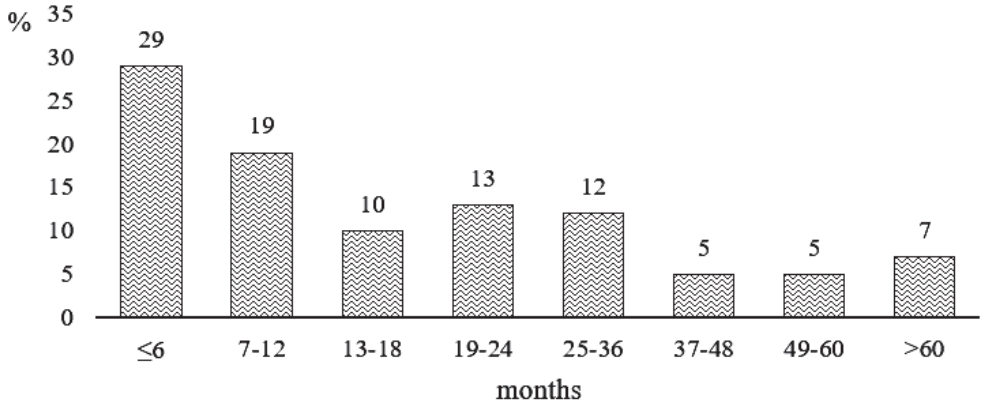

Figure 2. What is a fraud duration in Your company?

Source: [18].

Such fraud duration dynamic has negative impact on strategic goals of company and indicates that in most cases there are windows for financial controls improvement and other measures usage to prevent fraud in a company. That means that management of such companies also is involved in such fraud schemes.

The level of company involvement to economic fraud detection can identify its group in ASP (Anonymous, Suspects and Prospects framework) and identify measures how to improve quality of internal controls to have

reliable system of fraud prevention. Below are descriptions of each segment of ASP framework (groups of companies) and which vectors of improvement should be considered by each company (*table 1*).

Table 1

ASP framework to detect and overcome a fraud

Indicator	Description
Anonymous (aspirational companies)	Wide range of companies which could be affected by economic fraud, but they do not care about that yet.
Suspects (aware companies)	There companies that know about fraud in companies, try to organize some measures but do not control its effectiveness to be aware that it works well.
Prospects (engaged companies)	There companies which have well organized system of internal control, prevention measures for fraud detection, always control effectiveness measures and ways to overcome fraud. These companies have already faced economic fraud, know the profile of fraudster and have internal forensic specialist.

Source: developed by the authors.

Companies from Anonymous group should consider using some internal controls politics. After fraud detection in such company will be transferred to Suspects group, where the company considers organizing some other measures but does not control its effectiveness to be aware that it really works well. In case the level and frequency of fraud detection by sophisticated measures will growth, company considers extending the system and quality of fraud prevention. After such changes company will be considered in Prospects group that cares about fraud detection and prevention in high level.

Due to the results of the survey, a significant fraud committed by employees (from 28 % in 2016 to 56 % in 2018) has increased in Ukrainian entities, among which the proportion of fraud committed by senior management has also significantly increased (from 27 % in 2016 to 55 % in 2018) [19].

Due to the fact, that fraud is the long-lasting process in a company, some internal techniques should be used to prevent it. The most effective measure to minimize fraud losses is to use some tests (*table 2*).

Table 2

List of anti-fraud tests to prevent it in a company

Question block	Test discription
Does a company provide some training for staff to clarify how to prevent fraud?	• Do all employees know what fraud means? • Do all employees know how fraud affects on a company's results and corporate culture? • Do all employees know what to do when they identify fraud? • Has a company any anti-fraud policy? Do all employees know how it works?
Does a company have some preventional measures known by employees?	• Will fraudster be punished or can commit fraud one more time? • Is there unexpected audit in a company? • Are there any analytical methods used in a company to detect a fraud? • Do all business processes correspond to agreed internal company policy?

End of the table 2

Question block	Test discription
Does a company have agreed fraud reporting process?	• Do the employees know how to communicate about potential fraud? • How many channels have staff for fraud reporting and are they easy accessible? • Can staff trust these reporting channels? • Does preventional fraud mechanism cover only internal process or cooperation with vendors as well?
Is company's management honest?	• Do the employees have possibility to avaluate management honesty? • Are all business goals clearly clarified to staff? • Does a company use fraud commitment as an indicator to staff and management evaluation? • Does the board of directors evaluate and control fraud in a company?
Does a company have a regular fraud risk assessment?	• Does a company have risk assessment plan? • Doesa a company have risk assessment check-list?
Does a company have some standard anti-fraud procedures?	• Segregation of duties • Identification of persons • Job rotations • Regular planned in advance vacations
Does a company have internal control system or interal auditor which provides regular auditing?	• Does company have internal auditor? • Does company have internal audit schedule?
Does a company have employee support programs?	Such program is required in case an employee suffers from some preasure (finansial, psyhical, personal) and that preasure can negatively affect the company. The employees should know they can discuss it any time with the company support team
Does a company have open-door policy allowing staff to share any pressures faced at work (may be anonimus assessment of personnel)?	The employee should feel free to share any information with the management or special responsible person from support team about any evidence referred to fraud commitment in the company. It should be personal talk or anonimus letter

Source: developed by the authors.

Such anti-fraud check list allows the company to clarify the level of internal anti-fraud policy development. Answering the question, you will clarify whether your company is suffered from fraud or you will find such "red flags" which sould be controlled. It also allows to optimize anti-fraud preveventional measures to protect the company in the future.

Conclusion. Fraud is a major problem that should be constantly monitored in the company in fast-growing business environment today. Fraud has a negative impact on business processes because the company irreversibly loses part of the revenue from the sale of its services. Ongoing fraud risk evaluation and its prevention is necessary part of any management level. The main status and trends of economic fraud in the world and Ukraine have been analyzed in this atricle. Methods of preventing and minimizing the risks of fraud in a company have been developed in this paper since fraud level in Ukrainian businesses is high.

To prevent the fraud, each company can use short chek-list of anti-fraud tests, which have been developed in the article. Such implementation allows companies to minimize fraud risk and business losses. Fraud usually has long-lasting duration and all anti-fraud controls should be performed on regular base, it must have anti-risk procedures that are willing to build anti-fraud culture.

All companies suffer from fraud and they can be divided into three groups depending on the level of their involvement in fraud struggle. Company should consider exact measures to fraud prevention in each group due to ASP framework.

REFERENCES

1. Sujc, V. P., & Anushevskij, I. I. (2014). Forenzik: metody i metodika finansovogo rassledovanija [Forensic: methods and techniques of financial investigation]. *Audit I finansovyj analiz – Audit and financial analysis*, *6*, 215-227 [in Russian].
2. Nazarova, K. O., Zaremba, O. O., Kopotienko, T. Yu., & Misiuk, V. O. (2018). Internal control system: SOX-requirements approach to assessment. *Financial and credit activity: problems of theory and practice*, 185-192. Retrieved from http://fkd.org.ua/article/view/154190 [in English].
3. Kovbel' A. (2019). Hroniki auditora. Forenzik – iskusstvo rassledovanija ljudej i deneg [Auditor's chronicle. Forensic is the art of investigating people and money]. Kiev [in Russian].
4. Kovbel', A. Forenzik – A-B-C [Forensic – A-B-C]. *blog.liga.net.* Retrieved from https://blog.liga.net/user/a.kovbel/article/35985 [in Russian].
5. Kovbel', A. Forenzik – unikal'nyj mul'tizadachnyj instrument v rukah sobstvennika [Forensic is a unique multitasking tool in the hands of the owner]. *blog.liga.net*. Retrieved from https://blog.liga.net/user/a.kovbel/article/35532 [in Russian].
6. Kovbel', A. Forenzik: prakticheskie kejsy frodov i metody ih minimizacii [Forensic: practical cases of fraud and methods of their minimization]. *blog.liga.net*. Retrieved from https://blog.liga.net/user/a.kovbel/article/38068 [in Russian].
7. Deb, R. (2018). Financial Audit or Forensic Audit? Government Sector Panorama. *Indian Journal of Corporate Governance*, *11*, 135-158 [in English].
8. Shelupanov, A. A., Smolina, A. R. (2020). Forenzika. Teorija i praktika rassledovanija kiberprestuplenij [Forensic. Theory and practice of cybercrime investigation]. Moscow: Gorjachaja linija – Telekom [in Russian].
9. Enofe, A., Omagbon, P., Ehigiator, F. (2015). Forensic Audit and Corporate Fraud. *IIARD International Journal of Economics and Business Management*, *1*, 8, 55-64 [in English].
10. Sujc, V. P., & Anushevskij, I. I. (2014). Forenzik: metody i metodika finansovogo rassledovanija [Forensic: methods and techniques of financial investigation]. *Audit I finansovyj analiz – Audit and financial analysis*, *6*, 215-227 [in Russian].
11. Dubinina, M., Ksonzhyk, I., & Syrtseva, S. (2018). Forensic accounting: the essence and prospects of development in Ukraine. *Baltic Journal of Economic Studies*. (Vol. 4), *1*, 131-138 [in English].
12. Gorodilov, M. A., & Shkljaeva, N. A. (2018). Forenzik v ramkah jekspertno-analiticheskoj i auditorskoj dejatel'nosti: teoreticheskoe issledovanie ponjatija. [Forensic in the framework of expert-analytical and auditing activities: theoretical study of the concept]. *Uchet. Analiz. Audit – Accounting. Analysis. Audit*. (Vol. 5), *2*, 72-78 [in Russian].

13. Solomina, G. V. (2018). Forenzik – instrument finansovogo rozsliduvannja dijal'nosti pidpryjemstva [Forensic is a tool for financial investigation of the enterprise]. *Naukovyj visnyk Mukachivs'kogo derzhavnogo universytetu – Scientific Bulletin of Mukachevo State University*. Ekonomika. Issue 2(10), 144-149 [in Ukrainian].
14. Deb, R. (2018). Financial Audit or Forensic Audit? Government Sector Panorama. *Indian Journal of Corporate Governance*, *11*, 135-158 [in English].
15. Semenec', A. (2019). Forenzik audyt jak efektyvnyj zasib antykryzovogo upravlinnja torgovel'noju dijal'nistju [Forensic audit as an effective means of crisis management of trade activity]. *Biznes Inform – Business Inform*, *4*, 280-287 [in Ukrainian].
16. Presreliz Kyi'vs'koi' torgovo-promyslovoi' palaty, jakyj je u rozporjadzhenni Ukrinformu, za pidsumkamy II Mizhnarodnogo forumu "Kiberbezpeka – zahysty svij biznes" [Press release of Kyiv Chamber of Commerce and Industry, which is available to Ukrinform, following the Second International Forum "Cyber security. Protect your business!"]. Retrieved from https://www.ukrinform.ua/rubric-economy/2800152-svitovij-biznes-za-rik-moze-zaznati-zbitkiv-vid-kiberatak-na-6-triljoniv-eksperti.html [in Ukrainian].
17. PwC Global Economic Crime and Fraud Survey 2018: Ukrainian findings. Retrieved from https://www.pwc.com/ua/en/survey/2018/economic-crime-survey.html [in English].
18. Global study on occupational fraud and abuse. *www.acfe.com*. Retrieved from https://www.acfe.com/report-to-the-nations/2020 [in English].
19. Nazarova, K. O., Zaremba, O. O., Kopotienko, T.Yu. (2018). MiInternal control system: SOX-requirements approach to assessment. *Financial and credit activity: problems of theory and practice*, 185-192. Retrieved from http://fkd.org.ua/article/view/154190 [in English].
20. Shelupanov, A. A., & Smolina, A. R. (2020). Forenzika. Teorija i praktika rassledovanija kiberprestuplenij [Forensic. Theory and practice of cybercrime investigation]. Moscow: Gorjachaja linija-Telekom [in Russian].
21. Association of Certified Fraud Examiners. *www.acfe.com*. Retrieved from https://www.acfe.com [in English].

Стаття надійшла до редакції 07.12.2020.

Нежива М., Мисюк В. ASP структура: попередження економічного шахрайства.

Постановка проблеми. *У сучасному швидкозростаючому бізнес-середовищі шахрайство є головною проблемою, що потребує постійного вивчення в компанії. Шахрайство негативно впливає на бізнес-процеси і призводить до того, що компанія безповоротно втрачає частину доходу від реалізації своїх послуг, а тому управлінська ланка будь-якого рівня повинна забезпечувати ефективність проведення перманентної оцінки ризику шахрайства та вживати заходів, які будуть йому запобігати у майбутньому.*

Метою *статті є вивчення тенденцій економічного шахрайства у світі та Україні, визначення методів запобігання та мінімізації ризиків шахрайства в компаніях.*

Представлене дослідження базується на застосуванні таких ***методів****, як: монографічний; аналіз та синтез, індукція та дедукція; системний аналіз; класифікаційно-аналітичний; графічний.*

Результати дослідження. *Виявлення шахрайства є важливим фактом для команії, оскільки швидкість та спосіб його виявлення можуть значно впливати на розмір заподіяної шкоди. Виявлення шахрайства також є ключовим процесом для його запобігання, оскільки компанії можуть вжити заходів для вдосконалення способів його вияву, що, у свою чергу, збільшує усвідомлення персоналу про те, що шахрайство буде виявлено, і цей факт може стати превентивним методом, який*

запобігатиме шахрайству у майбутньому. У проведеному дослідженні розроблено контрольний список запитань, згідно з яким компанія зможе провести системну ідентифікацію шахрайства, і залежно від виявленого рівня шахрайства та внутрішньокорпоративної політики з боротьби із шахрайсвом, кожна компанія має змогу розробити заходи щодо запобігання йому у майбутньому. Запропоновано можливі рішення ефективного запобігання шахрайству у компанії з використанням ASP структури.

Висновки. *З ціллю допомогти компаніям зрозуміти потенційний вплив різних заходів проти шахрайства розроблено список контрольних питань. Визначено, що усі компанії на ринку, які страждають від шахрайства, можна поділити на три групи залежно від рівня їх участі у боротьбі з шахрайством. Для кожної групи компаній діють свої ефективні засоби по боротьбі із шахрайством, реалізаціях яких представлена за допомогою ASP структури.*

Keyworlds: шахрайство, економічне шахрайство, шахрай, хабарництво, форензік, ASP, ACFE.