DOI: 10.30525/978-9934-588-61-7-4

Gavrilko T. O.
Candidate of Economic Sciences, Associate Professor
National Aviation University

RISKS OF FRAUD IN THE FIELD OF FINANCIAL SERVICES

Summary

The article considers the risks of fraud that arise in the field of financial services in the context of technological and information changes occurring in modern society. The risks of fraud in the banking sector have been studied and the existing approaches to the typology of risks have been analyzed. Internal and external risks of fraud in banking institutions have been considered. The tendencies of external fraud with the use of cyberspace in the conditions of a coronavirus pandemic have been analyzed. The classification of frauds in relation to customers and employees of banking institutions and ways to prevent it have been proposed. The risks of fraud in the field of non-banking financial services have been studied. The sources of fraud in financial companies, credit unions and insurance companies have been identified. The NBU's initiatives to regulate the non-banking financial services market were considered.

Introduction

The current situation in the world indicates the need to increase attention and to improve the means of preventing and struggle with fraud in the field of financial services. The global picture of fraud in the field of financial services is quite disappointing: internal and external threats of fraud arise in the banking sector, in the field of non-bank financial institutions, in the field of insurance, in the field of non-cash circulation.

Fraud is threatening for individuals, businesses and the state as a whole, given that technological and information changes taking place in modern society create conditions for the emergence of new forms of crime and, accordingly, require new ways to struggle with it. The rise of fraud is increasingly related to the use of cyberspace; the transfer of physical assets and processes into the digital space within the implementation of «Industry 4.0» has expanded opportunities for businesses and organizations; active application and expansion of business contacts on the basis of the Internet platforms has introduced new priorities in the markets «business to consumer», «business to business», «business to government». At the same time, the typology of fraud and ways of inflicting financial and non-financial losses increased (for companies – the decrease of reputation, loss of trust of clients, business partners).

The coronavirus pandemic has caused serious economic recession in the world; due to the introduction of strict preventive measures by many countries to control the spread of the epidemic, it has become necessary to transfer the business activity of enterprises to on-line mode. The collapse of the economy led to rising unemployment, declining incomes and it led to the search for earnings and opportunities to pay off debts using online platforms. At the same time, there was a quick increase in the number of the Internet fraud and cybercrimes committed by those seeking to enrich themselves through the crisis.

This situation is fully inherent also for the Ukrainian society, so it is advisable to analyze the possible risks of fraud in financial services, taking into account the specifics of the crisis, and to identify sources of threats, and to understand the behavior to prevent fraud.

Part 1. Risks of fraud in the banking sector

Fraud related to the activities of banking institutions, both in quantitative and in value terms, are among the leading countries in the financial sector. According to research by analysts of the company «Bottomline Technologies», the results of which are presented in the report «UK Business Payments Barometer: Payments For a New Economy», in 2018, 56% of the UK companies were victims of banking fraud; no more than 75% of the total number of victims were able to recover lost funds only partially. A large number of respondents could not fully determine the amount of loss; 27% estimated their losses in the range of 10-50 thousand GBP, 9% – up to a quarter of a million, 2% – more than a million GBP.

Global study conducted from November 2018 to February 2019 in 43 banks (13 of them belonged to the countries of the Asia-Pacific region, 5 of them are in America, the location of 25 countries is in Europe, the Middle East and Africa) found that more than half of the banks located in different countries confirmed the increase in losses from fraud, and more than 60% – an increase in the number of frauds; while most of them managed to recover only a quarter of the loss [1].

Fraudulent actions in the banking sector are characterized by both external and internal nature. Typology of fraud in the banking sector is devoted to a number of studies based on the application of various criteria for the classification of fraud. The subjects who commit fraud, as a rule, include: bank employees; customers served by banks; joint fraudulent actions of employees and customers; fraudsters who do not belong to these categories and commit fraud alone and are members of criminal groups.

Kushnerov O.S. distinguishes four groups of fraudulent transactions related to the use of bank cards, deposit and credit services, as well as the implementation of settlement and cash services [8]. Shevchenko A.M. focuses on the most common abuses in the banking sector: intentional bankruptcy,

cash withdrawal, money laundering and withdrawal, direct embezzlement, other fraudulent actions of bank staff [14].

According to Kuznietsova N.V., persons committing fraudulent activities are divided into «domestic» fraudsters, professional fraudsters and borrowers who use the services of professional fraudsters; the author proposes the use of scoring models, which make it possible to cut off persons with intent to defraud at the stage of analysis of loan applications [7].

Melnyk S.S. provides a sufficiently capacious classification of fraud in relation to a commercial bank, using a number of classification features, which includes reasons for determination, the environment of manipulation, the degree of coverage, the scope, the direction of manipulation, the method of acquisition of financial resources, the volume of commitments, the direction of financial consequences and others [9].

Hrytsenko K.H. considers fraud by bank staff and proposed the use of economic and mathematical methods to establish fraudulent actions: qualitative, quantitative, using artificial intelligence and hybrid [4].

Cherniavskyi S.S. proposes the classification of crimes in the field of banking in terms of a criminal approach to their evaluation: depending on the nature of banking operations; features of the object of criminal actions; characteristics of persons committing crimes; technologies used in the process of organizing and committing criminal acts [12].

Analysis of the legal assessment of crimes committed in the banking sector is given in the study of Klochko A.M. The author distinguishes between crimes committed by bank employees, persons who are not bank employees, as well as organized groups [6].

According to research, banking institutions around the world see an increase in fraud schemes during the crisis, the intensification of cybercriminals and financial fraudsters. Although there is primarily an increase in the external risks of fraud, abuses involving bank staff remain significant, and the lack of available information is in many cases due to banks' reluctance to tarnish their reputations in the eyes of customers and business partners.

According to existing data, almost 90% of all criminal acts in the banking sector are committed with the participation of bank employees themselves. The way out of this situation is insurance against abuse of employees, which is very developed in foreign countries and, as a rule, is part of the Comprehensive Banking Insurance program. Banks in Ukraine do not show much desire yet to insure this type of risk and this is due to a number of reasons: the high cost of the franchise, the lower threshold of compensation (starting from 50-100 thousand USD), the need to attract a reinsurer with high financial capacity.

It should be noted that the European banks, in contrast to the Ukrainian ones, are characterized by a lower level of fraud by bank employees due to the interest of banks in disclosing such information, which prevents further

stay of a person with a negative reputation in the banking sector. Internal fraud in domestic banks in many cases is not accompanied by punishment, except for voluntary dismissal, which allows criminals to continue their abuse in other banks.

The most attractive area for abuse is retail lending, which is due to fewer opportunities to control the procedure of processing loans due to their larger number and smaller amounts compared to corporate lending. One of the ways of this kind of fraud is to issue a bank loan to a consumer without his or her knowledge using forged or stolen documents. Such a situation may arise in the case of signing additional credit agreements by the client without understanding their essence or providing extra copies of certified personal documents.

Quite common is the situation when customer funds for loan repayment are credited to other people's accounts or in case of loan repayment a very small amount that remained and has not been notified to the borrower over time due to the accrued penalty becomes large enough that the bank requires to pay.

Cases of fraud with deposits are not uncommon: when drawing up bank documents, they may indicate a smaller amount than actually paid; deposit funds can be credited to another account; an employee of the bank may offer higher interest on the deposit if the deposit will not be made through the cashier, which actually leads to the misappropriation of customer funds. In the process of settlement and cash service fraudulent actions can also be committed: issuance of counterfeit notes, withdrawal of notes in case the client receives a large amount, reduction of funds on the account as a result of writing them off without warning the account holder.

In recent years, and especially during the coronavirus pandemic, there has been a sharp increase in the number of external frauds, which include attacks on citizens' accounts through the misappropriation of personal data, cyberattacks, and fraud in the field of cardless transactions.

At the same time, in Ukraine, there is a decrease in losses from illegal use of payment cards. In 2019, based on information provided by banks, payment instrument holders and trade structures, the amount of losses due to abuse in the use of payment cards amounted to 0.0042% of the total amount of all transactions with it (for comparison, in 2018 this indicator had a level of 0.0092%, its value in 2017 was 0.0077%) [15].

According to the NBU the amount of criminal transactions per 1 million UAH of all executed expenditure transactions with the use of cards in 2019 amounted to 42 UAH and it was twice less than in 2018; the average value for one criminal operation was 2100 UAH (in 2018 – 2500 UAH). The number of cases of payment card fraud also decreased from 105.5 thousand in 2018 to 71.9 thousand in 2019.

Despite the positive trend in the use of payment cards, the main tool for this type of abuse is the Internet, which carries 58% of fraud, although in 2019 the

number of cases of fraud committed through the network also decreased almost twice and amounted to 41.4 thousand cases [15].

Despite this, the amount of funds stolen from the bank accounts of the Ukrainians in 2019 amounted to 362 million UAH, in 2018 – 245 million UAH. The most common schemes of payment fraud concerned obtaining fraudulently obtaining the details of cards, keys and passwords of access to the Internet banking from citizens themselves. According to the Ukrainian Interbank Association of Members of Payment Systems «EMA» the largest share of fraud in 2018-2019 (65%) was carried out using the Internet and social engineering (psychological impact on victims) [17].

The value of the estimated income of criminals increased from 245.81 million UAH, in 2018, to 361.99 million UAH, in 2019, including due to social engineering – from 240.92 million UAH up to 282.25 million UAH. Also the amount that fraudsters received for committing one abuse increased: on the Internet – from 85 UAH up to 336 UAH, using social engineering methods – from 2 333 UAH up to 3 400 UAH, as a result of SIM card replacement – from 3 620 UAH up to 6 200 UAH.

Attacks on ATMs (skimming, cash trapping, physical attacks) are not excluded from the arsenal of criminals: they make up about 24% of all fraudulent actions. In 2019, 80 cases of skimming (card cloning) were recorded – 22 less than in 2018 and 33 less than in 2017. The number of abuses with the use of cash trapping (blocking the process of withdrawing cash from an ATM) was 193 in 2019, which is 103 cases more than in the previous year. The number of ATM hacks has also increased to 77 (in 2018–2020). The largest number of break-ins was carried out using a gas explosion – 38, 13 – by breaking, 12 – by organizing an explosion, 7 – by stealing software and technology self-service complex.

In the context of the coronavirus pandemic, the number of cyber frauds increased. According to the cyber police, the number of phishing attacks has quickly increased taking into account a favorable environment due to panic and anxiety of people about coronavirus issues, the need to work remotely from home, to use video services.

Cybercrime is reviewed by world experts as a threat that may take the first place in the near future, even ahead of terrorism. Due to the actions of cybercriminals, the losses of the world economy each year amount to about 114 billion USD. The USA estimates its losses over the Internet at 400 billion USD, which is three times the annual cost of education.

Cybersecurity experts consider Ukraine as one of the centers of hacking, along with such countries as Russia, Brazil, and China; it is one of three leading countries of DDoS attacks (12% of the total number of attacks). In Ukraine, most cybercrime cases originate in its own territory, although when it comes to using fraudulent schemes to intrude on the system, distort information, spam or use software with criminal intent, the addresses of fraudsters can be in any other country.

Today, the most common type of cybercrime is phishing, as a result of which attackers extract confidential data: passwords, logins, information about personal accounts, the details of cardholders. There are various types of phishing: SMS-phishing (for example, notification of blocking a credit card by a bank with the condition of providing details for its unblocking); Internet phishing (creation of fake pages imitating the official pages of a bank, online store, etc.); vishing (receiving information about the card details by phone calls allegedly from bank officials).

According to Check Point experts who together with Dimensional Research conducted a survey among experts in the field of information technology and information security around the world, 71% of respondents recorded a quick increase in cyberattacks since the beginning of the pandemic; 55% identify phishing as the predominant threat; second place is given by 32% to fraudulent sites that offer advice on coronavirus; 28% focus on increasing the number of malware; 19% – on the growth of the number of extortionists [19].

In April 2020, Trend Micro Incorporated released data on the cyber threats that were most prevalent during the coronavirus pandemic: spam (65.7% of cyberattacks), malware (26.8% of cyberattacks), malware URLs and sites. The largest number of criminal files with words «covid» or «covid19» was found in the United States – 26.6%, France – 12.2%, Canada – 11.2% [20] (Figure 1).

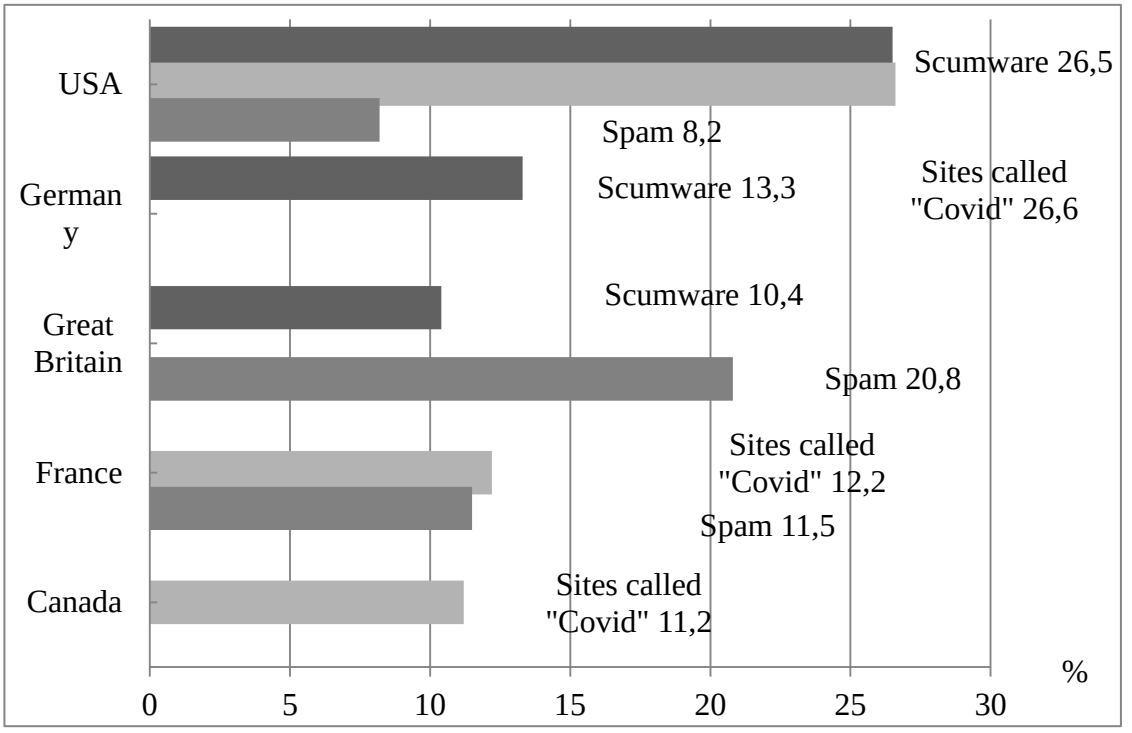

Figure 1. Types of cyberthreats during a pandemic

Source: built by the author according to the data [20]

Antivirus company Eset made a report in March 2020 on ways to enrich criminals in cyberspace. The most common way was to disseminate information ostensibly on behalf of the World Health Organization; the transition to malicious links ended with the theft of personal information and payment data.

In Ukraine, there is currently no complete information on cybercrime during the quarantine period, but according to information security experts, its number has increased sharply: each bank is the object of dozens and sometimes hundreds of cyberattacks, and this situation is not unique for banks of Ukraine, as well as banks in many countries. The lack of statistics is associated with reputational risks, which can increase sharply as a result of customers' doubts about the security of their funds in a particular bank. The problem is complicated by the lack of a single center in Ukraine, which would act as an accumulative structure for decision-making in the field of cybersecurity, harmonizing the actions of the State Special Communications Service, the Ministry of Digital Transformation, the National Security and Defense Council, Cyber Department of Security Service of Ukraine.

Table 1 shows a generalized classification of fraud in relation to customers and employees of banking institutions and ways to prevent them.

Payment card fraud and other forms of abuse with the use of online banking are not ignored in Ukraine and in the European countries. In 2018, the NBU of Ukraine developed «Recommendations for Reducing the Risk of Fraudulent Transactions», which considered the following types of fraud: fraud in the case of using an ATM; fraud in the Internet space; fraud using terminals; fraud that occurs during the implementation of remote maintenance; social engineering. This document provides recommendations for preventing abuse with use of payment cards and security in the case of banks using remote customer service [16].

The European Union has also taken a number of steps to reduce the threat of banking fraud. It especially concerns the Directive adopted in 2017, which has outlined a number of key provisions on combating fraud and counterfeiting non-cash payment instruments. Clause 2.3 of paragraph 2 of this Directive is of particular importance, which substantiates the cross-border nature of abuses involving non-cash payments not only in the EU member states but also those that form a globalized community [18].

Particular emphasis is placed on the need for concerted action by countries seeking to ensure a high level of security in the field of online payments to prevent such phenomenon as, for example, skimming payment card data in the EU country and on the basis of data obtained forgery of the card with subsequent misappropriation of funds outside the country.

Table 1

Classification of fraud and methods of prevention

No.	Type of fraud	Ways to prevent
1	2	3
Internal fraud		
1.	Credit	From customers Preliminary acquaintance with credit conditions Careful study of credit documentation Requirement to receive a payment document in case of loan repayment and a certificate of its full repayment On the part of bank employees Application of modern methods of customer identification Credit history analysis of clients Study of the financial condition of borrowers
2.	Deposit	From customers Control of payment documents on deposited funds Adherence to the official procedures for making a deposit Constant control of own deposit account Storage of payment documents for at least three years
3.	At settlement and cash operations	From customers Control of the issued amount in the presence of the cashier Checking the status of issued notes in the presence of the cashier Control of issued payment documents
External fraud		
4.	Cybercrime	From banking institutions Organizational, legal, engineering and technical means of cyber defense Operating model optimization Multifactor authentication Physical biometrics From customers Use of licensed software Constantly updating the operating system Application of anti-virus programs Use of official and well-known sites Backup files with important information Application of limits on transactions when using payment cards
5.	Phishing	From customers Secure storage and non-disclosure of card PINs, CVC2 / CVV2 codes, data for Internet banking login, one-time passwords for additional authentication Creating strong passwords Caution in cases of requesting card details outsiders Ignore suspicious emails and links
6.	Social engineering	From customers Do not answer phone calls that cause doubts Do not trust calls allegedly from bank representatives who try to request personal information (neither representatives of the NBU nor any other bank have the need and authority to make such calls) Use SMS-informing services Do not use your financial number on social networks Do not send a copy of your passport or ID code over the Internet Constantly increase the level of your financial literacy

Source: compiled by the author

The EU initiatives to struggle international crime in the field of non-cash payments are reflected in the EU policy cycle EMPACT and it has been introduced in 2010 and extended for the period 2018-2021. The essence of the political cycle is to identify criminals who commit fraud, through the cooperation of the EU institutions with law enforcement agencies and other structures that have certain powers and interests.

Part 2. Risks of fraud in the field of non-banking financial services

Non-bank financial institutions play an important role in meeting the needs of consumers, their successful operation is one of the factors ensuring economic stability of the country. From July 1, 2020, in accordance with the so-called «split» law the NBU becomes the regulator of the non-banking financial services market, which employs credit unions, insurance companies, pawnshops, and financial companies.

Lending in the non-banking financial market is characterized by a steady upward trend today. The largest share of loans issued falls on financial companies: the amount of loans issued in 2019 amounted to 79.2 billion UAH, in 2018 this figure was 51.9 billion UAH. Loans issued by credit unions in 2018 reached 16.4 billion UAH, in 2019 – 18.2 billion UAH. The volume of lending by pawnshops in 2018 amounted to 2.3 billion UAH, in 2019 – 2.7 billion UAH [21].

The ratio of lending by financial companies of two categories of borrowers – individuals and legal entities – has changed in the new loan portfolio: more than half of loans to individuals and individual entrepreneurs (at the end of 2019 loans to legal entities prevailed – about 78% of the total volume).

A high share of loans is carried out online. In 2019, the share of remotely concluded credit agreements was distributed depending on the term of validity as follows: 92.33% – credit agreements with a term of up to 30 days; 5.28% – with a validity period from 30 to 90 days; 1.28% – from 90 days to 1 year; 1.1% – more than 1 year.

For consumers – individuals, it is characterized by demand mainly for microloans (the average loan amount in 2019 was 3711 UAH), which do not require collateral; legal entities apply for loans of a significant amount, which can reach hundreds of thousands of dollars and require collateral.

Although, business loans can be quite expensive compared to bank loans and attractive feature is the short terms of the decision to grant a loan and the lack of requirements for the financial condition of the borrower. This explains the possibility of the risk of fraud on the part of the borrower, whose credit history is usually not studied, as well as not established its actual solvency.

As the real situation shows, financial companies in most cases ignore the provisions of the guidelines developed by the National Commission for State Regulation of Financial Services Markets (No. 1033 dated June 06, 2019) and related to electronic credit agreements in the conditions of using information and telecommunication systems. The proposed measures included applying to

the credit bureaus for information about the borrower, the introduction of a better procedure for identifying customers using modern IT solutions.

The risks of fraud in the non-banking financial sector may be related to the wrongful acts of the financial companies themselves, which do not provide borrowers with complete information on credit terms; this is especially true of loan repayment terms and penalties that will be applied in case of violation. As a result, the advertised interest-free loan or with a minimum annual interest rate can be converted into a loan of 100% or 200% per year.

There are many cases of concluding a loan agreement on the condition of payment of certain preliminary installments (in many cases monthly), after which the loan is postponed, which can last more than one month; while the continuation of the payment of contributions remains mandatory, otherwise the loan agreement may be terminated.

The new regulatory model set out by the NBU in the White Paper «Future Regulation of the Lending Market by Financial Companies», which concerns the further activities of financial lending companies, provides a new approach to licensing financial companies and applying a number of criteria in monitoring the NBU's market behavior: protection of clients' rights, including compliance with service delivery standards and requirements for their advertising; ensuring transparency and disclosure of information; ensuring the impeccable business reputation of owners and managers; counteraction to anticompetitive activity; counteraction to abuse and illegal activity; control over the implementation of the CPO authority» [21].

The NBU published a number of White Papers, which set out the intentions to regulate the activities of other participants in the market of non-banking financial services: financial companies, credit unions, pawnshops, companies operating in the insurance market, factoring market and non-bank leasing [22-26].

The lack of norms for full-fledged regulation of credit unions by National Commission for State Regulation of Financial Services Markets led to a basis for fraudulent actions by employees of these structures. Despite the fact that for the period 2015-2019, 230 credit unions have been excluded from the State Register of Financial Institutions and today the number of officially registered is 337, only 241 credit unions reported to the State Regulation of Financial Services Markets on their activities [22].

The most common cases of fraud in credit unions are related to:

– criminal actions of staff leading to misappropriation of credit union property (falsified credit agreements executed without the knowledge of citizens; seizure of funds placed on deposit accounts of credit union members; use of fictitious persons for loans);

– illegal activity without state registration as a financial institution or continuation of operation in case of removal from the registration list and liquidation of the license;

– fraud on the part of depositors – obtaining loans on false documents;

– use of «financial pyramids» with the involvement of members of the credit union on the condition of receiving remuneration in case of increase in the number of members of the organization.

The «Financial pyramid» is a phenomenon that periodically occurs not only in credit unions, but also in all areas of the financial services market. The creators of the «financial pyramids» promise trusting citizens high incomes, but they can only arise from the redistribution of funds of many people in favor of a small number of people. In many cases, fraudsters are the initiators of the pyramids after receiving the money disappear without a trace; even if the «financial pyramid» has worked, its lifespan is three to nine months, after which it falls apart.

A new «financial pyramid» with all the signs of fraud has recently appeared on the Ukrainian market – the Exlimited project; the organizers of the project promise to receive a quick income in the case of investing funds in hryvnia or cryptocurrencies with a daily profit of 0.4% to 1.5%. The project's website links to a questionable license and 28 allegedly implemented international projects without giving their names. The fraudulent nature of this project is confirmed by the fact that the legislation of Ukraine gives the right to attract funds from the population and pay interest only to banks and credit unions registered in Ukraine.

An important area of the market of non-banking financial services is insurance, currently represented in Ukraine by 225 insurance companies, 22 of which – IC «life», 203 – IC «non-life». In comparison with the insurance markets of foreign countries in terms of assets and volume of consumed insurance services, the domestic insurance market is at an insufficient level of development. The value of the penetration of insurance services in Ukraine is 1.4%, while its average value reaches 5% in Europe, and 6.1% in the world.

Obstacles to the growth of the insurance market are, first of all, lack of trust in insurance companies due to lack of transparency in their activities, inefficient consumer protection system, widespread violations of insurance conditions by insurance companies, unreliability and low level of professionalism of insurance intermediaries.

Insurance fraud can be organized by both insurers and policyholders, and in some cases by agreement of both parties. Offenses by insurance companies include:

– violation of licensing conditions of activity (for example, implementation of those types of insurance activity for which there are no licenses);

– deceptive actions of the insurer during the conclusion of the insurance contract, which leads to the transfer of responsibility to the insured in the case of an insured event;

– appropriation by employees of the insurance company of insurance premiums of policyholders.

Insurers, in turn, can commit fraudulent actions by: artificially increasing the sum insured on the basis of false information provided; concluding insurance contracts simultaneously in several insurance companies without notifying them, and in case of an insured situation – receiving full insurance indemnity from them; committing malicious acts leading to the occurrence of an insured event to receive insurance payments.

The NBU's initiative to regulate the insurance services market to increase the reliability of the insurance sector, first of all to form a legal framework that will help to protect the rights of policyholders, to apply constant monitoring of the risk management system and compliance of management with qualification requirements.

Conclusions

Fraud should be understood as illegal actions aimed at misappropriating property or financial resources through fraud or abuse of trust. The implementation of fraudulent actions in the field of financial services not only leads to significant material damage to the subjects involved in financial relations and also damages their reputation, image, relationships with business partners. The development of digital technologies creates the basis for the intensification of fraud, while opening opportunities for the use of innovative methods and tools to prevent and eliminate fraud.

The warning of internal fraud in banking and non-banking financial institutions should be an effective mechanism for prevention and struggle with fraud, based on effective legal, organizational, software and technical methods of protection. The basis for the implementation of this mechanism should be the corporate culture of the organization, which would provide for the presence of high moral and ethical standards of behavior of employees, and especially senior management.

With regard to external fraud, which is carried out primarily using cyberspace, it is necessary to develop cyber insurance in Ukraine, which would insure the following cyber risks: risks of financial loss due to the loss or violation of the integrity of financial information as a result of DDoS-attack; risks of financial loss due to interference with the operation of computer systems; risks of financial loss due to virus attacks on the computer system or in cases of damage to software by attackers.

The problem of fighting corruption remains urgent, which is not only a significant factor in influencing the risks of financial fraud, but also one of the main political, economic and social problems. Particular attention should be paid to the phenomenon of White-Collar Crime, which is relatively new for Ukraine and has been known for a long time in developed countries.

References:

1. Hlobalne doslidzhennia z pytan shakhraistva u bankivskii sferi. KPMG (2019) [Global study on banking fraud. KPMG]. Available at: https://home.kpmg/ua/uk/home/insights/2019/12/fraud-banking.html (accessed 15 June 2020).

2. Baranovsky O.I. (2014) *Filosofiia bezpeky: monohrafiia* [Philosophy of security: monograph]. Kyiv : UBS NBU, 715 p. (in Ukrainian)

3. Bidnyak H. S. (2019) *Teoriia i praktyka vykorystannia spetsialnykh znan pry rozsliduvanni shakhraistv : monohrafia* [Theory and practice of using special knowledge in the investigation of fraud: a monograph] Dnipro: Dnipro. state University of Internal Affairs affairs, 152 p. (in Ukrainian)

4. Gritsenko K.G. (2019) Analiz metodiv vyiavlennia shakhraistv u bankakh, shcho zdiisniuiutsia personalom banku [Analysis of methods of detecting fraud in banks by bank staff]. *Matematychni metody, modeli ta informatsiyni tekhnolohiyi v ekonomitsi* [Mathematical methods, models and information technologies in economics], vol. 34, pp. 333-337.

5. Gladkikh D.M. (2019) *Zabezpechennia bankivskoi bezpeky Ukrainy v umovakh rozvytku informatsiinoi ekonomiky: desert. na zdob. nauk. st.. dokt. ekon. nauk za spetsialnistiu 21.04.01 – ekonomichna bezpeka derzhavy (ekonomichni nauky).* [Ensuring banking security of Ukraine in the development of information economy: dessert. on zdob. Science. st. dr. econ. Sciences, specialty 21.04.01 – economic security of the state (economic sciences)]. Kyiv: National Institute for Strategic Studies, 531 p.

6. Klochko A.M. (2014) Zlochyny u sferi bankivskoi diialnosti[Crimes in the field of banking]. *Pravovyy visnyk Ukrayins'koyi akademiyi bankivs'koyi spravy* [Legal Bulletin of the Ukrainian Academy of Banking], no. 1(10), pp. 68-71.

7. Kuznetsova N.V. (2017) Skorynhovi tekhnolohii otsiniuvannia ryzykiv shakhraistva v bankivskii diialnosti) [Scoring technologies for assessing the risks of fraud in banking]. *Informatsionnyye tekhnologii i bezopasnost'* [Information Technology and Security], pp. 43-47.

8. Kushnerev O.S. (2019) Tendentsii shakhraiskykh operatsii na bankivskomu rynku ta mozhlyvosti protydii [Trends in fraudulent transactions in the banking market and opportunities for counteraction]. *Innovatsiyna ekonomika* [Innovative economy], no. 3-4 (79), pp. 180-188.

9. Melnik S.S. (2017) Klasyfikatsiia finansovoho shakhraistva v komertsiinomu banku [Classification of financial fraud in a commercial bank]. *Naukovyy visnyk Khersons'koho derzhavnoho universytetu* [Scientific Bulletin of Kherson State University], vol. 23, pp. 89-92.

10. Oliynychuk O. (2017) Bankivski kartky yak obiekt shakhraistva: stan i protydiia yavyshchu (2017) [Bank cards as an object of fraud: the state and counteraction to the phenomenon]. *Aktual'ni problemy pravoznavstva* [Actual problems of jurisprudence], vol. 1(9), pp. 91-94.

11. Sokrovolska N.Ya., Hamiga Yu.A. (2018) Protydiia finansovomu shakhraistvu u vitchyznianykh orhanizatsiiakh [Counteraction to financial fraud in domestic organizations]. *Naukovyy visnyk Uzhhorods'koho natsional'noho universytetu* [Scientific Bulletin of Uzhhorod National University], pp.73-76.

12. Chernyavsky S.S. (2010) *Finansove shakhraistvo: metodolohichni zasady rozsliduvannia [Tekst]*: [monohrafiia] [Financial fraud: methodological principles of investigation]. Kyiv : Hi-TechPress, 624 p. (in Ukrainian)

13. Chunytska I.I. (2017) Zakhody zapobihannia finansovomu shakhraistvu ta lehalizatsiia koshtiv, zaroblenykh zlochynnym shliakhom [Measures to prevent financial fraud and money laundering]. *Problemy ekonomiky* [Problems of the economy], vol. 2, pp. 282-291.

14. Shevchenko A.M. (2015) Zlovzhyvannia ta makhinatsii na rynku finansovykh posluh: metody borotby, zasoby protydii [Abuse and fraud in the financial services market: methods of struggle, means of counteraction]. *Hlobal'ni ta natsional'ni problemy ekonomiky* [Global and national economic problems], vol. 7, pp. 767-771.

15. NBU zafiksuvav zmenshennia kilkosti shakhraistv iz platizhnymy kartkamy (2020) [The NBU has recorded a decrease in the number of payment card fraud]. Available at: https://www.ukrinform.ua/rubric-economy/2891790-nbu-zafiksuvav-zmensenna-kilkosti-sahrajstv-iz-platiznimi-kartkami.html (accessed 16 June 2020).

16. Rekomendatsii dlia znyzhennia ryzyku shakhraiskykh operatsii: NBU. Lyst vid 04.07.2018 No. 57-0009/36366 (2018) [Recommendations for reducing the risk of fraud: NBU. Letter dated 04.07.2018 No. 57-0009/36366]. Available at: https://zakon.rada.gov.ua/laws/show/ v3636500-18#Text (accessed 17 June 2020).

17.Tartasyuk S.(2020) 13 shakhraiskykh skhem, yaki dozvolyly potsupyty v ukraintsiv 362 miliony [13 fraudulent schemes that allowed Ukrainians to steal 362 million]. Available at: https://minfin.com.ua/ua/2020/02/14/40729350/ (accessed 17 June 2020).

18. Dyrektyva Yevropeiskoho Parlamentu ta Rady «Pro borotbu z shakhraistvom ta pidrobkoiu bezghotivkovykh platizhnykh zasobiv ta zaminoiu Ramkovoho rishennia Rady 2001/413/JHA» 2017 roku (2017) [Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413 / JHA 2017]. Available at: https://zakon.rada.gov.ua (accessed 17 June 2020).

19. Nefedova M. (2020) Check Point: pandemyia koronavyrusa sozdala ydealnye uslovyia dlia kiberatak [Check Point: The coronavirus pandemic created ideal conditions for cyberattacks]. Available at: https://xakep.ru/2020/04/08/corona-infosec-problems/ (accessed 18 June 2020).

20. Kak kyberprestupnyky yspolzuiut pandemyiu koronavyrusa (2020) [How cybercriminals use the coronavirus pandemic] ComNews. Available at: https://www.comnews.ru/content/205449/2020-04-07/2020-w15/kak-kiberprestupniki-ispolzuyut-pandemiyu-koronavirusa (accessed 19 June 2020).

21. Bila knyha. Maibutnie rehuliuvannia rynku kredytuvannia finansovymy kompaniiamy: NBU (2020) [White book. Future regulation of the lending market by financial companies]. Available at: https://bank.gov.ua/admin_uploads/article/ White_paper_credit_fincompanies_2020 (accessed 26 June 2020) (accessed 26 June 2020).

22. Bila knyha. Maibutnie rehuliuvannia kredytnykh spilok. NBU (2020) [White book. Future regulation of credit unions. NBU] Available at: https://bank.gov.ua/ua/news/ all/bila-kniga-maybutnye-regulyuvannya-kreditnih-spilok?fbclid=IwAR0dnYLy7IZ9c65V9_ A7uQUxKzRY6wN3z80seDvQXadGwydhCL6xCwnw0QQ (accessed 26 June 2020).

23. Bila knyha. Maibutnie rehuliuvannia diialnosti lombardiv. NBU (2020) [White book. Future regulation of pawnshops. NBU]. Available at: https://bank.gov.ua/ ua/news/all/bila-kniga-maybutnye-regulyuvannya-diyalnosti-lombardiv (accessed 26 June 2020).

24. Bila knyha. Maibutnie rehuliuvannia rynku strakhuvannia v Ukraini. NBU (2020) [White book. Future regulation of the insurance market in Ukraine. NBU]. Available at: https://bank.gov.ua/ua/news/all/bila-kniga-maybutnye-regulyuvannya-rinku-strahuvannya (accessed 27 June 2020).

25. Bila knyha. Maibutnie rehuliuvannia rynku faktorynhu. NBU (2020) [White book. Future regulation of the factoring market. NBU]. Available at: https://bank.gov.ua/ ua/news/all/bila-kniga-maybutnye-regulyuvannya-rinku-faktoringu (accessed 28 June 2020).

26. Bila knyha. Maibutnie rehuliuvannia nebankivskoho lizynhu. NBU (2020)[White book. Future regulation of non-bank leasing. NBU]. Available at: https://bank.gov.ua/ ua/news/all/bila-kniga-maybutnye-regulyuvannya-nebankivskogo-lizingu (accessed 28 June 2020).