Internal Audit of Cybercrimes in Information Technologies of Enterprises Accounting

Ruslan Dutchak[1*], *Olha* Kondratiuk[1], *Olena* Rudenko[1], *Andrii* Shaikan[1], and *Elizaveta* Shubenko[1]

[1]State University of Economics and Technology, Department of Accounting and Taxation, Kryvyi Rih 50000, Ukraine

Abstract. The article is devoted to the problem's research of cybercrimes at the enterprise and the efficient methods of its solvation. The main trends of the cybercrime's development in the national and the global scope are defined. The analysis of the normative-legal acts on cybercrime is made. The main risks of cyberthreats before the illegal alienation of the enterprise assets are determined. The specific peculiarities of cybercrimes in the information technologies of enterprises accounting are revealed, the main ones of which are: cyberspace, the anonymity, harmful program products, the electronic (digital) track. The practicability of the internal audit use for the system opposition to cybercrimes at the enterprise is grounded. The main competences of the internal audit employees for the efficient work in the cyberspace of the enterprise are formulated. The recommendations, concerning rules of behavior for the employees in the cyberspace, are elaborated. The method of the internal audit is improved by the additional involvement of the modern ways of watching the electronic (digital) tracks of ill-intentioned persons in the cyberspace of the enterprise. The order of the juridical registration, concerning the methods use of watching the electronic (digital) track in practice of the internal audit at theenterprise, is offered.

1 Introduction

The rapid development of information technologies and their spreading practically in all spheres of the social-economic life of any country have become the main trend of the humankind development at the beginning of XXI century. The mentioned development caused the digital transformation of the processes, connected with collection, storage, processing and widening of information. The following advantages of digitalization have become undeniable for business: the increase of speed and transparency of business-processes; the growth of labor productivity; the reduction of costs on work with information; the transition from the paper documents to the electronic ones; processing of the data great volume; synchronization of information flows; acceleration of the managerial decisions-taking and others. In spite of the advantages, the new technologies are used to commit crimes, to inflame hatred, to falsify information and to interfere in private life [1]. According to the data of the World Economic Forum report, the cyberattacks belong to the five main dangers, threatening to the mankind so, as the natural disasters and the climate changes [2]. The cybercrimes, which main purpose is the expropriation of property (including the robbery of assets from the bank accounts) from their owners, are of special danger. According to the investigations data of McAfee and the Center of Strategic and International Research (CSIS), the world economy has lost more than 1 trillion of USA dollars in 2020 due to the hacker attacks [3].

The information technologies of enterprises accounting are significantly popular among the cybercriminals, namely: "SAP R3", "BAS", "OneBox", "MS Dynamics", "Perfectum", "IT-Enterprise", "1 S: Enterprise 8", "Parus 8" and the programs on the distant control of the enterprises bank account. The reason of such liking is the concentration of information on the available assets of the enterprise in the accounting, the possibility of manipulations with the accounting documents for their alienation, the distant access of employees to the accounting programs (especially actual in the period of COVID-19 pandemic) and others.

The objective necessity in protection of its assets appears for the enterprise's management with the purpose of avoiding the losses from cybercriminals. The most practicable method of such protection is the organization of the internal audit's service operation in the structure of the enterprise. However, the specificity of the struggle with the principally new cybercriminality requires the definite innovations for the traditional methods of the internal audit, which will correspond to the modern provocations of swindling in the cyberspace of the enterprise.

The problem of the internal audit is presented in the modern scientific literature by the wide interest of scientists. The analysis of the latest sources and publications on this problem allow select the main works results of the leading scientists. Thus, P. Rosati, F. Gogolin та T. Lynn [4] confirm, that the incidents with the cybersecurity affect the quality reduction of the financial reporting's audit. G. D'Onza, G. Sarens and S. DeSimone [5] determined, that the management system's maturity of risks depended on the development of the internal audit functions. J. Christopher [6] researched the negative consequences for the functioning

*Corresponding author: dutchakrr@ukr.net

of the internal audit from its role's manipulation by the enterprise's Board and higher leadership. M. N. Ivanova and A. Prencipe [7] examine the influence's (swindling's) components of the companies' higher administration on the audit remuneration. JR. Cohen, JR. Joe, JC. Thibodeau and GM. Trompeter [8] reveal the problem essence of the internal control, according to the audits of the financial reporting, being the subject of the intensive learning by the Council on Supervision of Public Company Accounting. N. Betti and G. Sarens [9] made the analysis of the internal audit's function development in the digitalized business environment. The obtained analysis showed, that the digitalized business environment influenced the functions of the internal audit from the three aspects: 1) the flexibility of the internal audit planning and the necessary knowledge will increase, but the risks of the information technologies will gain the great importance, especially the threats of cybersecurity; 2) the higher demand on the consultation measures, being performed by the internal auditors; 3) the digitalization modifies the work practice of the internal auditors in their everyday tasks. The new technologies, such as the tools of the data analysis, are gradually introduced into the departments of the internal audit, but the digital skills are considered to be the important asset. Y. Chen, B. Lin, LZ. Lu and GG. Zhou [10] proved the existence of the quality influence of the internal audit functions on the efficiency increase of the firm operation. The authors demonstrate that the competence of the internal audit makes the operational efficiency of the firm better, but the interrelation between the independence of the internal audit and the operational efficiency of the firm is insignificant. D. Weekes-Marshall [11] investigated the role of the internal audit in the process of risks management of the countries, being developed. T. Bondarenko, R. Dutchak, O. Kondratiuk, O. Rudenko, A. Shaikan and E. Shubenko [12] grounded the perspective reality of the internal audit for the solvation of conflicts in accounting of the enterprise with the help of the tools of the artificial intellect (artificial neuron networks and machine training). Yu. M. Popivnyak [13] revealed the identification methods of cyberthreats in the sphere of the accounting information's use and defined the means of its protection from stealing, damaging or loss in the cyberspace. L. P. Polovenko with S.V. Merinova [14] analyzed the instruments of the social character and offered the operating mechanisms, giving the opportunity to watch and to reveal the indications of the social engineering operatively at the early stages, warning of cyberthreats at the enterprise and opposing to the social hackering. L. Smidt, A. Ahmi, L. Steenkamp, D. P. and D. Lubbe [15] made the estimation of the generalized software's maturity level for the fulfillment of the internal audit functions. They determined that the internal audit in the whole world is still at the relatively low level of development, in spite of the intensified introduction of information technologies and the generation of the great data in the organizations.

The conducted analysis allows come to the conclusion, that the problem of the internal audit of cybercrimes in the information technologies of enterprises accounting has no any system research. Some fragments investigations of the presented topic are met in the scientific literature: the internal audit, cybersecurity, information technologies and others. The traditional methods of the internal audit do not correspond to the modern specificity of cybercrimes. That's why the absence of the internal audit's system approach to overcome the problem of cybercrimes at the enterprise is left to be the unsolved part of the lined problem.

The aim of the presented article is to research the nature of the cybercrime phenomenon in information technologies of accounting and to elaborate the theoretical-methodic principles of the internal audit for the improvement of enterprises cybersecurity.

In order to achieve the set aim, the methods of the research, which basis is the dialectical method of cognition (knowledge), is used in the article. At the same time, the following scientific methods are additionally used in the research, namely: the historical one – at studying the trends of cybercriminality; the analysis – at the research of cybercrime components, information technologies of accounting and the process of the internal audit; the synthesis - at studying the indications and the ways of cybercrime at the enterprise, new competences of the employees and new methods of the internal audit; the abstracting – at the formation of the internal audit's new tasks; the induction – at the influence's definition of some cyberthreats on the general level of the enterprise's cybersecurity; the deduction – at the research of connection between the complex of the internal audit measures with the demonstrations of cybercriminality; the explanation – at the revealing of the cybercrime essence in information technologies of accounting; the classification – at the types' definition of the fixation methods (programs) of electronic (digital) tracks; the systematization – at the regulation of the enterprise's cybersecurity components; the concretization – at the determination of the cybercrime's commitment methods; the generalization – at the formation of documents for the juridical fixation of the behavior rules for the personnel in the cyberspace of the enterprise and the fixation methods use of the electronic (digital) tracks in practice of the enterprise's internal audit.

2 Presentation of the main research material

The auditor company "PricewaterhouseCoopers" published the report on "World Research of Economic Crimes and Swindling of 2020: Questioning Results of Ukrainian Companies" in 2020. According to the data of this report, it's determined that 51% of the Ukrainian organizations had suffered from the swindling cases during the last 24 months. This indicator is higher than the average one in the world (47%) and it grew, compared with 48% in 2018. More than 1/3 of the respondents in Ukraine have suffered from 2-5 incidents of swindling for the last 24 months. The main subjects of swindling essentially in the Ukrainian organizations have become: the employee of the organization – 25%,

the third side – 41%, the conspiracy between the employee and the third side – 25%. The Ukrainian respondents answered the question: "What was the approximate sum of your organization's direct losses from swindling during the last 24 months?" in the following way: 38% - less than 50 000 USA dollars, 13% - 50 000 - < 100 000 USA dollars, 13% - 100 000 - < 1 mln.USA dollars and 9% - 1 mln.USA dollars or more. However, only 59% of the Ukrainian organizations made the investigation of their worst case of swindling.

According to the data of the conducted research by "PricewaterhouseCoopers", cybercrimes occupy the fourth place among the TOP-5 ones from the most widely-spread types of economic crimes: 31% of the organizations in Ukraine suffered from them; 16% of the Ukrainian respondents are not only waiting for their cyberattacks at their organizations in the next two years, but they are convinced that the cyberattacks will be the most significant for their organization from the view-point of financial losses or the other consequences. Besides, the most part of the organizations in Ukraine is not ready enough for cyberattacks, only every third part of organizations in Ukraine has the program of cybersecurity [16].

The Article 8 of the Convention on Cybercriminality from 23.11.2001, which was ratified with the warnings and the statements by the Law of Ukraine "On Ratification of Convention on Cybercriminality" from 07.09.2005 № 2824-IV foresees that the criminal responsibility in relation to the internal legislation of the state is established for the premeditated committal, without any right for it, of the actions, resulting in the property loss of the other person by the following:

a) any introduction, change, destruction or concealment of computer data,

b) any interference into the functioning of the computer system,

gaining the economic advantages for themselves or another person, without any right for it, with the swindling or unfair purpose.

According to p. 8 of the Art.1 of the Law of Ukraine "On Main Principles of Cyber-Security Ensuring in Ukraine" from 5.10.2017 № 2163-VIII, the cybercrime (computer crime) – is the socially dangerous guilty action in the cyberspace and/or with its use, the responsibility for which is foreseen by the Law of Ukraine on Criminal Responsibility and/or which is recognized to be the crime by the international treaties of Ukraine.

The Criminal Code of Ukraine from 5.04.2001 № 2341-III (further on - CCU) determined the list of the main cybercrimes, for which the punishment is foreseen, namely:

violation of the copyright and adjoining rights (art. 176 of CCU);

taking possession of the unfamiliar property or acquiring the right for the property by the deception or the trust abuse (art. 190 of CCU);

illegal actions with the documents for remittance, payment cards and the other means of access to the bank accounts, electronic money, equipment for its production (art. 200 of CCU);

illegal use of the brand for the goods and services, the firm name, the qualified indication of the product's origin (art. 229 of CCU);

non-sanctioned interference into the operation of the electronic-computing machines (computers), the automation systems, computer networks or the systems of the electric connection (art. 361 of CCU).

Thus, you should understand that, according to art. 176 of CCU, art. 190 of CCU, art. 200 of CCU, art. 229 of CCU or art. 361 of CCU, the cybercrime is any crime, taking place with the help of the computer engineering, information technologies, computer systems, the compatible (united) communication systems and the Internet system.

According to the data of the General Public Prosecutor's Office of Ukraine, being reflected in the annual reports ("United Report on Criminal Offences") for the period of 2016-2020 [17], the number of the crimes, being committed in the cyberspace of Ukraine, is equal to the following (Table 1):

Table 1. Registered Number of Cybercrimes in Ukraine during 2016 - 2020

CCU Articles	Number of Crimes				
	2016	**2017**	**2018**	**2019**	**2020**
art. 176	157	95	126	148	118
art. 190	46019	37014	33290	32358	26830
art. 200	176	390	609	711	724
art. 229	168	121	111	62	123
art. 361	865	2573	2301	2204	2498

The data, presented in the Table 1, demonstrate the scope of the cybercrime phenomenon in the social-economic life of Ukraine. The mentioned data don't allow separate the exact indicator of cybercriminality in the very information technologies of the enterprise's accounting. The reason – the methods of filling in the mentioned report don't foresee the analytical criterion "cybercrimes at enterprises". However, the data in the Table 1 characterize successfully the environment, in which the enterprise functions and its employees live, namely:

- traditionally high scope of swindling quantity;
- the rapid quantity growth of the non-sanctioned interference into operation of the electronic-computing machines (computers) and the illegal actions with the documents for the remittance, payment cards and the other means of access to the bank accounts;
- the periodic activity of the copyright violation and the illegal use of the brand for the goods and services, the firm name.

Ukraine took the 25-th place among 160 countries in the National Cyber-Security Index (NCSI) in 2020 with the indicator of 68,83 (68,83%). The presented indicator demonstrates the level of Ukraine's readiness to prevent the cyberthreats and to control the cyber-incidents. At the same time, the digital development level (DDL) of Ukraine in 2020 was equal to 58,1 (58,1%). The

difference between the estimation mark of NCSI (68,83) and DDL (58,1) is equal to 10,73. The positive result shows that the development of cybersecurity in Ukraine during 2020 anticipates its digital development by 10,73%. The countries-leaders in the National Index of Cybersecurity (NCSI), where the development of cybersecurity anticipates its digital development, are the following: Greece (NCSI – 96,1, DDL – 65,44, the difference – 30,66), the Czech Republic (NCSI – 92,21, DDL – 69,37, the difference – 22,84), Estonia (NCSI – 90,91, DDL – 79,27, the difference – 11,64), Lithuania (NCSI – 88,31, DDL – 70,95, the difference – 17,36), Spain (NCSI – 88,31, DDL – 73,24, the difference – 15,07). It's reasonably to indicate separately the countries, where the digital society is more developed than the national zone of cybersecurity, namely: Denmark (NCSI – 81,82, DDL – 83,55, the difference – (-1,73)), the Netherlands (NCSI – 81,82, DDL – 83,88, the difference – (-2,06)), Germany (NCSI – 80,52, DDL – 81,95, the difference – (-1,43)), Singapore (NCSI – 80,52, DDL – 83,11, the difference – (-2,59)), the USA (NCSI – 79,22, DDL – 82,33, the difference – (-3,11)), Great Britain (NCSI – 77,79, DDL – 83,96, the difference – (-6,04)), Switzerland (NCSI – 76,62, DDL – 85,13, the difference – (-8,51)) [18].

Ukraine took the 25-th place in the world (from 30 countries), the 10-th place among the European countries and the 3-rd one in the post-Soviet space in the rating of the National Cyber-Power Index (NCSI) for 2020. According to the estimation of the Belfer Center of Science and International Relations, the most all-embracing cyber-powers among the world countries (TOP-10) had: the USA, China, Great Britain, Russia, the Netherlands, France, Germany, Canada, Japan and Australia [19].

According to the information on the revealed cybercrimes on the territory of Ukraine in 2020, being located on the official web-site of the Cyberpolice Department of the Ukraine National Police [20], the most typical methods of cybercrimes realization in the sphere of information technologies of enterprises accounting are the following:

1) the ill-intentioned people ring up to enterprises and pretend themselves as the employees of the bank's IT-support. They try to convince the enterprise's accountant-cashier to realize some "testing" operations as if they check the payment system of the bank. They made the illegal remittances of money to the accounts, being controlled by them, as if they realized "the testing of the payment system";

2) the use of the harmful software ("virus") in order to receive the distant access to the accountant's computer and the access keys to the program of the remote control of the enterprise's current account. After that the ill-intentioned person receives the complete access to the current account of the enterprise and realizes the money remittance to the private accounts already on behalf of his/her name;

3) the evil-minded people leave the flash drives (as a rule, of the famous brands with the high price) or the CD-disk with the harmful software ("virus") in the accountant's working place intentionally, after what the accountant's curiosity makes him/her to put such an information bearer into the computer (to check the information it contains) – and realizes the non-sanctioned access to the accountant's computer and its programs in such a very way;

4) the creation of the faked copy of the enterprise's web-site page (with the famous brand) and the location of photos of the not existent product on them with the essentially reduced price (action or sale). The evil-minded people receive the complete advanced payment on their own accounts for the virtual product, after which they send the joky message of the crime's commitment;

5) the ill-intentioned person receives the access to the enterprise's letter-box, through the use of the harmful software ("virus"), which is used by its employees to post the invoices for the clients' payment for the received product or service. The ill-intentioned person changes the account's requisites of the enterprise for his/her own requisites with the help of the definite manipulations with the document. The buyer realizes the money remittance to the bank account of the ill-intentioned person, using the requisites of the false invoce;

6) the destruction of the electronic documents (bill of parcels, invoice, order), containing information on the fact of the goods consignment's loading to the certain buyer, in the information system of accounting. The information on the client's liabilities and the fact of his product's receipt are lost in the result of such actions;

7) the conspirancy of the enterprise's commercial manager with its programist, concerning the regulation of the accounting's information system in such a way, that the maximal discount is set for the concrete buyers automatically at the definite manipulations in the documents for the goods realization;

8) the employee of the enterprise's staff service appropriated illegally the copies of the documents (the passport of the Ukraine citizen and the identification number certificate) of the job seekers at the selection of the candidates for the vacant positions, due to which he/she arranged the credits for them;

9) the fabrication of the loyalty cards' duplicates for the systems of supermarkets, produced for the other citizens, in order to pay by the money, accumulated on the bonus accounts. Using the software's vulnerability of the trade network's loyalty system, the evil-minded people restored the bonus balance through the definite program manipulations, which allowed them to realize the money removal repeatedly by the unlimited number of times;

10) the forgery of the Ukraine citizen's passport (who died) and his/her financial documents for the illegal getting of credit on the personal account of the ill-intentioned person in the bank with the following making the ready cash in the bankomats;

11) the use of the electronic-computing technics to take possession of data, concerning the enterprise's employees (passports of the Ukraine citizens and the identification numbers). The swindlers arrange credits in the Internet with the help of these documents, not giving any information to their owners. The obtained assets are

transferred to the personal bank accounts and are removed as the ready cash in the bankomats;

12) the supermarket cashier of the trade system made the copies of the buyers' card accounts requisites hiddenly with the help of a special device, with the following removal of all the assets from the card. The evil-minded person received the PIN-codes of the cards by watching how the clients put them in at the POS-terminal, while paying for the product;

13) abusing the official state, the bank employee forged the bank documents for the illegal remittance of clients' money to the account under his/her control;

14) the controller-cashier in the bank institution, who had an access to the automation client system, realized the not-sanctioned issue and the activation of the bank cards independently, after which he/she created the official electronic bank documents – cheques on the cash issue;

15) the change of the information, being processed in the electronic-computing machine, with the purpose of the illegal money appropriation of the bank's clients;

16) the use of the harmful software ("virus") to break up the personal cabinets of the communal enterprise's clients and the entry of changes into the accounting indicators of the consumed services;

17) the bank employee realized the forgery of the bank documents, not giving any information to its clients, for the illegal remittance of their money to the account under his/her control;

18) the repeated replenishment of the mobile account of the evil-minded person, who used one 500-UHR denomination, to which the isothermal ribbon was fixed, which gave the possibility to use it repeatedly;

19) the entry of the untruthful news into the information system of the financial institution by the bank's employee and the forgery of the corresponding documents with the purpose of the credit contract's arrangement for the not existent person. Later on, the illegally obtained credit was transferred to the account of the evil-minded person;

20) the use of the harmful software ("virus") to break up the electronic letter-boxes, accounts, logins and passwords of enterprises' employees for the collection and spreading of the secret information, which can potentially ruin the reputation of enterprises.

In order to have the objective estimation of the scope and the variety of cybercrimes in Ukraine, you should take into account that the significant number of such crimes is left as not being included into the United Register of Pre-Court Investigations. According to the questioning results of the Ukrainian organizations, conducted by "PricewaterhouseCoopers", it was determined: 28% of the organizations in Ukraine will not probably or will never inform of such facts to the state or to the law enforcing bodies (compared with 12% of the respondents in the world); more than half (54%) of these respondents state that they are not sure in the fact that the law enforcing bodies have the necessary qualification in this field, but the other 41% - do not trust the law enforcing bodies [21]. It's reasonably to add to the mentioned reasons too, that cybercrimes are very often qualified mistakenly as the technical or the program break in the operation of information technologies of accounting; the conscious hiding of the facts, concerning cybercrimes, with the purpose of keeping the reputation of the higher leadership and the enterprise before owners, investors, business-partners, clients and controlling bodies; the complexity of the expertise procedure of the cybercrime's circumstances by the cyberpolice employees (removal of servers, computers, modems and others), paralyzing the enterprise's operation for the long time.

According to the above-mentioned state of cyberthreats in Ukraine, the main aim of the evil-minded people lies in the enterprise's money (or goods) alienation, being achieved by the illegal influence on the behavior of the employees and the influence on the functioning of the accounting's information technologies. The protection's guaranties of enterprises assets stipulate the necessity in the adequate managerial decisions-taking on cybersecurity. Such decision should take into account the principally new specificity of cybercrimes in comparison with the traditional crimes against ownership, namely: the intellectual character of crime; the place of crime – cyberspace; the unpersonification of cybercrimes; the remoteness of a cybercriminal; the means of the crime commitment – the harmful program product; the electronic form of the cybercrimes commitment's arguments; the possibility of the fast remote change or the destruction of the electronic (digital) tracks of cybercrimes commitment; the additional need in special programs and equipment for the fixation of the cybercrimes commitment's arguments and the others.

The optimal managerial decision for the system opposition to cybercrimes in the enterprises accounting's information technology is the creation of the internal audit's service. Such selection is grounded by the fact that the internal audit has the majority of the necessary knowledge (competences) for the struggle with cybercrimes in the information technologies of the accounting at the enterprise, namely:

- on the object of control – the economic operations, taking place in the cyberspace of the enterprise;
- on accounting (financial reporting, accounting calculations, methods of accounting, primary documents, the rules of operation in information systems and others);
- on the remote control programs of the enterprise's bank accounts (the order of entry into the system, the creation and transaction of payment documents, the requisites of cashless payments);
- on the means and methods of control (actual, documental, calculation-analytical and others);
- on means of electronic communications (including the information-communication technologies, the program ones, the software-hardware means, the other technical and technological means and equipment);
- on social engineering (provocation of the employees for violation of security rules or illogical actions).

However, the struggle specificity with the principally new method of crimes against the ownership requires the definite innovations into the traditional methods of the internal audit that will correspond to the modern

provocations of swindling in the enterprise's cyberspace. The internal audit in this context is appealed for the improvement of the enterprise cybersecurity's existing level: to reveal, to avoid and to neutralize the real and the potential cyberthreats in time.

The methods of the internal audit requires the improvement in the part of the additional use of those methods of security and control, that will allow solve the following tasks: maintenance check-up of cybercrimes at the enterprise; the reveal of the criminal actions in the enterprise's cyberspace; the fixation of the electronic (digital) tracks in computers, systems, networks and others; the renewal of the cybercrime's commitment circumstances (the actions of the employees, the processes in the hardware and software); collection and storage of the electronic (digital) evidences of cybercrimes; the analysis of the operation's principles of the harmful program products ("virus"); the definition of the place, from which the cyberattack has started; the determination of the cybercrime's subject; the elaboration of the recommendation for the higher leadership.

The service of the internal audit should improve its own staff provision, for the complex elaboration and the use of the mentioned methods at the enterprise, in the following way: to involve the professional in cybersecurity of the enterprise's IT-infrastructure into the complement of its service; to increase the digital competence's level of the internal auditors (the second education, passing of the cources, certification, the self-education, etc.).

As the weak place in cybersecurity of information technologies of enterprises accounting is the human factor (curiosity, trust, carelessness, inability to understand), then, the methods of the internal audit should foresee the maintenance check-up of the employees' mistakes in cyberspace. It's reasonably for the internal audit's service to develop the "Protocol of Behavior Rules for Employees in Enterprise's Cyberspace". The Protocol contents should reflect the list of the rules, which the employees would be obliged to observe at their work in the cyberspace. The main recommendations of such rules are the following:

- the use of the complex access passwords (letters and numbers, not less than 8 symbols, the different decomposition of the keyboard (fingerboard);
- the logins and passwords should be kept in secret from the other persons;
- the logins and the passwords of access to the accounting and banking programs should be kept on the physically separated information bearer (flash drives) – the operation in which is possible only on the working computer and at the presence of the put on flash drive (token);
- the prohibition to use the found unknown flash drives (or CD-disks) on the enterprise's computers;
- to ensure the access to the enterprise's internal local network only through the identification of the computer MAC- address;
- the use of the multi-level authorization of access (sms dispatch with the temporary code to the employee's mobile telephone);
- the prohibition to use the social networks at the working places;
- "hygienics" of the electronic mail – not to open the letters from the incomprehensible addressers, the prohibition to set the unknown programs, the transition, according to the doubtful dispatch, the change of passwords or the other ones;
- the physical access prohibition of the strangers or their devices to the internal network of the company;
- the differentiation of access to Wi-Fi between the guest one and the system one;
- the prohibition to set the programs independently or for their renewal, not giving any information to the professional in cybersecurity;
- the limitation of the remote access to the working table from the private (home) computers of the employees;
- the prohibition to realize the dispatch of the enterprise's accounting documents with the help of the programs (Viber, Facebook, WhatsUpp, Telegram and others) on the personal smartphones of the employees.

Such a document is formaly approved by the enterprise's leader in the form of the order and is designed for the obligatory fulfillment, in the first turn, of the higher leadership, the employees of the accounting, the financial, the personnel, the warehouse and the other services of the enterprise. The internal audit service should conduct the trainings in cybersecurity systematically (not less than once a month) additionally for the increase of the digital competence of the employees and their culture of safe behavior in the enterprise's cyberspace.

The traditional methods of the internal audit require the addition by the special methods of watching the electronic (digital) track in the enterprise's cyberspace, which will allow analyze the influence on the enterprise's employees, their actions with the electronic documents, the operation of the software and the hardware, the physical connection of computer systems and others. The peculiarity of such methods is the fact that they are represented by the computer program products in the majority of cases. The recommended list of such programs and their functioning design for the internal audit are presented lower:

1) it's recommended to use the special programs-analyzers of traffic, which operation's methods allow recognize the structure of the different network protocols with the aim of catching and analyzing traffic of the enterprise's networks, - namely: to examine the caught packages and to decode them in the real time; to see IP-connection (IP-addresses, ports, sessions), MAC-addresses, the host's name and others. You may refer "Wireshark", "tcpdump", "Comm View", "Ultra Network", "RMON" and others to such programs;

2) it's reasonably for the internal audit's service to use the programs of analysis and restoration of the browsers' history for the control and the analysis of the electronic (digital) tracks, concerning the committed actions by an employee in the Internet system at the working place. The most popular among such programs are: "Hetman Internet Spy", "Starus Web Detective", "RS Browser Forensics" and others. The operation's

methods of the mentioned programs allow fot the internal audit's service fix the electronic (digital) evidences of the cybercrime: the history of searching, the visited pages of sites, the lists of loadings, the examined documents in the browser, the read electronic letters, correspondence in the electronic letter-boxes, revision of the correspondence in the social networks, the reviewed video-rollers and others. The value of such programs is the fact that they allow restore the very that history of the user's events, which was removed by him/her in the browser or formed on the disk with the purpose of hiding;

3) all the information technologies of enterprises accounting ("SAP R3", "BAS", "1 S: Enterprise 8" and others) practically have the standard interface mechanism of the history reflection of actions. The mentioned history contains information of all the actions of the user, being connected with the electronic document. The revision of such a history allows watch, who, when and how created or changed the existing document in the program. The fixation's arrangement of the history of changes in the electronic accounting documents and the obtaining of access for its revision are taken place at the level of the information system administration. Therefore, the methods of the information technology's functioning of the enterprise accounting are the integral component of the internal audit's methods;

4) the use of the monitoring program products at the enterprise (the hardware or the software products, containing Keylogger as a modul), which allow fix the activity of the users (or processes) and determine the identification of their participation in the definite events. It's recommended to use one of the presented programs for the tasks of the internal audit at the enterprise: "Spytech SpyAgent", "Spyrix Personal Monitor", "All ln One Keylogger", "Punto Switcher", "REFOG" and others. The use of Keylogger in the internal audit's operation will allow analyze the circumstances of a cyber-incident at the enterprise efficiently: the access to information, concerning the composition of the key words and word combinations on the key-board of the employee, the selection's attempt of login and password for the access, the time of the employee's activity at the computer, catching of the mouse's clicks, catching of the exchange buffer, monitoring of the file activity, monitoring of the system register, monitoring of the tasks' turn, the documents, sent to the printer, the use of the external bearers of information (USB, CD, memory cards) informed immediately of the behavior and others. The analytical information of the mentioned type of programs allows to the internal audit determine groundly the reason-result connections in the cybercrime's circumstances.

The use of the presented programs at the enterprise should be agreed with the owner, the legal services, the system's administrator; they should be officially gained with the corresponding licences, regulated in the documents (principles, instructions) of the internal audit, etc. with the purpose of the formation legitimacy of the electronic (digital) evidences.

It's reasonably for the internal audit's service to define the circle of the officials, who are intrinsic in the risk of participation in a cybercrime, due to the character of their functional duties. The following people belong to such employees in the first turn: the higher leadership; the accountants or the financiers, who realize payments through the programs of the remote control of the bank account; the storekeepers, who realize the loading of goods; the secretaries, who receive the electronic letters on the official e-mail, and others. It's the internal audit's service priority to use the methods of cyberthreats monitoring for the very such categories of enterprise employees.

The presence of the special controlling methods (programs) of the electronic (digital) tracks in the enterprise's cyberspace allows include groundly the tasks on testing of cyberthreats (or cybercrimes) into the programs of the internal audit at the enterprise. Correspondingly, the reports of the internal audit should reveal the result of the realized control of cybercrimes and should contain the practical recommendations on their maintenance check-up at the enterprise.

3 Conclusion

The rapid development of information technologies at the beginning of XXI century caused the absolute progress of human civilization. The appearance and development of cybercriminality in the global scale have become the attendant phenomenon of such a progress. The main danger of cybercriminality lies in the illegal expropriation of property from their owners by the way of any interference into the functioning of the computer system or the manipulation with the computer data. Cybercrimes are principally different from the traditional crimes against the ownership by the fact, that the crime takes place in the cyberspace; the anonymity of cybercrimes; the harmful program product is the means of crime; the remoteness of a cybercriminal; the electronic (digital) form of evidences for the cybercrimes' commitment and others.

Cybercrimes in Ukraine take the fourth place among the most widely-spread types of economic crimes in the sphere of enterprises' economic activity. The most attractive for cybercriminality are information technologies of enterprises accounting. The real possibility of access to the information, concerning the available assets of the enterprise and the manipulations with the accounting documents for their alienation have become the reasons of such attractiveness. The actual level of cybersecurity at the Ukrainian enterprises is left to be absolutely low – only every third organization in Ukraine has the program of cybersecurity.

In order to protect the enterprise's assets from cybercriminals, it's reasonably to organize the adequate opposition at the level of the internal audit's service. However, the methods of the internal audit should take into account the specificity of struggle with the crimes against the ownership in the cyberspace of the enterprise. Therefore it's recommended to do the following for the

efficient organization and functioning of the internal audit's service at the enterprise:

1) to involve the enterprise's IT-structure professional in cybersecurity into the staff complement of the internal audit's service and to increase the level of digital competence of the internal auditors;

2) to elaborate the rules of behavior for the employees in the cyberspace of the enterprise and to introduce them at the enterprise in the form of the internal document "Protocol of Behavior Rules for Employees in Enterprise's Cyberspace";

3) to add the traditional methods of the internal audit by the special methods (programs) of watching the electronic (digital) track in the cyberspace of the enterprise, namely: the programs-analyzers of traffic, the programs of the analysis and renewal of the history of browsers, the information technologies of accounting (in the part of the history analysis of the user's actions with the document), the monitoring program products (the hardware or the sofrware products, containing Keylogger as the modul); to develop the internal Principle "On Programs' Use of Watching Electronic (Digital) Track in Cyberspace of Enterprise by Internal Audit" and to introduce it at the enterprise.

Thus, the introduction of the above-mentioned recommendations into the traditional practice of the internal audit's operation will allow create the reliable system of cybersecurity at the enterprise, which will be able to oppose to the modern cybercrimes.

References

1. O. Pyschulina, Digital Economics: Trends, Risks and Social Determinants (Razumkov Center, 2020), p. 274
2. The Global Risks Report 2019. 14th Edition (World Economic Forum, 2019), p. 114
3. J. A. Lewis, Z. M. Smith, E. Lostri, The Hidden Costs of Cybercrime (CSIS, 2020), https://www.csis.org/analysis/hidden-costs-cybercrime. Accessed on 25 January 2021
4. P. Rosati, F. Gogolin, T. Lynn, European Accounting Review (2020)
5. G. D'Onza, G. Sarens, S. DeSimone, Accounting Horizons, **34 (4)**, 57-74 (2020)
6. J. Christopher, Journal of Management Inquiry, **28 (4)**, 472-483 (2019)
7. M.N. Ivanova, A. Prencipe, Journal of Accounting Auditing and Finance, 0148558X20971947 (2020)
8. JR. Cohen, JR Joe, JC. Thibodeau, GM. Trompeter, AUDITING: A Journal of Practice & Theory, **39 (4)**, 57-85 (2020)
9. N. Betti, G. Sarens, Journal of Accounting and Organizational Change (2020)
10. Y. Chen, B. Lin, LZ. Lu, GG. Zhou, Managerial Auditing Journal, **35 (8)**, 1167-1188 (2020)
11. D. Weekes-Marshall, Journal of Corporate Accounting and Finance, **31 (4)**, 154-165 (2020)
12. T. Bondarenko, R. Dutchak, O. Kondratiuk, O. Rudenko, A. Shaikan, E. Shubenko, Atlantis Press, **129**, 39-46 (2020)
13. Yu. M. Popivnyak, Business Inform, **8**, 150-157 (2019)
14. L. P. Polovenko, S. V. Merinova, Entrepreneurship and Innovations, **10**, 183-187 (2019)
15. L. Smidt, A. Ahmi, L. Steenkamp, D. P. van der Nest, D. Lubbe, Australian Accounting Review, **29**, 516-531 (2019)
16. World Research of Economic Crimes and Swindling of 2020: Questioning Results of Ukrainian Companies (PwC, 2020), p. 14
17. General Public Prosecutor's Office of Ukraine (2021), https://old.gp.gov.ua/ua/statinfo.html. Accessed on 25 January 2021
18. National Cyber Security Index (2021), https://ncsi.ega.ee/ncsi-index/. Accessed on 25 January 2021
19. Harvard Belfer National Cyber Power Index 2020 (NCPI, 2020), p. 84
20. Cyberpolice in Ukraine (2021), https://cyberpolice.gov.ua/. Accessed on 25 January 2021
21. World Research of Economic Crimes and Swindling of 2018: Questioning Results of Ukrainian Organizations (PwC, 2018), p. 19