UDC 331.1

Zatonatskiy D.
Ph. D. student,
National Institute for Strategic Studies, Kyiv, Ukraine;
e-mail: dzatonat@gmail.com; ORCID ID: 0000-0002-4828-9144
Marhasova V.
Doctor of Economics, Professor,
Professor Department of Theoretical and Applied Economics,
National University «Chernihivska Politehnika», Ukraine;
e-mail: viktoriya.margasova@gmail.com; ORCID ID: 0000-0001-8582-2158
Korogod N.
Ph. D. in Pedagogic Sciences, Associate Professor,
Head of the Department of Intellectual Property and Projects Management,
National Metallurgical Academy of Ukraine, Dnipro, Ukraine;
e-mail: n.korogod@gmail.com; ORCID ID: 0000-0002-0242-5497

INSIDER THREAT MANAGEMENT AS AN ELEMENT OF THE CORPORATE ECONOMIC SECURITY

Abstract. This paper considers the insider threats in the companies from different sectors and various methods of their assessment. The problem of information leakage is becoming increasingly important for companies in all areas of economic activity. The problem of insider threats is becoming increasingly important, as the company may incur losses not only due to the leakage of information about its inventions, but also through lawsuits in case of theft of personal information of the customers, contractors and more. This means that in order to gain access to the international markets, Ukrainian companies must have an appropriate level of protection not only of the company's confidential information, but also of the data on customers, contractors, etc. The objective of the article is to analyze the existing methodological approaches to the assessment of insider threats in the enterprise as a component of personnel and economic security. We came to the conclusion that different industries have different vulnerabilities to insider threats and different approaches to insider threat management. It was determined that information leaks are a serious threat to the company's economic and personnel security. It was discovered that firms have achieved significant improvements and developed effective procedures for counteracting external threats, however, protection against insider attacks remains rather low. In the course of the research, the concept of an insider attacker was defined, the types of insider threats were established, and the main actions of the personnel prior to the insider attack were outlined. It was proved that the degree of insider threat is determined by the type of activity of the company and the liquidity of information that may be leaked. Most leaks are observed in high-tech companies and medical institutions, while the most liquid is the information of banks, financial institutions, industrial and commercial companies.

Keywords: corporate economic security, human capital, personnel security, insider threat management, information database

Formulas: 0; fig.: 5; tabl.: 0; bibl.: 20.

Затонацький Д. А.
аспірант,
Національний інститут стратегічних досліджень, Київ, Україна;
e-mail: dzatonat@gmail.com; ORCID ID: 0000-0002-4828-9144
Маргасова В. Г.
доктор економічних наук, професор,
професор кафедри теоретичної та прикладної економіки,
Національного університету «Чернігівська політехніка», Україна;
e-mail: viktoriya.margasova@gmail.com; ORCID ID: 0000-0001-8582-2158

Корогод Н. П.
кандидат педагогічних наук, доцент,
завідувачка кафедри інтелектуальної власності та управління проєктами,
Національна металургійна академія України, Дніпро, Україна;
e-mail: n.korogod@gmail.com; ORCID ID: 0000-0002-0242-5497

УПРАВЛІННЯ ІНСАЙДЕРСЬКИМИ ЗАГРОЗАМИ ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Анотація. Розглянуто інсайдерські загрози в компаніях, що належать до різних секторів економіки, а також визначено різні методи їхньої оцінки. Проблема витоку інформації стає дедалі важливішою для компаній в усіх галузях економічної діяльності. Проблема інсайдерських загроз набуває усе більшого значення, оскільки компанія може понести втрати не лише через витік інформації про її винаходи, а й через судові позови в разі крадіжки особистої інформації клієнтів, контрагентів тощо. Це означає, що для виходу на міжнародні ринки українські компанії повинні мати належний рівень захисту не тільки конфіденційної інформації компанії, а й даних про клієнтів, контрагентів тощо. Метою статті є аналіз наявних методологічних підходів до оцінки інсайдерських загроз на підприємстві як складової економічної та кадрової безпеки. Ми прийшли до висновку, що різні галузі промисловості і сфера послуг мають різну вразливість до інсайдерських загроз, тому застосовують особливі підходи до управління інсайдерськими загрозами та кадрової безпеки. Було встановлено, що витоки інформації є серйозною загрозою економічної та кадрової безпеки підприємства. Підприємства досягли значних успіхів і створили ефективні процедури для запобігання зовнішнім загрозам, однак захист від внутрішніх загроз залишається на дуже низькому рівні. У процесі дослідження було дано визначення поняттю внутрішнього зловмисника, виділено окремі типи інсайдерських загроз і встановлено, які основні дії виконують співробітники підприємства перед проведенням інсайдерської атаки. Було доведено, що ступінь вразливості до інсайдерської загрози визначається типом господарської діяльності компанії та ліквідністю інформації, яку можуть вкрасти. Найбільше витоків спостерігається у високотехнологічних компаніях і фармацевтичних компаніях, тоді як найліквіднішою є інформація в банках, фінансових установах, промислових і торговельних компаніях.

Ключові слова: економічна безпека підприємства, людський капітал, кадрова безпека, управління інсайдерськими загрозами, інформаційні бази даних.

Формул: 0; рис.: 5; табл.: 0; бібл.: 20.

Introduction. Traditionally, the personnel security as a part of the corporate economic security considered mainly physical aspects such as protection of the enterprise and personnel, physical protection of important documents, maintenance of access control procedures and policies, etc. However, with the development of the information technology, other threats to economic and personnel security began to appear. In particular, this applies to information held by the enterprise as a whole. If the procedures of physical security have already been worked out, then most companies, especially in Ukraine, do not yet have sufficient experience in protecting information in cyberspace. The problem of information leakage is becoming increasingly important for companies in all areas of economic activity. The problem of insider threats is becoming increasingly important, as the company may incur losses not only due to the leakage of information about its inventions, but also through lawsuits in case of theft of personal information of the customers, contractors and more. This became especially relevant after the entry into force of the Pan-European General Data Protection Regulation (GDPR) in the spring of 2018, which sets the size of sanctions for breaches of the rules on the protection of personal data of EU citizens. This means that in order to gain access to the international markets, Ukrainian companies must have an appropriate level of protection not only of the company's confidential information, but also of the data on customers, contractors, etc. What is generally perceived as a normal event in Ukraine can lead to huge fines and lawsuits in the EU. In particular,

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

very often, when dismissed, a company employee takes with him a database of customers or suppliers, because the company does not have appropriate procedures in place to prevent such actions. What in Ukraine remains only a private problem of the company, in the EU market can turn into sanctions, fines and loss of customers and partners. That is why insider threats and information leakage become an important component of economic and personnel security of the enterprise, especially if its goal is to enter foreign markets. For example, according to the international analytical center InfoWatch, which is constantly monitoring the leakage of confidential information, in 2018, 2,263 cases of serious leakage of confidential information were registered. It should be noted that companies and analytical centers researching and monitoring insider threats are not able to cover all cases of leakage, so they focus on the largest companies and major leaks that have had significant negative financial consequences for companies. Thus, according to the center, in 2018, as a result of the leaks, more than 7.28 billion personal data records were compromised (social security numbers, details of bank and other types of cards, other information).

Literature review and problem statement. The issue of insider threats and protection against them has recently become widespread in the scientific literature. Scientists have begun to actively draw attention to the problem of information leakage, as well as to the fact that it has not only external but also internal sources.

Homoliak et al. [1] conducted a thorough analysis and systematization of research on insider threats and identified four main areas of research: 1) analysis of specific cases and data sets; 2) research into aspects of the behavior of insiders, life cycle, indicators and channels for the spread of insider attacks; 3) modeling and creating software methods to determine the attack; 4) an overview of possible procedures for protection against insider threats.

Costa et al. [2] tried to create an ontology of insider threats. To do this, the authors defined the insider threat and the main areas of its occurrence, proposed their own ontology of threats and technology of automatic word processing for its implementation.

To identify the most common insider threats, Whitty [3] created a model that includes psychological, behavioral, and social variables that point to potential insiders. The author also explored possible channels for the spread of insider attack.

In particular, according to Agrafiotis et al. [4], the threat to the organization from its own employees continues to grow steadily and significantly, as evidenced by many examples. For many years, the security organization has focused on internal threats, including information. The authors emphasize that the possibility of an insider threat cannot simply be ignored. They consider possible technologies that can be used to detect threats automatically. These technologies must identify threats by monitoring personnel to perform certain actions of concern. According to scientists, these actions can be divided into two categories: 1) actions that violate policies, procedures and regulations that were created specifically to prevent the behavior of personnel that could pose a threat; 2) actions similar to those already identified as an insider attack. In particular, it is proposed to use so-called «traps» in the information system that will respond to the above actions and warn of danger.

Mahajan & Sharma [5] pointed out that firms are increasingly using cloud technologies to store important information, so they are not able to fully control security and protection procedures. In their study, the authors identify several types of clouds that companies can use to store their information, in particular, private, common, public, hybrid clouds that have different degrees of protection. Also, the authors highlight two main possibilities: the presence of an insider among the staff of a company engaged in the provision of cloud services and the presence of an insider in another company, which is involved in the organization of the cloud in the framework of outsourcing. The authors suggest several possible actions that can identify the threat and neutralize it.

An important aspect considered in the scientific literature is the identification of possible methods for detecting insider attacks. In particular, Sanzgiri & Dasgupta [6] believe that most insider attacks are carried out by individuals with relevant technical skills, so the most successful is a combination of different strategies and methods for their recognition.

Kont et al. [7] tried to create a universal program for detecting and recognizing insider threats. To this end, they identified five different types of threats (sabotage, theft, fraud, espionage,

and accident) and proposed six separate indicators based on the behavioral and technical aspects of the threat. According to the authors, the simultaneous use of all indicators will minimize the damage and, at best, even prevent the incident in general.

Ring et al. [8] proposed a new algorithm for identifying insider threats by detecting anomalous interference in the work of the internal network. To increase the effectiveness of this approach, the authors propose to use historical data on insider attacks and analysis of actions that preceded them to avoid false alarms.

Park et al. [9] proposed to use the behavior of employees in social networks to identify possible insider threats. The authors proposed an algorithm and criteria by which to identify a potential insider. They came to the conclusion that an insider can be identified by analyzing his posts on social networks, provided that he uses a certain set of words and phrases that express negative emotions and intentions.

Gawai et al. [10] focused on identifying insider threats through employee activity on social media and the Internet. To construct the relevant indicators, the authors suggest using the content and pattern of e-mail correspondence, browser and browsing history, frequency of e-mail exchange, pattern of access to files and equipment. Researchers suggest two approaches: 1) without personal observation using automated systems that detect atypical user behavior; 2) with personal surveillance used to assess threats from former employees. It was found that the use of the dashboard with points proposed by the authors will allow the human resources department to quickly identify potential internal attackers and prevent possible attacks.

In turn, Elifoglu et al. [11] proposed to increase the effectiveness of combating insider threats through more fruitful cooperation between the departments of information technology management and human resources management. They emphasize that the main causes of insider attacks are mistakes, negligence, greed or reckless behavior.

Eggenschwiler et al. [12] noted that firms that provide financial services are among the most vulnerable to insider attacks because they lead to huge losses. The authors focused not only on how firms detect attacks, but also on possible ways to respond to them. They noted that financial firms use two approaches: internal and external response. If, in their opinion, the attack had minimal negative consequences, then an internal approach is used, i.e. the problem is solved within the firm to prevent publicity. And only in the case when the consequences cannot be hidden, an external approach is used, which requires the involvement of a third party in resolving the conflict.

Clarke et al. [13] emphasize that the creation of a dashboard with key indicators that pinpoint potential internal attackers is one of the main areas of combating insider threats. They found that one of the main indicators is the degree of satisfaction in the workplace, and the priority should be to identify anomalies in data visualization.

Linkov et al. [14] tried to establish a link between the introduction of procedures and regulations to prevent insider threats and the outcome of their use. The authors determined that insider attacks are facilitated not only by the lack of established rules, but also by over-regulation.

Growing number of the researchers are inclined to believe that in order to ensure personnel security and successfully counter insider threats, it is necessary to create and implement a comprehensive program to combat insider threats. For example, Scherer & Ruggiero [15] proposed a version of such a program that includes four main components: information and cybersecurity, people and culture, physical security and security and control of company resources.

While most of the insider attacks are intentional, there are also threats that can result from unintentional actions. Ismail & Yusof [16] drew attention to information leaks that occur due to carelessness in the daily work of the company. Researchers have noted that important channels of leakage are posts on social networks, when outsiders can receive the necessary information through targeted conversation due to the carelessness of the user. The second common channel of leakage is the use of personal technical means for work purposes, as they are less protected and more vulnerable to internal attacks. According to the authors, an effective strategy to prevent unintentional leakage of information should combine technical elements (technological support for information protection), organizational elements (management's focus on preventing leakage by

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

creating appropriate procedures and propagating appropriate information culture), behavioral elements (explanatory talks and trainings), and procedural elements (certain regulations, controls and sanctions).

Abd & Hassan [17] believe that the protection of trade secrets is one of the most important areas of the corporate economic security and should be part of personnel security. According to researchers, legal measures are not sufficient for reliable protection of information, so it must be accompanied by appropriate administrative tools. To do this, the authors propose to use five main methods: strict recruitment, the use of mandatory employment agreement, continuous awareness of employees with the company's information protection policy, constant monitoring of employees' actions with information and the use of adequate restrictions, removal of all documents containing commercial secret, from the employee upon dismissal.

Also, according to researchers, it is worth noting how information leaks and espionage detected in the organization will affect its future activities. Ho et al. [18] emphasize that after the detection of an insider attack within the firm, there may be a crisis of confidence in a large number of employees, regardless of whether a direct source of information leakage has been identified or not. The authors emphasize that very often people who have been in contact with or worked directly with the source of the leak will also be suspected, so it is important to define criteria that allow to assess the degree of their reliability.

No less important is the issue of the company's losses from insider threats. In this case, there may be not only direct losses (value of stolen invention, money, intellectual property), but also indirect costs or the so-called «lost profit». In most cases, it is very difficult to calculate, and existing methods focus mainly on certain aspects of the damage. Butkevičius [19] offers a universal model for calculating lost profits, which takes into account the cost structure of the company and allows you to take into account the maximum possible profit that the firm would have received if there was no leakage.

The purpose. The aim of the article is to analyze the existing methodological approaches to the assessment of insider threats in the enterprise as a component of personnel and economic security.

The scientific hypothesis is that different industries have different vulnerabilities to insider threats and different approaches to insider threat management.

Materials and methods. The methodological and information basis of our research is the analytical information and databases provided by the analytical center InfoWatch.

Results and discussion. Our literature review revealed that the vast majority of researchers emphasize that the protection of information from external and internal threats in the digital space is becoming a priority for the companies. While most companies already have effective procedures in place to ensure physical security and some successful efforts to protect information from external threats, the problem of preventing insider attacks still remains largely unresolved.

For example, according to a study conducted by the UK Government's Department for Enterprise and Regulatory Reform in 2008, most companies focused all changes to improve security in the area of external threats:

– 55% of enterprises had a clearly defined security policy in the form of a constituent document;
– 40% constantly conducted staff training on the prevention of external threats;
– 14% used a strict multifactor authentication procedure;
– 11% had already implemented the BS7799 / ISO27001 standards;
– 99% backed up system data;
– 98% had special software to protect against intrusion into the system;
– 97% used email filters;
– 97% used the software to protect against viruses;
– 94% encrypted all conversations on the network.

On the other hand, with regard to internal threats, the study found the following trends:

– 52% of enterprises did not assess the security risks of the enterprise from internal threats at all;

– 67% did not have any procedures for protection against leakage of confidential data on removable media;

– 78% of companies did not encrypt and did not protect the hard drives of their computers;

– 84% of companies did not have filters on the outgoing e-mails regarding the availability of confidential information.

This means that in today's environment, companies need to pay more attention to internal threats, because, unlike external ones, they are quite vulnerable to them and rely more on the integrity and work ethics of employees.

According to the study by Costa et al. [2], an insider attacker is a former or current employee, contractor or business partner who is subject to the following requirements:

– has or has had authorized access to the internal organizational network of the system or data;

– intentionally exceeded the level of access or used his access in such a way as to harm the confidentiality, integrity and accessibility of the information or information system of the organization.

As a result, insider threats are affected by technical, behavioral, or organizational problems, so policies, procedures, and technologies need to be developed to address them.

One of the first tasks in identifying and preventing an insider attack is to determine its type. For example, Whitty [3] identifies the following types of insider attacks: fraud, money laundering, reputation damage, theft (including theft of IP address, data, account), illegal employment.

Insider threats can result from intentional or accidental actions. Accidental actions can be prevented mainly by raising staff awareness of this possibility, i.e. increasing their information literacy. Instead, the company's personnel security strategy should be aimed at preventing intentional actions. According to Sanzgiri & Dasgupta [6], the most common actions of an insider attacker are:

– Unauthorized use, copying and deletion of data;
– Change of data or information belonging to the organization in order to distort it;
– Destruction or deletion of critical data or resources;
– Espionage with criminal intent;
– Using other users' accounts to commit criminal activity.

When using information technologies to prevent the leakage of information, as a rule, there are the following actions that pose an insider threat, which can be tracked automatically:

1) Physical impossibility of action (for example, login from an IP address that does not geographically coincide with the physical location of the employee, VPN connection from different IP addresses that are geographically remote but belong to the same account, etc.);

2) Access to blacklisted sites;

3) Use of external drives that are not authorized;

4) Multiple unsuccessful attempts to log in to different accounts;

5) Constant sending by e-mail of files with names that coincide with those registered in the system;

6) Constant sending of e-mails with large files in the appendix;

7) Excessive use of social networks during working hours;

8) Permanent deletion of files of large size or with names registered in the system.

Automatic tracking of such actions will help to identify insider threats at an early stage and prevent further leakage of important information.

The study by the analytical center InfoWatch [20] shows an increase in the threat of the information leakage, which leads to losses for companies. Recently, there has been a rapid increase in the number of such cases. In particular, the number of information leaks increased from 801 cases in 2011 to 2263 cases in 2018. The jump in 2017 was especially noticeable (the number of leaks increased by 36.9% (to 2131 cases) compared to the previous year (1556 cases)), while in 2018 the growth was somewhat moderate (only 6.1%).

It should be noted that the strength of the leaks can also be different. In particular, in 2018, 81 cases of large leaks were recorded, and in 47 cases the volume of data leakage exceeded 10

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

million records. In general, mega-leaks accounted for 97.5% of all leaks (7.1 billion records), i.e. threats were important mainly in large companies with a significant amount of information.

As for the source of information leakage, in 2018 the majority of cases (1393) (63%) occurred through the fault of insiders, while external attacks accounted for only 37%.

Among the leaks, most of them were caused by current and former employees of the company (*Fig. 1*).

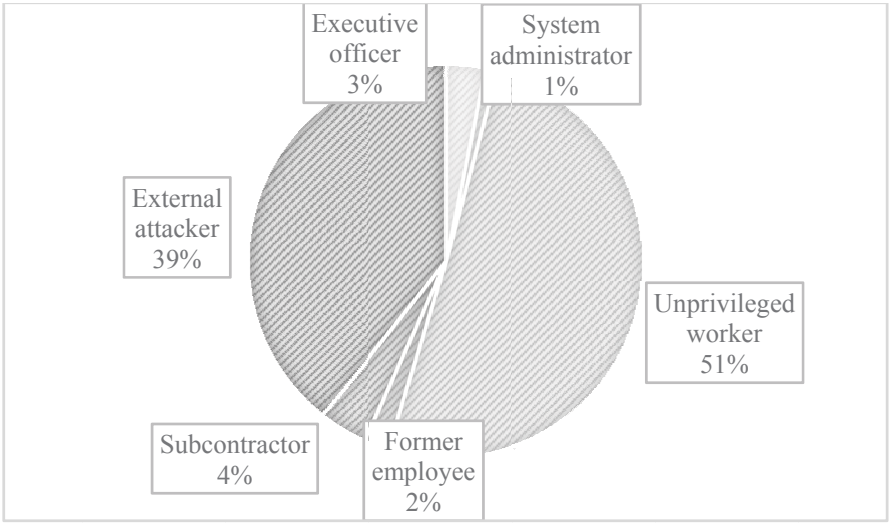

Fig. 1. **Shares of the leaks by source in 2018**

Source: compiled by the author on the basis of [20].

Thus, the share of leaks caused by privileged users, i.e. those with full and uncontrolled access to internal information, remains quite high.

As for the sources of information, personal data continue to dominate (69.5%), payment information is in the second place (16.9%), and trade secrets are in the third place (8.1%) (*Fig. 2*).

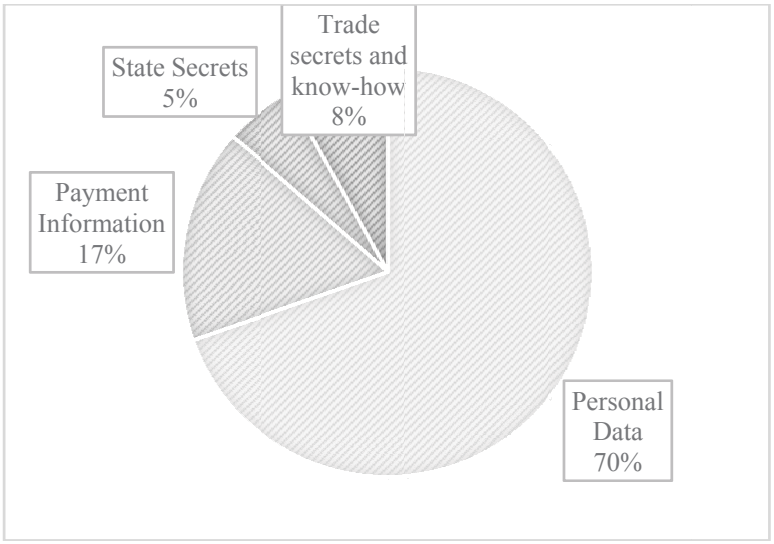

Fig. 2. **Shares of the leaks by data types in 2018**

Source: compiled by the author on the basis of [20].

It should be noted that all types of information are important for the company, as they can lead to potential losses. The problem is that losses from the leakage of commercial information can be calculated and predicted. Losses from the leakage of other types of information cannot be calculated directly. For example, leaks of customers' personal data can lead to a loss of trust in the company, lawsuits, penalties, falling stock prices, etc., depending on the publicity of the incident. We can say that at this stage such leaks are becoming increasingly dangerous for the economic security of the company.

On the other hand, the analytical center's research showed that in most cases the data leak was simply due to lack of qualifications (83.9%), i.e. it was not accompanied by further use of compromised information for fraud, personal gain, abuse of access rights. The share of leaks, which were accompanied by further use of the obtained data, was only 8.5%.

Leaks also occurred through various channels. Prioritizing the channels of insider threats is important for the development of further personnel security policy. The main channels remain theft or loss of equipment, mobile devices, removable media, network, e-mail, paper documents, exchange of information notifications. In particular, the leader remains the network (browser or cloud) (72.2% in 2018), and a significant share is accounted for by e-mail (8.0% in 2018) and paper media (11.0% in 2018). Other leakage channels were mobile devices, removable media, equipment loss and messaging, although their share remains low (*Fig. 3*).

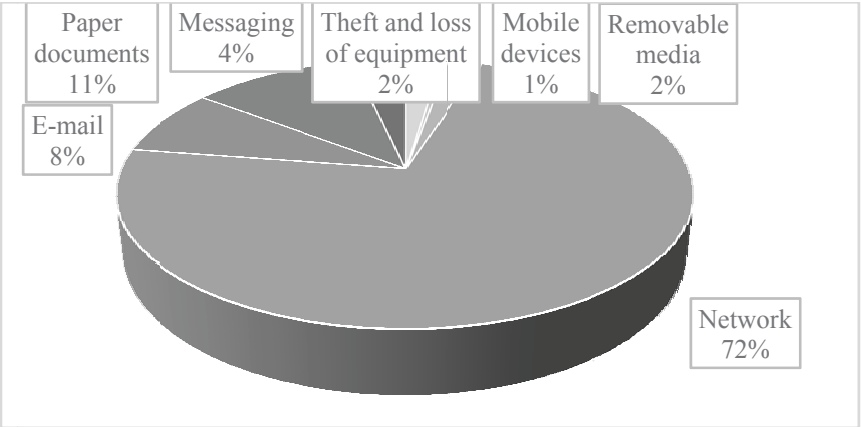

Fig. 3. **Shares of the leaks by channels in 2018**

Source: compiled by the author on the basis of [20].

On the other hand, if we consider random and intentional leaks separately, then the distribution is somewhat different. Although the network remains the leader for accidental leaks (55%), e-mail (15.9%) and paper media (17%) also account for a significant share. Instead, for intentional leaks, the main channel is the network (86.6%), while the other channels are secondary.

If we consider the areas of activity that were most vulnerable to the leaks, the leaders are high-tech companies and medical institutions, while the most protected here were companies in the field of HoReCa, industrial and transport companies (*Fig. 4*).

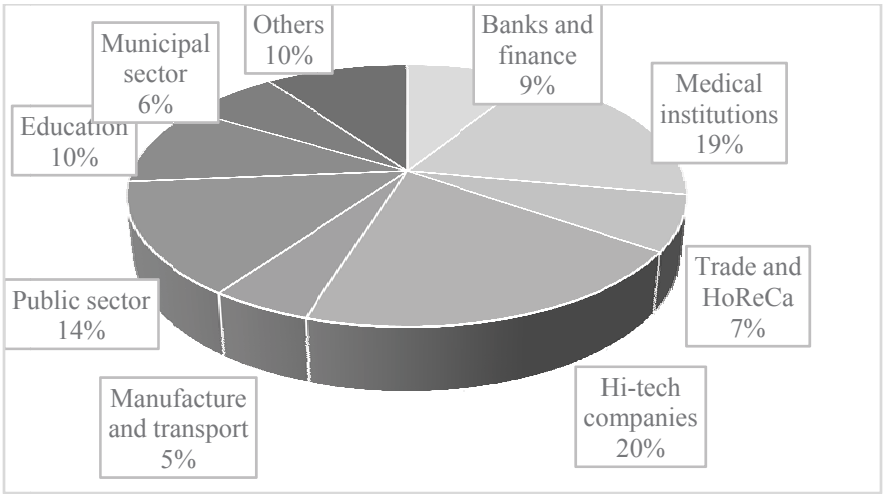

Fig. 4. **Shares of the leaks by industries in 2018**

Source: compiled by the author on the basis of [20].

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

It should be noted that such a distribution is quite natural. The attractiveness of the industry is determined by the relative liquidity of the data held by companies in this sector.

Attackers aim for quick profit, so they choose the least secure and most liquid data. Thus, it is possible to determine the attractiveness of the industry for leaks, which can be calculated as the proportion of intentional leaks in the industry in the total number of leaks (*Fig. 5*).

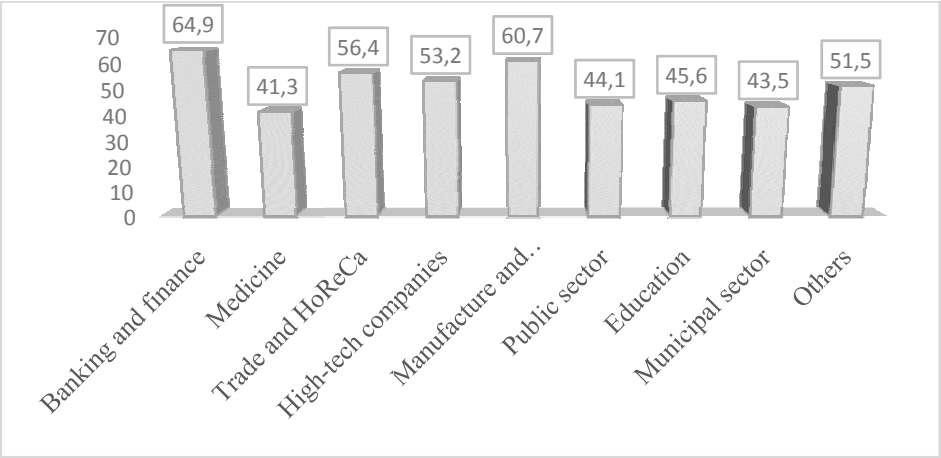

Fig. 5. **Shares of the intentional leaks of data in the total number of leaks by sector in 2018**
Source: compiled by the author on the basis of [20].

According to this distribution, it can be seen that the leaders were such sectors as banking and finance, industry and transport, trade and services, as well as high-tech companies.

Conclusions. Information leaks are a serious threat to the company's economic and personnel security. At present, firms have significant improvements and effective procedures for counteracting external threats, however, protection against insider attacks remains rather low. In the course of the research, the concept of an insider attacker was defined, the types of insider threats were established, and the main actions of the personnel prior to the insider attack were outlined.

It was determined that the degree of insider threat is determined by the type of activity of the company and the liquidity of information that may be leaked. Most leaks are observed in high-tech companies and medical institutions, while the most liquid is the information of banks, financial institutions, industrial and commercial companies.

In the future, to determine the level of awareness of Ukrainian companies about insider threats, we propose to conduct a survey among heads of security offices or senior managers of companies in Ukraine responsible for information and personnel security, which will determine the level of insider threats to economic security of these companies.

Література

1. Homoliak I., Toffalini F., Guarnizo J., Elovici Y., Ochoa M. Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*. 2019. № 52 (2). P. 1—40.
2. Costa D. L., Albrethsen M. J., Collins M. L. *Insider threat indicator ontology* (№ CMU/SEI-2016-TR-007). Pittsburgh : Carnegie-Mellon University, 2016.
3. Whitty M. T. Developing a conceptual model for insider threat. *Journal of Management & Organization*. 2018. P. 1—19.
4. Agrafiotis I., Erola A., Goldsmith M., Creese S. Formalising Policies for Insider-threat Detection: A Tripwire Grammar. *JoWUA*. 2017. № 8 (1). P. 26—43.
5. Mahajan A., Sharma S. The malicious insiders threat in the cloud. *International Journal of Engineering Research and General Science*. 2015. № 3 (2). P. 245—256.
6. Sanzgiri A., Dasgupta D. Classification of insider threat detection techniques. *Proceedings of the 11th annual cyber and information security research conference.* 2016, April. (pp. 1—4).
7. Kont M., Pihelgas M., Wojtkowiak J., Trinberg L., Osula A. M. Insider threat detection study. *NATO CCD COE.* Tallinn, 2015.
8. Ring M., Wunderlich S., Grüdl D., Landes D., Hotho A. A toolset for intrusion and insider threat detection. *Data Analytics and Decision Support for Cybersecurity*. Cham : Springer, 2017. P. 3—31.
9. Park W., You Y., Lee K. Detecting potential insider threat: Analyzing insiders' sentiment exposed in social media. *Security and Communication Networks*. 2018.
10. Gavai G., Sricharan K., Gunning D., Hanley J., Singhal M., Rolleston R. Supervised and Unsupervised methods to detect Insider Threat from Enterprise Social and Online Activity Data. *JoWUA*. 2015. № 6 (4). P. 47—63.

11. Elifoglu I. H., Abel I., Taşseven Ö. Minimizing insider threat risk with behavioral monitoring. *Review of Business*. 2018. № 38 (2). P. 61—73.
12. Eggenschwiler J., Agrafiotis I., Nurse J. R. Insider threat response and recovery strategies in financial services firms. *Computer Fraud & Security*. 2016. № 11. P. 12—19.
13. Clarke K., Levy Y., Dringus L., Brown S. How workplace satisfaction affects insider threat detection as a vital variable for the mitigation of malicious cyber insiders. *Online Journal of Applied Knowledge Management*. 2019. № 7 (1). P. 40—52.
14. Linkov I., Poinsatte-Jones K., Trump B. D., Ganin A. A., Kepner J. Rulemaking for insider threat mitigation. *Cyber resilience of systems and networks*. Cham : Springer, 2019. P. 265—286.
15. Scherer C. P., Ruggiero C. E. Overview of Tools for Insider Threat: Analysis and Mitigation (№ LA-UR-19-22069). Los Alamos : Los Alamos National Lab., United States, 2019.
16. Ismail W. B. W., Yusof M. Mitigation strategies for unintentional insider threats on information leaks. *International Journal of Security and Its Applications*. 2018. № 12 (1). P. 37—46.
17. Abd J. J., Hassan H. Protecting trade secret from theft and corporate espionage: some legal and administrative measures. *International Journal of Business & Society*. 2020. № 21.
18. Ho S. M., Kaarst B. M., Benbasat I. Trustworthiness attribution: Inquiry into insider threat detection. *Journal of the Association for Information Science and Technology*. 2018. № 69 (2). P. 271—280.
19. Butkevičius R. Universal Model of Lost Profits Calculation. *Ekonomika (Economics)*. 2019. № 98 (2). P. 97—111.
20. InfoWatch. A Study on Global Data Leaks in 2018. 2019. URL : https://infowatch.com/sites/default/files/report/analytics/Global_Data_Breaches_2018.pdf (date of access: 27.07.2020).

Статтю рекомендовано до друку 26.01.2021

References

1. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52* (2), 1—40.
2. Costa, D. L., Albrethsen, M. J., & Collins, M. L. (2016). Insider threat indicator ontology (№ CMU/SEI-2016-TR-007). Pittsburgh: Carnegie-Mellon University, 2016.
3. Whitty, M. T. (2018). Developing a conceptual model for insider threat. *Journal of Management & Organization*, 1—19.
4. Agrafiotis, I., Erola, A., Goldsmith, M., & Creese, S. (2017). Formalising Policies for Insider-threat Detection: A Tripwire Grammar. *JoWUA*, *8* (1), 26—43.
5. Mahajan, A., & Sharma, S. (2015). The malicious insiders threat in the cloud. *International Journal of Engineering Research and General Science*, *3* (2), 245—256.
6. Sanzgiri, A., & Dasgupta, D. (2016, April). Classification of insider threat detection techniques. *Proceedings of the 11th annual cyber and information security research conference.* (pp. 1—4).
7. Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A. M. (2015). Insider threat detection study. *NATO CCD COE.* Tallinn.
8. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2017). A toolset for intrusion and insider threat detection. *Data Analytics and Decision Support for Cybersecurity*. Cham: Springer.
9. Park, W., You, Y., & Lee, K. (2018). Detecting potential insider threat: Analyzing insiders' sentiment exposed in social media. *Security and Communication Networks*.
10. Gavai, G., Sricharan, K., Gunning, D., Hanley, J., Singhal, M., & Rolleston, R. (2015). Supervised and Unsupervised methods to detect Insider Threat from Enterprise Social and Online Activity Data. *JoWUA*, *6* (4), 47—63.
11. Elifoglu, I. H., Abel, I., & Taşseven, Ö. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of Business*, *38* (2), 61—73.
12. Eggenschwiler, J., Agrafiotis, I., & Nurse, J. R. (2016). Insider threat response and recovery strategies in financial services firms. *Computer Fraud & Security*, *11*, 12—19.
13. Clarke, K., Levy, Y., Dringus, L., & Brown, S. (2019). How workplace satisfaction affects insider threat detection as a vital variable for the mitigation of malicious cyber insiders. *Online Journal of Applied Knowledge Management*, *7* (1), 40—52.
14. Linkov, I., Poinsatte-Jones, K., Trump, B. D., Ganin, A. A., & Kepner, J. (2019). Rulemaking for insider threat mitigation. *Cyber resilience of systems and networks*. Cham: Springer.
21. Scherer, C. P., & Ruggiero, C. E. (2019). Overview of Tools for Insider Threat: Analysis and Mitigation (№ LA-UR-19-22069). Los Alamos: Los Alamos National Lab., United States.
15. Ismail, W. B. W., & Yusof, M. (2018). Mitigation strategies for unintentional insider threats on information leaks. *International Journal of Security and Its Applications*, *12* (1), 37—46.
16. Abd J., J., & Hassan, H. (2020). Protecting trade secret from theft and corporate espionage: some legal and administrative measures. *International Journal of Business & Society*, *21*.
17. Ho, S. M., Kaarst B. M., & Benbasat, I. (2018). Trustworthiness attribution: Inquiry into insider threat detection. *Journal of the Association for Information Science and Technology*, *69* (2), 271—280.
18. Butkevičius, R. (2019). Universal Model of Lost Profits Calculation. *Ekonomika (Economics)*, *98* (2), 97—111.
19. InfoWatch. (2019). A Study on Global Data Leaks in 2018. *infowatch.com.* Retrieved from https://infowatch.com/sites/default/files /report/analytics/Global_Data_Breaches_2018.pdf.

The article is recommended for printing 26.01.2021

 ISSN 2306-4994 (print); ISSN 2310-8770 (online)