International Journal of Engineering & Technology, 7 (4.8) (2018) 856-859

International Journal of Engineering & Technology

Website:www.sciencepubco.com/index.php/IJET

Research paper

Information Systems Protection in Financial Institutions

Svitlana Onyshshenko[1], Svitlana Sivitska[2], Olena Shapovalova[3], Anna Cherviak[4]*

[1]Poltava National Technical Yuri Kondratyuk University
[2]Poltava National Technical Yuri Kondratyuk University
[3]Ukrainian State Center for International Education at Ministry of Education and Science of Ukraine
[4]Poltava National Technical Yuri Kondratyuk University
**Corresponding author E-mail: anncherviak@gmail.com*

Abstract

Information security is of great importance for the vital interests of any state. Creation of a developed and protected environment is an indispensable condition for the development of society and the state, which should be based on the latest automated technical means. Because for the prompt execution of transactions, all services may be carried out through the Internet.
Every day, the most pressing problem is the protection of information. Because the different areas of our lives are computerized, they have a wider range of viruses and unauthorized penetration. In order to counter external attacks, it is necessary not only to have effective protection tools, but also to know their system of work, settings and weaknesses of operating systems.
Knowledge of the basics of information security, the ability to effectively prevent the leakage of information is particularly valuable at present due to the fact that there is an acute shortage of skilled professionals in the market.
The basic concepts, structure and features of information technologies functioning in financial institutions operating are investigated. Unauthorized access possible types analysis to the institution information carried out. Methods and mechanisms financial institution information systems effective protection analysis is carried out.

***Key words**: information security, information technology, financial institution, fraud unauthorized access.*

1. Introduction

Financial institutions in the system of providing their activities use only advanced software, advanced technologies and technical equipment in their work. All these factors serve as a guarantee for reliable operation in the key sector of the organization's successful activity what are information activities. Automated information systems are characterized by extremely prompt and precise work, which helps to increase market participant economic activity management and results level.
However, financial institutions information systems have extensive spheres influence on them. With information and technological environment development, not only services and programs variety in the information sector but also threats types increase. Currently, all financial institutions must provide their information security by introducing the latest technologies into the security system. The urgency of this issue lies in the fact that enabling financial institutions stable operation is development important component not only a separate branch, but the economy as a whole.
Recent research and publications analysis. The issue of financial institution information security e is devoted to scientific works of such scientists as Baranovsky O.I., Melnyk O. O., Koyda P.M., Koyda O.P., Grinova V.M., Lepekiko T.I., Vasiltsev T. G. and others. However, there is almost no non-bank financial institutions information security analysis. Therefore, an important issue is analysis and threats identification unified system formation, which would be expedient for use by both banking and non-banking institutions.

2. Main body

Economics in the modern digital age is impossible without information. Enterprises, financial institutions, taxpayers, and many other market entitities are information flows that need not only to be processed and evaluated but also protected by effective information systems.
Financial institution financial security is a complex system that can only be achieved after all elements interaction (Fig. 1).
Information is one of the most important strategic resources that provides institution development. That is why, like other resources, it needs special protection.
Most financial institutions do not have an integrated system for protecting their information resources. Creating such a system is a long and financially costly process, but without safety of information security, the institution suffers significantly more damage.
Today, at constant rates of information technologies development, all operations directly or indirectly relate to the institution information systems. Any information provided its authenticity and uniqueness has its value, therefore, must be securely protected.
The Law of Ukraine "On the Protection of Information in Information and Telecommunication Systems" [1], the Regulations "On Technical Protection of Information in Ukraine" [2] and the Criminal Code of Ukraine [3] provide for administrative and criminal liability for information crimes.
The Integrated Information Protection System (hereinafter referred to as the "IIPS") is a set of organizational and engineering-technical measures aimed at protecting information from disclosure, leakage and unauthorized access [4].

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

According to Volodymyr Libman, an expert in Cisco's information security industry, IT security professionals must invest more in their organizations' protection. They rely on automation, machine learning and artificial intelligence. Most organizations use behavioral analytics to detect attacks and minimize their consequences [5].

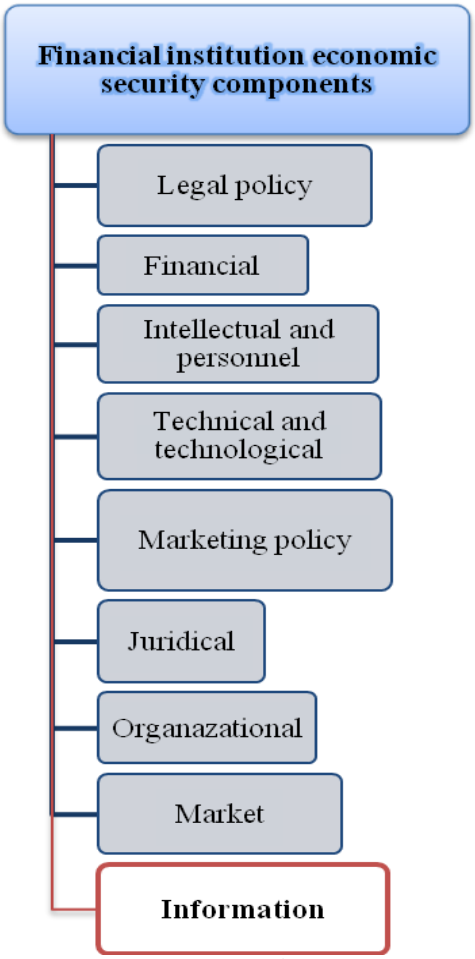


Fig. 1: Financial institution financial security components

According to an expert, organizations increasingly rely on cloud storage. Today, 53% of the company manages more than half of its infrastructure through clouds, as it provides benefits such as better security (57%), scalability (48%), easy usage (46%) and resource savings (41%). [5].

Many government agencies (tax, antimonopoly, law enforcement agencies, etc.), when performing their functions, receive from a variety of organizations or individuals a significant amount of information that forms Internet crime various mechanisms: computer viruses spread, internet fraud, theft of funds, attacks on the network, obscene data distribution [6].

In fig. 2, according to data [7], there are information security systems that provide security for the financial institution.

In financial institutions, there are two approaches to protecting information:

- Autonomous - directed towards the protection of a particular site or part in the information system, which is usually the most vulnerable or may be a source of abuse.
- Integrated - protects the information system as a whole, all its components, premises, staff, etc. [8].

In order to integrate the information security of the institution, it is necessary to implement measures that will constantly monitor the information system and activate in the immediate commission of unlawful actions.

The universal protection, which monitors the system, analyzes all authorizations in the system of the institution, conducts operations and analyzes the rejected operations (whether the transaction was executed and canceled by the actual employee of the company or whether an information crime was committed to check the response rate of the security system), should constantly work.

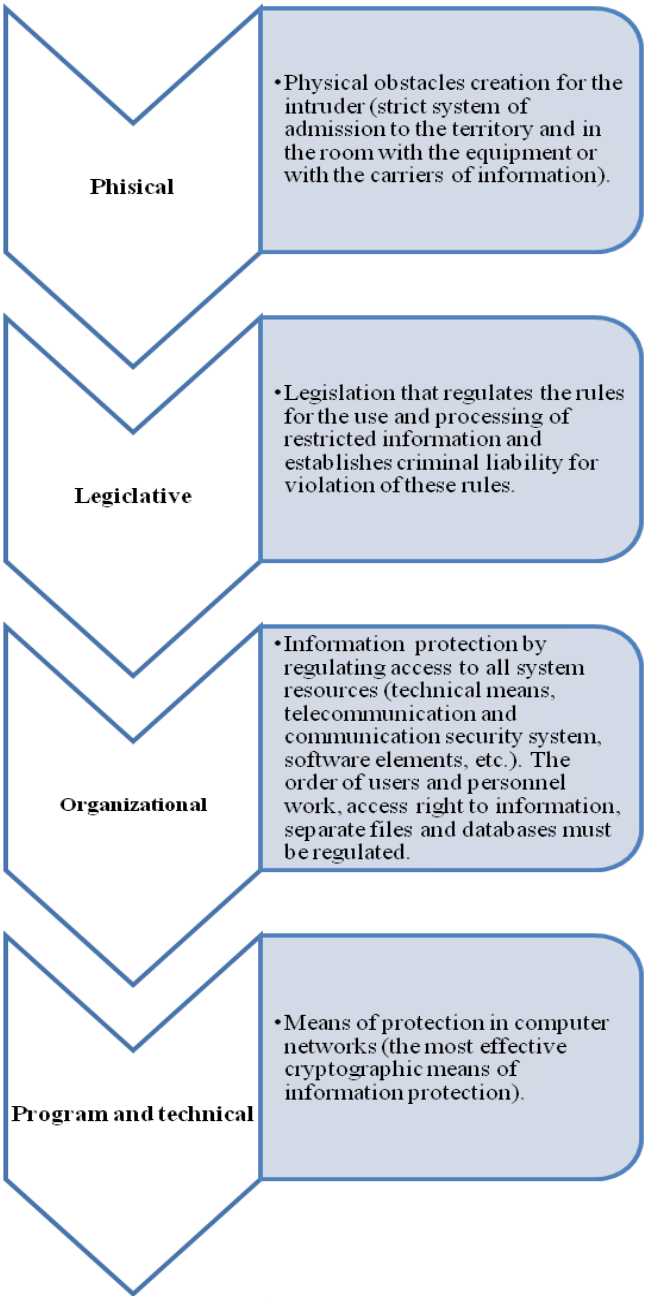


Fig. 2: Information security systems

Accordingly, when identifying unlawful actions on one of the links of the system functioning at the institution activated individual protection. It provides for the cancellation of the relevant operations, termination of the server's activity with the information and blocking the last data revenues.

The integrated defense system should combine the uninterrupted work of universal and individual protection with elements of statistical analysis of unauthorized access not only in this company but also in the overall financial institutions of the country. With the help of a global analysis of the attacks, you can trace and predict the specificity of the action that the agency's sector of activity is targeting unauthorized access. With the help of the obtained data it is necessary to strengthen the methods of protecting information systems in the relevant sector.

In the strategy of protecting computer networks from unauthorized access to information systems, special attention is paid to ensuring the security of the borders on the side of access to the Internet.

Programs of protection of computer systems from the influence of the Internet network are called antivirus programs - a program that detects and neutralizes computer viruses.
The most common antivirus programs in include [9]:

- Eset NOD32 Antivirus.
- Norton AntiVirus.
- Kaspersky Anti Virus
- Ad-Aware
- Panda Antivirus Pro
- Avast.
- Panda Cloud Antivirus.
- Security Essentials.
- Emsisoft Anti-Malware.
- PC Tools AntiVirus Free.
- Avira AntiVir Personal.
- AVG Anti-Virus Free.
- PC Tools ThreatFire.
- Zillya!.

For example, in 2017, a powerful cyber attack on computers with a Petya virus encryption was implemented. According to ESET [10], antivirus software development company, Ukraine accounted for 75.2% of the total number of infections in the world. Germany - 9%, Poland - 5,8%. Only 0.8% came to Russia (Fig. 3).

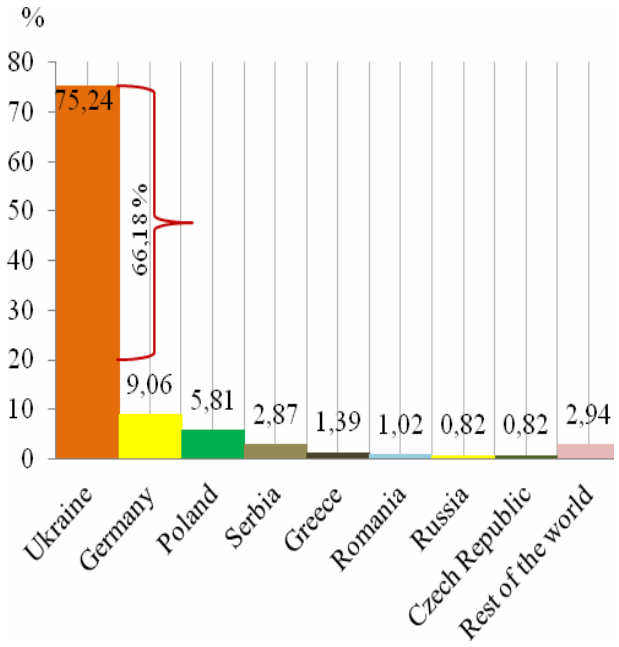


Fig. 3: Types of fraud that is characteristic for banks

In the results of the analytical data obtained, the cyber security of Ukraine needs to be improved and updated not only in the sphere of ensuring the penetration of viruses to databases but also prompt response to the penetration of the virus in the network of institutions.
How to protect yourself as for ESET [10]:

- Use reliable antimalware software: This is a basic but critical component. Just because it's a server, and it has a firewall, does not mean it does not need antimalware. It does! Always install a reputable antimalware program and keep it updated.
- Make sure that you have all current Windows updates and patches installed
- Run ESET's EternalBlue Vulnerability Checker to see whether your Windows machines are patched against EternalBlue exploit, and patch if necessary.
- For ESET Home Users: Perform a Product Update.
- For ESET Business Users: Send an Update Task to all Client Workstations or update Endpoint Security or Endpoint Antivirus on your client workstations.

Activities of banking institutions are different from non-bank financial institutions. Therefore, in the banking sector there are types of fraud with information systems and reading of information that is characteristic only for them are in fig. 4.

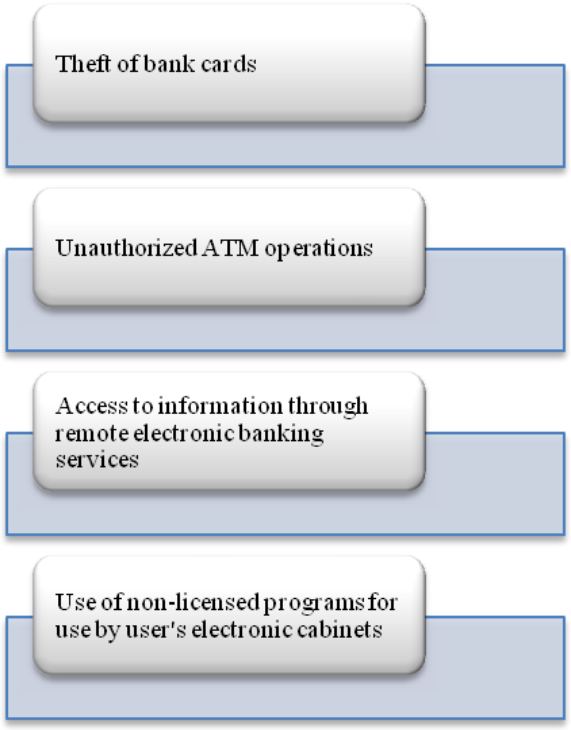


Fig. 4: Types of fraud that is characteristic for banks

The most important security requirements that should be implemented in electronic document management systems are the following:
- Authentication and authorization - checking the claimed identity and granting access rights;
- Integrity - supporting data integrity and detecting changes;
- Confidentiality - data cannot be passed on to unauthorized persons or systems;
- Non-contradiction - the verifier can obtain evidence that confirms data integrity and origin;
- Approval - receipt, registration, tracking of informed consent of the patient to access his medical data;
- Audit - all actions must be recorded in chronological order [12].

Cyber attacks can have indirect influence on activity of financial institution. So, for example, it has been carried out cyber attacks to various industries. They in turn had failure in work or in general the terminations of activity for some time that couldn't but affect activity of financial intermediaries. According to the published international data only as of September 2017 year, 12 industries became the victims of cyber attacks (Fig. 5).
This statistic presents a ranking of the industries most commonly impacted by cyber attacks worldwide as of September 2017. During the survey, 26 percent of respondents from the energy sector stated that their company had been victim of cyber attacks in the past 12 months [13].

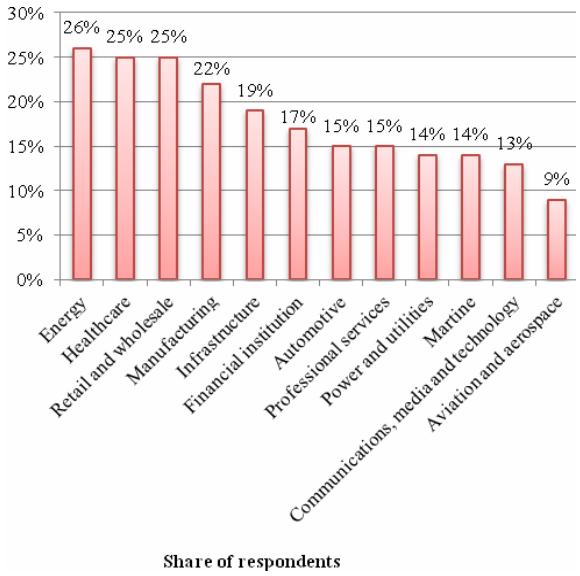


Fig. 5: Industries impacted by cyber attacks worldwide as of September 2017
*Compiled by the authors according to [13]

One more source of penetration into information systems of financial institutions of the program, search engines, e-mail and social networks. That is, all browsers which demand connection in the Internet. Considering information technology development each employee of any finance company uses such networks. Confirmation of danger in use of these such programs data of the Statistics Portal. Information at table 1 presents a selection of the biggest online data breaches worldwide as of September 2018, ranked by number of records stolen.

Table 1: Number of compromised data records in selected data breaches as of September 2018 (in millions)

Program	Millions
Yahoo	3000
River City Media	1370
Aadhar	1000
MySpase	427
Friend Finder Network Inc	412
US Voter database	191
Adobe	152
eBay	145
Equifax	143
Heartland	130
Linkedln	117
VK	100
AOL	92
MyHeritage	92
Facebook	87

*Compiled by the authors according to [13]

To determine the information system protection degree, one can conduct a stress test at a financial institution without first informing the employees. In such circumstances, it will be possible to assess the coherence and responsiveness of the threat response, taking into account the human and technical factors.
Before stress testing you can include:
- Viral links to the most used Web site employees;
- Simulation of cyber-attacks with the passage to different levels of information systems protection;
- Unauthorized entry into the premises (at the stage of passing the security and to the server organization);
- The possibility of fraudulent access to information through cooperation with employees;
- Study of employee response to spam from mobile applications;
- Analysis of the quality of verification of identity documents of persons who do not work in an institution but were called to perform the relevant work.

It can also be conducted a survey of staff and clients on information security issues of the financial institution. Only direct participants in financial transactions will be able to evaluate the quality of the work performed and make optimization suggestions.

3. Conclusions

Information security is an integral part of a comprehensive system of economic security at a financial institution. Reliable protection of information resources is a prerequisite for the development of an institution, maintaining competitiveness and maintaining its economic security.
Information security of financial institutions is an integral part of information security of the country [14] and it is not so broad definition. However, analyzing the foregoing, one can say that the information security of a financial institution is a state of security of information and data about clients and employees of the institution, which should be systematically provided with obtaining reliable and complete data that is carefully scrutinized, limited access, effective antivirus and unauthorized access blocking .
To date, there are many fraudulent operations, unauthorized access and manipulative actions to obtain confidential information from the institution. That is why it is impossible to secure the financial security of a financial institution without proper protection and constant improvement of the information protection system.

References

[1] Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh", Zakon Ukrainy, available online: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
[2] "Pro tekhnichnyi zakhyst informatsii v Ukraini", Polozhennia, available online: http://zakon3.rada.gov.ua/laws/show/1229/99
[3] Kryminalnyi kodeks Ukrainy, available online: http://zakon5.rada.gov.ua/laws/show/2341-14
[4] Vinnytskyi apeliatsiinyi administratyvnyi sud, available online: http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/
[5] "Multymediina platforma inomovlennia Ukrainy", Ukrinform, available online: https://www.ukrinform.ua/rubric-technology/2418011-kilkist-hakerskih-atak-v-ukraini-za-rik-zrosla-vdesatero.html
[6] Kavun S.V., Holubiev V.O. "Analiz kiberzlochynnosti u sferi ekonomichnoi bezpeky", Naukovi pratsi. Kompiuterni tekhnolohii, Vol 229, (2013), pp. 9-13
[7] Kozachenko I.P., Holubiev V.O. "Zahalni pryntsypy zakhystu informatsii v bankivskykh avtomatyzovanykh systemakh", Information Security Center, available online: http://www.bezpeka.com/ru/lib/spec/infsys/art92.html
[8] Metody zakhystu informatsii v korporatyvnykh IS, available online: http://www.rusnauka.com/16_NPRT_2014/Tecnic/12_171491.doc.htm.
[9] Antivirus programs and their types, available online: http://vadimkoshka.blogspot.com
[10] ESET researchers unmask sophisticated "greyenergy" cyber-espionage group, available online: https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/
[11] Bezshtanko D.V. "Informatsiina bezpeka banku v systemi upravlinnia informatsiinym ryzykom", (2012), available online: http://fkd.org.ua/article/download/28875/25883.
[12] Bernaz-Lukavetska O. M. "Informatsiina bezpeka finansovykh ustanov available online: http://dspace.onua.edu.ua/bitstream/handle/11300/9896/Bernath-Lukavezka%20Tom%202_2017-196.pdf?sequence=1&isAllowed=y.
[13] The Statistics Portal, c https://www.statista.com/statistics/784590/cyber-attacks-on-industries-worldwide-2017/.
[14] "On the Doctrine of Information Security of Ukraine", Decree of the President of Ukraine, available online: http://zakon.rada.gov.ua/laws/show/514/2009
[15] Onishchenko, S., Matkovskyi, A., & Puhach, A. (2014). Analysis of threats to economic security of ukraine in conditions of innovative economic development. Economic Annals-XXI, 1-2(2), 8-11.