004.056.5:336.7

RISCURILE DE SECURITATE CIBERNETICĂ ALE INSTITUȚIILOR FINANCIARE ȘI METODELE POSIBILE DE ELIMINARE A ACESTORA*

Conf. univ. dr. Andrei PETROIA, ASEM
petroia5@hotmail.com
Cercetător independent Ivan BANU,
„Illumax studio" SRL, RM
ivezdehod@gmail.com

Studiul examinează problemele ce țin de utilizarea tehnologiilor informaționale în sfera organizațiilor financiare. În plus, autorii examinează sursele riscurilor de securitate cibernetică în aceste organizații și mecanismele de influenţare a consecințelor manifestării lor asupra principalelor riscuri financiare.

Drept rezultat al cercetării efectuate, autorii au citat domenii-cheie de activitate, care vizează reducerea riscurilor de securitate cibernetică și care sunt legate de elaborarea și crearea controlului intern, și utilizarea instrumentelor de securitate internă, cum ar fi utilizarea instrumentelor fizice de protecție a informațiilor, instrumentelor electronice de bază pentru protecția informațiilor și utilizarea criptării datelor în timpul transmiterii informațiilor în format electronic (protecție end-to-end), precum și alte metode de minimizare a riscurilor.

Cuvinte-cheie: *tehnologii informaționale, risc de securitate cibernetică, riscuri financiare, mijloace de asigurare a securității interne.*

JEL: D81, G32, K24, L86, O32.

Introducere

Actualitatea temei. Informaţia constituie componenta importantă a vieţii socio-economice, prin intermediul căreia se acumulează toate tipurile de resurse, chiar şi resursele financiare, reprezentând, de fapt, fundamentul şi motivaţia, pe care este constituită societatea. În această ordine de idei, protejarea informaţiei reprezintă una din cele mai importante sarcini pentru instituţiile financiare.

004.056.5:336.7

THE RISKS OF CYBERSECURITY OF FINANCIAL INSTITUTIONS AND POSSIBLE METHODS FOR THEIR ELIMINATION*

Assoc. Prof., PhD Andrei PETROIA, ASEM
petroia5@hotmail.com
Independent researcher, Ivan BANU,
"Illumax studio" LTD, RM
ivezdehod@gmail.com

The study addresses issues related to the use of information technology in the field of financial organizations. In addition, the authors considered the sources of cybersecurity risks in these organizations and the mechanisms of the impact of their consequences on the main financial risks.

As a result of the study, the authors cited key activities aimed at reducing cybersecurity risks and related to the development and creation of internal controls and the use of internal security tools, such as the use of physical information protection tools, basic electronic information protection tools, the use of data encryption during transmission information in electronic format (end-to-end protection), as well as other methods to minimize risks.

Keywords: *information technology, cybersecurity risk, financial risks, internal security tools.*

JEL: D81, G32, K24, L86, O32.

Introduction

Topicality of the theme. Information is an important component of the socio-economic life, through which all types of resources are accumulated, even financial resources, representing in fact the foundation and motivation, on which the society is constituted. In this sense, protecting information is one of the most important tasks for financial institutions.

Purpose of the research. Illustration of the nature of cyber security risks of the financial insti-

* Lucrarea a fost prezentată în cadrul Conferinței Științifico-Practice Internaționale „Controlul intern în cadrul instituţiilor financiare în contextul noului cadru de reglementare şi al provocărilor tehnologice", 22-23 martie 2019/ The paper was presented at the International Scientific and Practical Conference "Internal Control in Financial Institutions in the Context of the new Regulatory Framework and Technology Challenges", 22-23 March 2019.

Scopul cercetării constă în ilustrarea naturii riscurilor de securitate cibernetică ale instituțiilor financiare, prezentarea metodelor posibile de eliminare a acestora, precum şi formularea unor aprecieri şi concluzii referitoare la tema dată.

Sarcinile cercetării rezidă în fundamentarea esenței noțiunii de risc de securitate cibernetică, evidențierea surselor riscurilor de securitate cibernetică în organizațiile financiare, precum şi mecanismelor de influențare a consecințelor manifestării lor asupra principalelor riscuri financiare.

Obiectul investigat. Obiectul de cercetare, în cadrul studiului, îl constituie riscul de securitate cibernetică examinat în parte pe tipuri ale acestuia.

Noutatea ştiinţifică constă în sistematizarea aspectelor teoretice şi practice în ceea ce priveşte riscurile de securitate cibernetică în organizațiile financiare.

Baza informaţională. Ca surse de informaţii servesc bazele de date din Internet, precum şi alte surse electronice ce relatează subiectul supus cercetării.

Metode aplicate

În vederea elaborării prezentului studiu, s-a recurs la diverse metode, precum: studierea literaturii domeniului de cercetare, numeroaselor surse de informare (dintre cele mai cunoscute fiind constatările experţilor şi studiile de specialitate), procedeelor şi instrumentelor de cunoaştere ştiințifică a proceselor economice, precum analiza logică şi comparativă.

Rezultate obţinute şi discuţii

1. Neglijarea securității cibernetice ca risc care necesită atenție specială

Există numeroase mecanisme de gestionare a sistemului intern de securitate cibernetică, ce se raportează la elaborarea şi crearea de mijloace de control asupra instrumentelor de asigurare a securităţii.

În anii următori, există probabilitatea ca gestionarea riscului în domeniul securității cibernetice să necesite o schimbare radicală în activitățile instituțiilor financiare, astfel încât acestea să se simtă protejate.

Cybersecuritatea reprezintă un set de instrumente: strategii, principii de asigurare a securităţii, garanţii de securitate, abordări de gestionare a riscurilor, instruire profesională, experiență practică, asigurări şi tehnologii, care pot fi utilizate pentru protejarea sferei cibernetice, resurselor organizației şi ale utilizatorilor. Resursele organizației şi ale utilizatorilor includ dispozitive informatice conectate, personal, infrastructură, aplicații, servicii, sisteme de telecomunicații şi tutions, as well as presentation of possible methods of eliminating them, formulation of appraisals and conclusions regarding the given topic.

Tasks of research. Foundation of the concept essence of cyber security risk, highlighting the sources of cyber security risks in financial organizations and mechanisms to influence the consequences of their manifestation on the main financial risks.

Object of investigation. The research object in the study is the risk of cyber security examined in part by its types.

Scientific novelty consists in systematizing the theoretical and practical aspects regarding cyber security risks in financial organizations.

Information base. As sources of information serve the Internet database, as well as other electronic sources that report the investigated subject.

Structure of the work. The paper is composed of the introduction, the basic chapter with three sub-chapters, conclusions and bibliography.

Applied methods

In order to elaborate the present study, various methods were used, such as: studying the literature in the research field; numerous sources of information, the most known being the findings of experts and specialized studies; the procedures and tools for scientific knowledge of economic processes, such as logical and comparative analysis.

Obtained results and discussions

1. Neglect of cybersecurity as a risk requiring special attention

There are many mechanisms for managing the internal cybersecurity system aimed at developing and building security controls.

In the coming years, cybersecurity risk management is likely to require a radical change in the activities of financial institutions in order to make them feel secure.

Cybersecurity is a set of tools, strategies, principles of security, security guarantees, risk management approaches, training, practical experience, insurance and technologies that can be used to protect the cybersphere, organization and user resources. Organization and user's resources include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the entire set of transmitted and / or stored information in the cybersphere [1].

To meet the needs of financial institutions and improve intrastructural communication, online solutions are increasingly integrated into

întregul set de informații transmise și/sau stocate în sfera cibernetică [1].

Pentru a răspunde cerințelor din cadrul activității instituțiilor financiare și a crește eficiența comunicării intra-structurale, soluțiile online sunt, din ce în ce mai des, integrate în rețelele interne ale instituției, ceea ce, desigur, creează un grad suplimentar de comoditate de utilizare, dar implică o serie de vulnerabilități pentru cyber-criminali. Acest lucru este confirmat de numeroase studii efectuate la nivel mondial în domeniul securității informațiilor, inclusiv un studiu realizat de Echipa de Management a Centrului Național de Răspuns la Incidente de Securitate Cibernetică în Domeniul Protejării Sistemelor de Control Industrial al Statelor Unite (ICS-CERT). Aproape toate instalațiile de infrastructură critică sunt expuse riscului.

Există două tipuri principale de amenințări la adresa securității informațiilor:

1. Încălcarea neintenționată (accidentală):
   - defecțiuni ale sistemului de securitate;
   - dezastre naturale;
   - defecțiuni ale echipamentului;
   - factorul uman.
2. Încălcarea intenționată:
   - angajați nemulțumiți;
   - spionaj industrial;
   - hackeri;
   - viruși și viermi;
   - terorism.

2. Eliminarea amenințării crescânde

Pentru a depăși amenințările, multe departamente, organizații non-profit și state, în decursul anilor, au dezvoltat diferite standarde. Există standarde elaborate pentru o țară, ținând cont de specificul acesteia și care se aplică numai pe teritoriul țării respective, dar există și standarde care sunt aplicate peste tot în lume. Standardele respective oferă îndrumări privind dezvoltarea strategiilor de apărare aprofundată (defence-in-depth) pentru organizațiile care utilizează componente de control financiar intern și conțin informații despre configurare sigură, cele mai bune practici, politici de securitate, arhitectură de rețea și proceduri de operare sigure.

Măsurile prioritare pentru combaterea amenințărilor cibernetice se raportează la partea tehnică a problemei și reprezintă investiții în măsuri de securitate, cum ar fi firewall-urile, antiviruşii și alte soluții hardware-software pentru detectarea și prevenirea intruziunilor. Cu toate acestea, există o opinie, care denotă că această problemă nu poate fi the internal networks of institutions, which, of course, create additional usability, but entail a number of vulnerabilities to cybercriminals. This is confirmed by many global researches in the field of information security, including research conducted by the US Industrial Control Systems Computer Emergency Response Team (ICS-CERT). Almost all critical infrastructure facilities are under threat.

There are two main types of information security threats:

1. Unintentional (accidental) violation:
   - Malfunctions of security systems;
   - Natural disasters;
   - Equipment failures;
   - Human factor.
2. Premeditated (intentional) violation:
   - Dissatisfied employees;
   - Industrial espionage;
   - Hackers;
   - Viruses and worms;
   - Terrorism.

2. Eliminating the increasing threat

To overcome the threats, many departments, non-profit organizations and states have been developing various standards for several years. There are standards developed for one country, taking into account its specificity, and acting only on the territory of this country, but there are also standards that are applied everywhere in the world. These standards are guidelines for developing “defence-in-depth” strategies for organizations that use internal financial control components. These standards provide information on secure configuration, best practices, security policy, secure network architecture, and secure operating procedures.

Priority measures to counter cyber threats are focused on the technical side of the problem and represent investments in such security measures as firewalls, antiviruses and other software and hardware solutions for intrusion detection. However, there is an opinion that this problem cannot be solved only at the technical and operational level, as it has now become clear that many of the above-mentioned technical solutions are ineffective or they are not enough when they are not integrated with redundancy solutions. The magnitude of the security problem can lead to stupor, but this can be avoided. In reality, there are answers, and they are based on

rezolvată doar la nivel tehnic şi operaţional, deoarece, în prezent, a devenit clar că multe dintre soluţiile tehnice, menţionate anterior, sunt ineficiente sau insuficiente, atunci când nu sunt integrate cu soluţii de rezervă. Exagerarea problemei de asigurare a securităţii poate duce la stupoare, dar acest lucru poate fi evitat. În realitate, există răspunsuri şi ele se bazează pe tehnologii, dar tehnologia este doar un instrument. Managementul este, în cele din urmă, la îndemâna oamenilor. Acest lucru înseamnă că, pentru cea mai eficientă apărare împotriva atacurilor cibernetice, o cultură de securitate trebuie să se situeze la acelaşi nivel ridicat ca şi instrumentele de securitate.

Standardele prezumă importanţa a trei factori, precum procesul în sine, tehnologiile şi oamenii. Securitatea sistemului depinde de toţi aceşti factori combinaţi:

Personalul:

Cât de strict angajaţii execută procesele?

Procesul:

Care este procedura de implementare, operare şi întreţinere a soluţiei?

Tehnologiile:

Ce funcţionalitate tehnică este încorporată în soluţia de automatizare?

Aceşti trei factori principali joacă un rol important în domeniul securităţii interne a oricărei instituţii financiare.

Fiecare sector are propriile probleme şi ameninţări, iar standardele au, de asemenea, propriile lor caracteristici. De exemplu, standardul NERC CIP (Asigurarea securităţii sistemelor informaţionale din domeniul Alimentării cu Energie Electrică a Statelor Americii de Nord împotriva atacurilor cibernetice) este aplicat în sectorul energetic. Unele standarde se aplică la nivel mondial, cum ar fi IEC 62443 (Security for Industrial Automation and Control Systems).

3. Vulnerabilităţi comune şi metode de atac

O justificare rapidă a motivelor, pentru care operatorii de infrastructură cibernetică (sau infrastructurile instituţiilor financiare) ar trebui să acorde mai multă atenţie problemei durabilităţii, poate fi făcută, dacă sunt luate în considerare cele mai cunoscute vulnerabilităţi şi metode de atacuri cibernetice, care pot afecta negativ funcţionarea continuă a sistemelor cibernetice (şi activitatea serviciilor dependente de aceste sisteme) [2].

Printre cele mai frecvente vulnerabilităţi, pot fi identificate următoarele:

- Vulnerabilităţile inerente software-ului/ hardware-ului (defecte de proiectare);

technology. But technology is only a tool. Governance is ultimately in the hands of the people. This means that for the most effective protection against cyber-attacks, a safety culture must be at the same high level as security.

Standards emphasize the importance of three factors: process, technology and people. System security depends on all these factors combined:

Staff

How strictly do employees perform processes?

Process

What is the procedure for implementing, operating and maintaining the solution?

Technologies

What technical functionality is incurporated in the automation solution?

These 3 main factors play a direct role in the internal security sphere of any financial institution.

Each sector has its own problems and threats, and standards also have their own specifics. For example, the NERC CIP (Protection of the Critical Infrastructure of the North American States for Reliable Power Supply) standard is applied in the energy sector. Some standards are applied throughout the world, such as IEC 62443.

3. Common vulnerabilities and attack techniques

Quickly justify the reasons why operators of cyber infrastructure (or infrastructure of financial institutions) should pay more attention to the issue of sustainability can be taken into account if we take into account most of the well-known vulnerabilities and methods of cyber-attacks that can adversely affect the continuous operation of cyber systems services) [2].

Among the most frequently occurring vulnerabilities can be identified such as:

- Inherent software/ hardware vulnerabilities (design flaws);
- Lack of (physical and logical) protection measures;
- "Vulnerabilities of Zero Day";
- Incorrect configuration/ incompatibility of system components;

- Lipsa măsurilor de protecție (fizice și logice);
- „Vulnerabilitățile de Zero Day";
- Configurarea incorectă/ incompatibilitatea componentelor sistemului;
- Lipsa actualizărilor sau testarea inadecvată a actualizărilor înainte de implementare;
- Pregătirea insuficientă a administratorilor de sistem;
- Calificările inadecvate ale utilizatorilor;
- Învechirea fizică a infrastructurii sau a unor părți ale sistemelor;
- Subestimarea riscurilor rezultate din vulnerabilitatea fizică a instalațiilor, în care se află componentele sistemului cibernetic (de exemplu, expunerea la inundații, activități dăunătoare etc.).

Principalele tipuri de atacuri cibernetice includ:

- Refuzul distribuit al serviciului (DDoS);
- Intruziuni în rețea;
- Software malițios, cal troian (trojan horse), backdoor;
- Atacuri asupra anumitor utilizatori (administratori-operatori în pozițiile principale);
- Atacuri asupra anumitor echipamente/ dispozitive (de exemplu, controlere logice programabile – PLC);
- Distrugerea completă sau parțială a sistemelor (generate de incendii, explozii etc.);
- Ingineria socială;
- Insiderii.

Infractorii, de obicei, aleg organizațiile financiare cel mai puțin informate și nepregătite din punct de vedere tehnic, care nu sunt în măsură să reziste atacurilor hackerilor ca victime.

În majoritatea cazurilor, acest lucru nu necesită nicio spargere tehnică. Metodele funcționează la nivelul psihologiei. Anumite trucuri permit aflarea informațiilor pentru accesarea sistemelor financiare, pur și simplu, aranjând corect întrebări și, eventual, falsificând (fără a sparge) o scrisoare de la o bancă sau pagina unui site web, creând o copie a site-ului web cu modificarea unuia sau a mai multor caractere din numele domeniului. Acesta este phishing-ul clasic.

În același timp, instituțiile financiare nu fac decât să obțină informații din mediul public despre succesul hackerilor, deoarece acesta, întotdeauna, constă în eșecuri bancare, cu posibile riscuri suplimentare de reducere a loialității clienților, ceea ce se soldează cu pierderi financiare.

Una din posibilitățile de combatere a infracțiunilor digitale de tip phishing poate fi me-

- No updates or inadequate testing of updates before deployment;
- Insufficient training of system administrators;
- Insufficient user skills;
- Obsolescence of infrastructure or parts of systems;
- Underestimation of risks resulting from the physical vulnerability of objects in which cyber-system components are located (for example, susceptibility to flooding, malicious actions, etc.).

Among main types of cyber-attacks there can be identified:

- Distributed Denial of Service (DDoS);
- Network intrusion;
- Malicious software, Trojan horses, backdoors;
- Attacks on certain users (administrators – operators on the main positions);
- Attacks on certain equipment / devices (for example, programmable logic controllers – PLC);
- Complete or partial destruction of systems (due to, for example, fire, explosion, etc.);
- Social engineering;
- Insiders.

Scammers usually choose the least informed and technically unprepared financial institutions that are unable to resist hacker attacks.

In most cases, this does not require any technical hacking. Methods work at the level of psychology. Certain techniques allow you to find out information for accessing financial systems by simply arranging the questions correctly and, possibly, forging (not cracking) a letter from the bank or a website page, creating a copy of the website with a change in one or several characters in the domain name. This is classic phishing.

At the same time, financial organizations only as a last resort publicly announce the successes of hackers, since these are always failures of banks with possible further risks of reducing customer loyalty, which leads to financial losses.

You can fight banal phishing by either using new authentication methods: not just through the username/password, but, for example, through the application of biometrics characteristics, when a client, even a misleading one, will not be able to transfer the "access code" to the attacker, because his face, fingerprints, voice

toda de autentificare, nu doar prin nume de utilizator/ parolă, dar, de exemplu, prin aplicarea caracteristicilor biometrică, când un client, chiar cel indus în eroare, nu poate transmite „codul de acces" atacatorului, deoarece faţa, amprentele degetelor, vocea etc. reprezintă codul lui de acces. Al doilea mod de a lupta împotriva tentativelor de asemenea fraude constă în creşterea gradului de instruire a angajaţilor în domeniul securităţii informaţionale.

4. Abordarea orientată spre stabilitate şi durabilitate

Experienţa ultimilor ani şi a evenimentelor recente a relevat probabilitatea ca măsurile de protecţie să eşueze în cele din urmă. Din acest motiv şi având în vedere că măsurile de protecţie pentru infrastructurile critice pot fi evitate cu uşurinţă, toţi actorii implicaţi în asigurarea securităţii unei astfel de infrastructuri delicate şi vitale ar trebui să acorde mai multă atenţie durabilităţii infrastructurii critice.

O politică de durabilitate a cybersistemelor creată de la zero, ar trebui să se bazeze pe patru linii de apărare:

1. Prima linie de apărare se raportează la nivelul tehnic şi fizic. Elementele tradiţionale de securitate intranet, cum ar fi firewall-urile, sistemele de prevenire a intruziunilor şi protecţia antivirus sunt răspândite şi pe larg utilizate în combaterea ameninţărilor cunoscute, dar insuficiente. Aceste elemente tradiţionale ale managementului securităţii reţelei, adesea, constituie baza combaterii ameninţărilor cibernetice esenţiale şi sunt de natură preventivă.

2. A doua linie de apărare se referă la nivelul personal. Rezilienţa personală este una dintre cele mai importante componente ale durabilităţii sistemului [3].

3. A treia linie de apărare priveşte nivelul organizaţional. Izolarea componentelor individuale ale sistemului cibernetic facilitează detectarea ameninţărilor şi distrugerea promptă a acestora.

4. A patra linie de apărare constă în dezvoltarea cooperării şi a parteneriatului între diferiţi actori. În Europa, Parteneriatul public-privat european pentru îmbunătăţirea sustenabilităţii (EP3R) a fost creat pentru a dezvolta o iniţiativă politică de protejare a infrastructurii informaţionale critice, adoptată de Comisia Europeană la 30 martie 2009. Obiectivele EP3R sunt: susţinerea procesului de schimb de informaţii, acumularea de bune practici în domeniul politicii şi become his access code. The second way to fight is to increase employee literacy in the field of information security.

4. Stability and sustainability approach

The experience of past years and recent events has revealed the likelihood of protection measures eventually failing. For this reason, and given that protection measures for critical infrastructures can be easily circumvented, all stakeholders involved in ensuring the security of such sensitive and vital infrastructure facilities need to pay more attention to the sustainability of critical infrastructure.

The cyber resilience policy created from scratch should be based on four lines of defense:

1. The first line of defence is at the technical and physical level. Traditional intranet security controls such as firewalls, intrusion prevention systems, and antivirus protection are widespread and sufficient to counter known threats, but not sufficient. These traditional elements of network security controls are often the basis for countering basic cyber threats and are preventive in nature.

2. The second line of defence is on a personal level. Personal resilience is an essential component of system resilience [3].

3. The third line of defence is at the organizational level. Isolation of individual components of the cyber system facilitates the identification of threats and their rapid destruction.

4. The fourth line of defence is the development of cooperation and partnership between various stakeholders. In Europe, the European Public-Private Partnership for Sustainability (EP3R) was created to develop a policy initiative to protect the critical information infrastructure adopted by the European Commission on March 30, 2009. The objectives of the EP3R are: maintaining information sharing, accumulating best practices in politics and industry, developing a common understanding, discussing priorities, objectives and measures of public policy, increasing coherence and coordination of safety and sustainability policies in Europe, identifying good basic practices their adoption for safety and sustainability [4].

The main sources of infection of computers in the technological infrastructure of organizations are the Internet, removable media and e-mail. Despite the common opinion about the isolation of the technological network, it is the Internet that has become the main source of

industriei, dezvoltarea unei înțelegeri comune, discuția priorităților, obiectivelor și măsurilor politicii publice, îmbunătățirea coerenței și coordonării politicilor de securitate și sustenabilitate în Europa, identificarea bunelor practici de bază și promovarea adoptării lor pentru a garanta siguranța și sustenabilitatea [4].

Principalele surse de contaminare computerizată a infrastructurii tehnologice a organizațiilor sunt internetul, suporturile amovibile și poşta electronică. În ciuda opiniei frecvente despre izolarea rețelei tehnologice, anume Internetul, în ultimii ani, a devenit principala sursă de contaminare a calculatoarelor în infrastructura tehnologică a organizațiilor [5].

Există o opinie despre necesitatea introducerii unei baze de date interbancare comune privind riscurile operaționale. Astfel, fiecare bancă înregistrează orice incidente operaționale – de la scurgeri de informații până la jaful unui bancomat. După aceea, organizația financiară, întotdeauna, efectuează unele ajustări în activitatea sa, schimbă procesele de afaceri. Băncile mici au mai puțină experiență, mai puține incidente, dar riscurile lor, din cauza lipsei de informații, sunt mai mari. Pentru aceasta, este necesar să se creeze un sistem care să permită schimbul online al acestor informații. În timpul schimbului, datele personale ale băncii, clienților sau angajaților săi nu sunt dezvăluite. Prima sarcină a acestei baze o reprezintă primirea la timp a informațiilor (ceea ce este foarte important pentru atacurile cibernetice). În al doilea rând, baza de date poate deveni un instrument analitic pentru băncile mijlocii și mici. Acestea vor putea obține întreaga imagine a incidentelor operaționale din țară și vor constata cum au fost rezolvate problemele în alte instituții bancare, înlăturând prompt și adecvat dificultățile.

Concluzii

Sarcina de a asigura securitatea cibernetică a sistemelor instituțiilor financiare este destul de complexă și nu toate aspectele acesteia au fost acoperite în cadrul acestui articol. Cu toate acestea, respectarea cerințelor standardelor internaționale de securitate și utilizarea instrumentelor certificate internațional reduc semnificativ probabilitatea de atacuri cibernetice de succes și consecințele negative asupra sistemelor cibernetice.

Factorii-cheie în asigurarea securității cibernetice, în prezent, sunt depistarea rapidă a amenințărilor, prevenirea răspândirii acestora și

infection of computers in the technological infrastructure of organizations in recent years [5].

There is an opinion about the need to implement a common interbank database on operational risks. Thus, each bank records any operational incidents – from information leakage to ATM robbery. After that, the financial organization always makes some adjustments in its work, changes business processes. Small banks have less experience, fewer incidents, but their risks due to lack of information are greater. To do this, you need to create a system that allows online to share this information. When exchanging, personal data of the bank, its clients or employees are not disclosed. The first task of this database is to receive information in a timely manner (which is very important in case of cyber-attacks). Secondly, the database can become an analytical tool for an average and small bank. They will be able to get the whole picture of operational incidents in the country and see how problems were solved in other banking institutions, timely and adequately responding to the difficulties encountered.

Conclusions

The task of ensuring the cybersecurity of financial institutions is quite complex, and not all of its aspects were covered in this article. However, adherence to the requirements of international security standards and the use of internationally certified tools significantly reduce the likelihood of successful cyber-attacks and their negative consequences for cyber systems..

The key factors for ensuring cybersecurity now are the rapid detection of threats, the prevention of their spread and the minimization of negative consequences, rather than the construction of the “Maginot Line” of cyber-systems, because technologies are constantly evolving and out-dated protection methods become useless.

There are no precedents in the world yet, when a single system would be able to protect all information resources, even highly specialized ones. Cyber security is always a complex of measures; therefore it is hardly possible to speak about building some kind of centralized security system. Rather, we need a unified approach, compliance with a number of standards at all levels, starting from the state, then through the commercial sector directly for users [6].

minimizarea consecinţelor negative, mai degrabă decât construirea unei „linii Maginot” de sisteme cibernetice, deoarece tehnologiile sunt în continuă evoluţie şi metodele de protecţie depăşite devin inutile.

Nu există precedente în lume, când un singur sistem ar fi capabil să protejeze toate resursele informaţionale, chiar şi cele extrem de specializate. Securitatea cibernetică, întotdeauna, reprezintă un set de măsuri, astfel, încât nu este posibil să vorbim despre construirea unui tip de sistem de securitate centralizat. Mai degrabă, este necesară o abordare unificată, respectarea unui număr de standarde la toate nivelurile, de la stat, apoi prin sectorul comercial direct către utilizatori [6].

Bibliografie/ Bibliography:

1. Тезаурус: кибербезопасность: https://postnauka.ru/faq/83781
2. Кибербезопасность и устойчивость промышленных систем управления: https://digital.report/promyishlennye-sistemy-upravleniya/
3. ICS–CERT Incident Response Summary Report 2009-2011: https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20(2009-2011)_accessible.pdf
4. Conclusion for the European Public-Private Partnership (PPP) for Resilience scheme http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r
5. Ландшафт угроз для систем промышленной автоматизации в первом полугодии 2018 года: https://securelist.ru/threat-landscape-for-industrial-automation-systems-in-h1-2018/91496/
6. Управление рисками финансовой кибербезопасности перейдет под госконтроль? https://kursiv.kz/news/finansy/2017-11/upravlenie-riskami-finansovoy-kiberbezopasnosti-pereydet-pod-goskontrol
7. Applied Cybersecurity Handbook. European Commission Tempus Project: 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES. Version 1, May 2015. https://www.ecesm.net/default/files/Dev.2.4-v1_new.pdf
8. Cybersecurity Management Guidelines. Ver 1.1. Ministry of Economy, Trade and Industry of Japan, Independent Administrative Agency Information-technology Promotion Agency. https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guidelines_v1.1_en.pdf
9. Cybersecurity Best Practices Guide For IIROC Dealer Members. Investment Industry Regulatory Organization of Canada. https://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf
10. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC), The Government of JAPAN. September 29, 2017. https://www.nisc.go.jp/security-site/campaign/files/aj-sec/handbook-all_eng.pdf
11. Никольская К.Ю. Проблемы информационной безопасности компьютерных сетей. În: Securitatea informaţională 2018: conf. int., (ediţia a 14-a), 20-21 martie 2018 – Chişinău: ASEM, 2018, p.183-185. ISBN 978-9975-75-910-6.
12. BURUC Alexanru; NISTOR Dan. Securitatea cibernetică şi securitatea naţională. Cazul Republicii Moldova. În: *Securitatea informaţională 2013*: conf. int., 19 aprilie 2013 (ed. a 10-a jubiliară) – Chişinău, ASEM, 2013, p. 83-89. ISBN 978-9975-75-640-2.