Securitatea sistemelor informatice - pilon de bază al siguranței informaționale

Colun Tatiana
Drd, Școala Doctorală Economie, Finanțe și Management, UTM
Chișinău, Republica Moldova
coluntatiana7@gmail.com

Summary **- The modern development of information technologies leads to the need to protect information. In this article were elucidated important aspects of the security of informatics systems and information security, being at the same time argued the necessity of security of information systems, for ensuring informational safety.**

Thus, were analyzed threats, vulnerabilities, standards, security levels, as well as solutions to the security of information systems as components of a more secure information society.

Key terms **- computer system, security of information systems, information security, standard, threat, requirements.**

I. INTRODUCERE

Actualitatea temei. Societatea contemporană îmbrățișează din ce în ce mai mult tehnologia informaţiei ca factor de producție. Până nu de mult informaţia avea la bază hârtia, actualmente, aceasta, este gestionată mai mult în forma electronică. [4].

Progresele științifice și tehnologice au transformat informațiile într-un produs care poate fi cumpărat, vândut sau schimbat. Deseori, costul datelor este de câteva ori mai mare decât costul întregului sistem tehnic care stochează și procesează informații.

Având în vedere că, calitatea informațiilor comerciale asigură efectul economic necesar pentru instituții, este foarte important să se protejeze datele critice de acțiuni ilegale.

O gestiune corespunzătoare a documentelor în format electronic face necesară implementarea unor măsuri specifice. Acestea ar trebui să asigure protecția informaţiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informaţiei gestionată de sistemele informatice în noul context tehnologic al economiei contemporane[9].

Scopul lucrării constă în delimitarea noțiunilor de securitate a sistemelor informatice și securitate informațională, identificarea cauzelor şi condiţiilor care favorizează lezarea securității sistemelor informatice, în vederea elucidării recomandărilor privind măsurile de asigurare a securității sistemelor informatice, care stau la baza siguranței informaționale. Totodată, în cadrul lucrării se propune să se definească conceptul de sistem de protecție a informației computerizate, precum și de identificat pilonii care stau la baza organizării unei protecții de rigoare a sistemelor informatice.

II. DEFINIREA TERMENILOR

Pentru o mai bună percepere a tematicii abordate, este necesar definirea elementelor constitutive ale conceptelor legate de securitatea sistemelor informatice.

Un sistem informatic reprezintă un sistem care permite introducerea de date prin procedee manuale sau prin culegere automată de către sistem, stocarea acestora, prelucrarea lor și extragerea informației (rezultatelor) sub diverse forme. Componentele sistemului informatic sunt: calculatoarele, programele, rețelele de calculatoare și utilizatorii [15].

Astfel, prin securitatea sistemelor informatice se presupune protejarea împotriva furtului sau a deteriorării hardware-ului, a software-ului și a informațiilor despre acestea, precum și perturbarea sau apariția unor greșeli pentru serviciile pe care le furnizează. Acesta include controlul accesului fizic la hardware, precum și protecția împotriva daunelor care pot apărea prin accesul la rețea, prin injecții de date și de cod și datorită unei practici incorecte de către operatori, fie intenționate, accidentale, fie datorită faptului că sunt înșelătoare pentru a se abate de la proceduri sigure [1].

În urma analizei noțiunii de securitate a sistemelor informatice, se elucidează necesitatea definirii conceptului de securitate informațională.

Conform Legii Republicii Moldova privind Concepţia securităţii informaţionale, aceasta reprezintă starea de protecţie a persoanei, societăţii şi a statului, care determină capacitatea de rezistenţă la ameninţările împotriva confidenţialităţii, integrităţii şi disponibilităţii în spaţiul informaţional [6]. Securitatea informațiilor se mai referă și la confidențialitatea, integritatea și disponibilitatea informațiilor.

Din cele expuse se delimitează conceptul de sistem informatic ca parte a sistemului informațional, prin intermediul căruia se asigură prelucrarea automata a datelor, în vederea obținerii informațiilor solicitate de utilizatori.

III. PROBLEME

Odată cu dezvoltarea și extinderea sferei de aplicare a instrumentelor de tehnologie informatică, problema asigurării securității în sistemele informatice și protecția informațiilor devine acută din mai multe motive obiective.

Astfel, cu trecerea timpului se face tot mai evidentă creșterea încrederii în sistemele informatice și tehnologiile

informaționale. Aceștia sunt însărcinați cu cele mai importante sarcini, de calitatea cărora depinde viața și bunăstarea multor oameni. Sistemele informatice controlează procesele tehnologice din întreprinderi și sistemele energetice, mișcarea aeronavelor și a rachetelor, realizează operațiuni financiare și procesează informații clasificate.

Și totuși, când vorbim despre securitatea sistemelor informatice, în multe organizații există un decalaj între conștientizarea nevoilor de securitate și respectarea măsurilor de securitate. Acest fapt se explică prin însuși concepțiile greșite asupra procesului de asigurare a securității informaționale, care pot rezulta în implementarea unor soluții ineficiente.

Conform Molddata zeci de mii de atacuri cibernetice sunt lansate în fiecare secundă. Zi de zi, au loc atacuri pe Internet menite să afecteze sisteme informatice, site-uri și rețele, dar adesea este dificil de a vizualiza acest tip de activitate. Atacurile cibernetice sunt lucruri abstracte despre care auzim în timp sau după ce s-au întâmplat [5].

Analiza amenințărilor la adresa sistemelor informatice și consecințele impactului acestora arată că obiectivele lor finale sunt denaturarea informațiilor, încălcarea procedurilor de schimb de informații, precum și încălcarea procedurilor de gestionare a componentelor de rețea sau a întregii rețele

În acest sens, problema cea mai frecventă pe care aproape fiecare sistem suferă este furtul datelor sau deturnarea datelor. Se întâmplă de mult timp, dar după atacurile *Ransomware,* cum ar fi *wannacry* și *petya*, oamenii au început să ia măsuri de precauție și de securitate. Furtul de date ar putea fi cel mai rău coșmar al oricărei persoane care are sistem de calculatoare.

Potrivit unui studiu al *InfoWatch*, organizațiile rusești sunt cele mai preocupate de scurgerea informațiilor confidențiale. Aproape toți (98% dintre respondenți) pun această amenințare pe primul loc. Alte pericole ce amenință mult mai puțin sunt: 62% - denaturarea informației, 15% - eșecul sistemului de informații din cauza neglijenței angajatului, 7% - pierderea datelor, 6% - furturile echipamentelor, 28% - alte probleme [13]. Aceasta înseamnă că securitatea informațiilor este fundamentală pentru supraviețuirea orice organizație care utilizează resurse electronice de informații.

IV. IDENTIFICAREA SOLUȚIILOR

Securizarea informațiilor este vitală pentru supraviețuirea multor organizații. Prin urmare, informațiile trebuie protejate proactiv împotriva atacurilor dăunătoare. Această securizare a informațiilor devine mai complexă atunci când există astfel de informații transmise prin rețele.

Organizațiile trebuie să înțeleagă că informația este o resursă foarte valoroasă și trebuie protejată și gestionată în corespunzător.

Astăzi, problema protecției sistemelor de calcul devine și mai importantă în legătură cu dezvoltarea și distribuția rețelelor de computere personale și Internet. Sistemele și rețelele distribuite cu acces la distanță au subliniat problema protejării informațiilor transmise.

Disponibilitatea tehnologiilor informaționale a condus la creșterea numărului de specialiști în domeniu, precum și la majorarea competențelor informatice a persoanelor obișnuite.

Aceastea, la rândul său, a provocat numeroase încercări de a interveni în activitatea sistemelor de stat și comerciale. Multe dintre aceste încercări și-au atins scopurile și au cauzat pagube considerabile proprietarilor de informații din sistemele informatice.

Pentru a asigura securitatea informațiilor în sistemele informatice, este necesar să se protejeze nu numai hardware-ul, ci și software-ul acestor sisteme. Software-ul în sine este o parte a resurselor informaționale ale sistemului informatic și, respectiv, securitatea informațiilor stocate, transmise sau prelucrate, depinde în mod semnificativ dacă au fost luate măsurile de protecție corespunzătoare și compatibile cu capacitățile sistemului informatic. Astfel, pentru a proteja informațiile din sistem informatic este necesar să se protejeze hardware-ul și software-ul, de acțiuni neautorizate asupra lor.

Cele expuse mai sus ne demonstrează, că este nevoie de implementat politici de securizare a sistemelor informatice, care vor avea ca efect siguranța informației. În acest sens, o atenție deosebită trebuie de atras standardului ISO/IEC 27002/2013, care tratează securitatea informațiilor prin cele trei componente principale: confidențialitatea, integritatea și disponibilitatea. Confidențialitatea este asigurată prin criptarea informației. Integritatea se obține prin mecanisme și algoritmi de dispersie. Disponibilitatea se asigură prin întărirea securității rețelei sau rețelelor de sisteme informatice și asigurarea de copii de siguranță [10].

Nu trebuie de neglijat nici sistemul de management al securității informațiilor (ISMS), care constă dintr-un set de politici și proceduri concepute pentru a ajuta o organizație să gestioneze datele sale sensibile și este completat de două specificații suplimentare.

Prima specificație este ISO 27001, care, conform documentației, a fost concepută pentru a "oferi un model pentru stabilirea, implementarea, operarea, monitorizarea, revizuirea, menținerea și îmbunătățirea unui sistem de management al securității informațiilor" [2].

La rândul său ISO/IEC 17799 tratează securitatea informaţiilor prin prisma a trei elemente principale:

- *confidenţialitatea* – informaţiile sunt accesibile doar persoanelor autorizate;
- *integritatea* – asigurarea acurateţei şi completitudinii metodelor prin care se realizează prelucrarea informaţiilor;
- *disponibilitatea* – utilizatorii autorizaţi au acces la informaţii şi la activele asociate în momente oportune.

Pentru a putea realiza un program de securitate eficient este nevoie de politici, proceduri, practici, standarde, descrieri ale sarcinilor şi responsabilităţilor de serviciu, precum şi de o arhitectură generală a securităţii. Aceste controale trebuie implementate pentru a se atinge obiectivele specifice ale securităţii şi pe cele generale ale organizaţiei [12].

Drept urmare, conchidem că ameliorarea securității sistemelor informatice trebuie să fie un obiectiv important al oricărei organizații.

Trebuie însă avută în vedere asigurarea unui bun echilibru între costurile aferente şi avantajele concrete obținute. Măsurile trebuie să descurajeze tentativele de penetrare neautorizată, să le facă mai costisitoare decât obținerea legală a accesului la aceste programe și date.

OECD (Organization of Economic Cooperation and Development) este unul din organismele internaționale preocupate de domeniul protecției datelor cu caracter personal, securității sistemelor informatice, politicii de cifrare şi al protecției proprietății intelectuale.

Potrivit OECD securizarea sistemelor informatice se poate pune în aplicare prin diverse metode pornind de la încuierea încăperilor cu calculatoare şi a calculatorului însuşi, protejarea intrărilor în rețeaua de calculatoare cu parole, folosirea sistemelor de protejare a fișierelor de date pentru împiedicarea distrugerii acestora, criptarea liniilor de comunicaţii din reţelele de calculatoare şi ajunge până la folosirea unor tehnologii speciale pentru împiedicarea interceptării diferitelor radiaţii emise de echipamentele de calcul în timpul funcţionarii normale a acestora [8].

De asemenea, o importanță deosebită trebuie acordată factorul uman care reprezintă o verigă sensibilă în spațiul cibernetic.

Conform Popovici S. Director general al Centrului de telecomunicaţii speciale (CTS), de cele mai multe ori, o eroare banală, neintenționată poate genera un atac cibernetic de proporții. Pe de altă parte, sunt înregistrate nu puține cazuri în care angajații acționează rău intenționat împotriva angajatorului. Datele statistice internaționale prezintă o pondere de 30 % a incidentelor cibernetice cauzate de angajați rău intenționați și 11% din indiferența și neglijența din partea acestora. La nivel global, 40 % din angajați ascund informația cu privire la înregistrarea unui incident cibernetic, fapt care implică desigur consecințe grave.

În cel mai amplu atac al anului 2017- WannaCry, cu peste 200 000 oameni și 10000 instituții din cel puțin 150 de țări afectate, erorile generate de factorul uman au jucat un rol esențial. Desigur Moldova nu a fost o excepție, 31 adrese IP publice au realizat conexiuni către un domeniu web asociat campaniei ransomware WannaCry. Având în vedere ca printr-un IP public pot comunica mai multe sisteme informatice, numărul total al sistemelor afectate a fost și mai mare [3].

În vederea celor expuse putem concluziona că este nevoie de asigurat un model de securitate pentru un sistem informatic, care poate fi văzut ca având mai multe straturi care reprezintă nivelurile de securitate ce înconjoară subiectul ce trebuie protejat. Fiecare nivel izolează subiectul și îl face mai dificil de accesat în alt mod decât cel în care a fost prevăzut.

În acest sens, este nevoie de divizat securitatea în:

- *securitate fizică* - reprezintă nivelul exterior al modelului de securitate și constă, în general, în închiderea echipamentelor informatice într-o alta incinta precum și asigurarea pazei și a controlului accesului.
- *securitate logică* - constă din acele metode logice (software) care asigură controlul accesului la resursele și serviciile sistemului.
- *securitatea accesului* - cuprinde accesul la sistem, accesul la cont și drepturile de acces.
- *securitatea serviciilor* - controlează accesul la serviciile unui sistem (calculator, rețea).
- *securitatea la nivel de gazdă* - se referă la entitățile ce au acces local la acea mașină (utilizatori, programe server, agenți locali), precum și drepturile acestora, serviciile oferite către exterior și sistemul de operare.

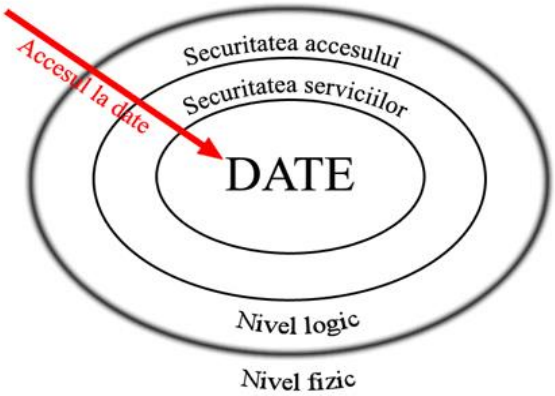

Fig. 1. Niveluri de securitate
Sursa: Mihai Ioan-Cosmin „Securitatea sistemului informatic" [7].

Totuși, unul dintre cele mai importante aspecte, în domeniul securității informațiilor, considerăm că este conştientizarea, o problemă legată de factorul uman. Este important să realizăm că "problemele umane" constituie principala cauză a încălcării securității. Cel mai eficient mod de a reduce riscurile de securitate a informațiilor într-o organizație este ca angajații să devină mai conştienți și trebuie să își asume responsabilitatea pentru propriile lor acțiuni la locul de muncă.

Menționăm că implementarea unui program eficace de sensibilizare cu privire la consecințele neglijării securității informațiilor, îi va ajuta pe toți angajații să înțeleagă, de ce trebuie să ia securitatea informațiilor în mod serios, ceea ce vor câștiga din punerea în aplicare a regulilor corespunzătoare și cum îi va ajuta în îndeplinirea sarcinilor atribuite.

Necunoscând metodele de securitate necesare și modul de aplicare al acestora, utilizatorii nu pot să răspundă adecvat la amenințări.

Practica, confirmă că organizațiile care au implementat mecanisme de protecție puternice și au educat personalul lor, cu privire la metodele corespunzătoare ce trebuie implementate pentru a-și proteja informațiile împotriva amenințărilor au numai de cîștigat. Procedurile de securitate a informațiilor trebuie să fie integrate în rutina obișnuită de zi cu zi, iar personalul ar trebui să recunoască securitatea mai degrabă ca factor de favorizare, decât o barieră.

Totodată, condiserăm că o altă soluție ar constitui implementarea unui sistem de management al securității informaţiei, despre care am menționat mai sus și totodată este specificat în cadrul ISO/IEC 27001:2005.

Implementarea unui sistem de management al securității informaţiei oferă o serie de avantaje:

- câştigarea încrederii partenerilor de afaceri (furnizori, clienţi);
- continuitatea afacerii;
- îmbunătăţirea sistemelor de prevenire şi răspuns în caz de incidente;
- minimizarea riscurilor pentru furtul, coruperea sau pierderea informaţiei;
- accesarea în siguranţă a informaţiei (de către angajaţi şi clienţi);
- justificarea și optimizarea costurilor necesare implementării controalelor de securitate;
- demonstrarea implicării și angajamentul managementului pentru securitatea informației;
- asigurarea faptului că riscurile și controalele sunt permanent revizuite [11].

Evaluând cele expuse putem conchide că, dezvoltarea unui sistem de protecție a sistemelor informatice, cât și a informației este un proces complex și multilateral.

Vestea bună este că conform Organizației Internaționale de Standardizare anul 2018, se anunță a fi anul inițiativelor majore în domeniul securității cibernetice, acest fapt datorându-se Regulamentului UE privind protecția generală a datelor, intrat în vigoare din 2018, precum și noii ediții a standardului internațional ISO/IEC 27000. Standardul ISO/IEC 27000: 2018 oferă o imagine de ansamblu a sistemelor de management al securității informaționale și prezintă terminologia utilizată în familia de standarde ISO / IEC 27000.

Întrucât există un set de standarde în familia 27000, noua versiune a standardului ISO/IEC 27000 oferă o imagine asupra scopurilor și funcțiilor acestor standarde, precum și a relației dintre ele. Standardul se adresează tuturor organizațiilor, indiferent de tipul și mărimea acestora, de la întreprinderi mici, mijlocii și mari, până la instituții guvernamentale sau organizații nonprofit [15].

V. CONCLUZII

În cele din urmă, conceptul de sistem de protecție a informațiilor computerizate poate fi definit drept un set de norme juridice, organizatorice, administrative și software-tehnice, menite să contracareze amenințările la adresa funcționării normale a sistemului, pentru a minimiza posibilele pierderi materiale și morale pentru utilizatorii și proprietarii sistemului.

Dat fiind că computerele și alte dispozitive digitale au devenit esențiale pentru marea parte a societății contemporane, acestea au devenit din ce în ce mai mult o țintă pentru atacuri. Pentru ca sistemele informatice să fie utilizate cu încredere, persoana/compania trebuie să se asigure, în primul rând, că dispozitivul nu este compromis în niciun fel și că toate comunicațiile vor fi în siguranță.

O imagine holistică a tuturor posibilităților de protecție este dificil de creat, deoarece nu există încă o teorie unificată pentru protecția sistemelor informatice.

Pentru organizarea unei protecții fiabile, este necesară identificarea clară a tipurilor de atacuri de informații care ar trebui protejate. O amenințare la adresa securității este un potențial impact asupra unui sistem care poate afecta direct sau indirect resursele sistemului informatic.

Considerăm că măsurile de protecție ar trebui să fie adecvate gradului de amenințare, precum și corespunzătore importanței informației care este păstrată în sistem. Numai o analiză amănunțită a amenințărilor și a tipurilor de securitate ale sistemelor informatice poate oferi o siguranță relativă.

BIBLIOGRAFIE

[1] Ce este securitatea sistemelor informatice? [Resursă electronică, accesat 07.03.2018]. https://www.quora.com/What-is-computer-system-security

[2] Cerinte ISO 27001 - Securitatea sistemelor informatice [Resursă electronică, accesat 02.03.2018]. http://www.intermanagement.eu/stire/Cerinte+ISO+27001+Securitatea+sistemelor+informatice.

[3] Factorul uman - element crucial în asigurarea securității cibernetice. [Resursă electronică, accesat 05.03.2018]. http://moldova.md/ro/content/factorul-uman-element-crucial-asigurarea-securitatii-cibernetice

[4] Gorobievschi S. Tehnici, instrumente și metode de comunicare managerială și utilizarea lor în cadrul firmelor contemporane.// În,: *M*anagementul industrial. Coord.: A.Cojuhari, dr.hab., prof.univ.; V. Mămăliga, dr. econ., conf. univ. Chișinău: UTM, 2017, pp. 356-389

[5] Harta uimitoare a atacurilor cibernetice [Resursă electronică, accesat 05.03.2018]. https://www.molddata.md/?pag=news&opa=view&id=341&tip=noutati

[6] Legea privind aprobarea Concepţiei securităţii informaţionale a R.Moldova [Resursă electronică, accesat 07.03.2018]. https://www.google.com/search?q=Legii+privind+Concep%C5%A3ia+securit%C4%83%C5%A3ii+informa%C5%

[7] Mihai Ioan-Cosmin; „Securitatea sistemului informatic", ISBN 978-973-627-369-8, Galați, Ed. Dunărea de Jos, 2007

[8] Păduraru M.Vulnerabilităţi ale sistemelor informatice [Resursă electronică, accesat 02.03.2018]. https://www.juridice.ro/412111/vulnerabilitati-ale-sistemelor-informatice.html

[9] Popa Sorin Eugen. Securitatea sistemelor informatice. Note de curs şi aplicaţii. [Resursă electronică, accesat 03.03.2018]. https://bogdanelb.files.wordpress.com/2009/12/curs_securit_sist_inf.pdf, p. 5

[10] Securitatea informației [Resursă electronică] [accesat 10.03.2018]. https://ro.wikipedia.org/wiki/Securitatea_informa%C8%9Biei

[11] Securitatea sistemelor informaţionale. [Resursă electronică, accesat 05.03.2018]. http://formare.contatic.ase.ro/pluginfile.php/46/mod_resource/content/1/Securitatea%20sistemelor%20informationale.pdf

[12] Securitatea sistemelor informatice [Resursă electronică, accesat 02.03.2018]. Disponibil pe http://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf, p.6

[13] Sisteme de control al accesului la Intranet. [Resursă electronică, accesat 05.03.2018]. https:// www.kp.ru/guide/sistemy-kontrolja-i-upravlenija-dostupom.html

[14] Sistem informatic. [Resursă electronică, accesat 02.03.2018]. https://ro.wikipedia.org/wiki/Sistem_informatic

[15] Standardul ISO/IEC 27000 a fost actualizat. [Resursă electronică, accesat 05.03.2018]. http://standard.md/libview.php?l=ro&idc=196&id=3006&t=%2FResurse-media%2FCo municate%2FStandardul-ISOIEC-27000-a-fostactualizat#.Wp0QZW 8wEqg.facebook.