SECURITATEA INFORMAȚIONALĂ: PROBLEME ȘI METODE DE PROTECȚIE

CZU: 005.591.6:004:007 **https://doi.org/10.5281/zenodo.7542849**

Ada ȘTAHOVSCHI, ORCID ID 0000-0002-3415-9509
Universitatea de Stat din Moldova

Abstract: *Increasing the dependence of contemporary society on the globalization of information systems and communication infrastructures leads to increasing the vulnerability of the person, society and the state to the more and more acute threats in the informational-technological and informational-media domains.*

In the informational age, cyber space is a comfortable platform for the preparation and execution of cybercrime, cyber-terrorism acts and other actions that directly or indirectly affect national state security.

Violation of the security of the information systems of public authorities and other institutions may compromise the confidentiality and integrity of this information and, as a result, cause financial or material damage, including damage to state security.

Keywords*: security, information system, cyber space, informational potential.*

INTRODUCERE

În condițiile digitalizării și utilizării noilor tehnologii informaționale, companiile în activitatea lor colectează, prelucrează, transmit diferite informații privind activitatea economico-financiară. Din acest motiv, un rol important îi revine managementului securității informaționale.

Obiectivul primordial al securității informaționale este de a proteja informațiile cu privire la activitatea entității pentru a micșora pierderile, a continua activitatea și pentru a introduce mecanisme pentru a asigura gestionarea, evaluarea și eliminarea riscurilor potențiale în relație cu disponibilitatea, integritatea și confidențialitatea informațiilor.

MANAGEMENTUL SECURITĂŢII INFORMAŢIONALE

Managementul securităţii informaţionale este obiectivul principal al standardelor internaționale ISO 27000, care tratează diferitele aspecte ale acestui domeniu, de la inventarierea valorilor care trebuie protejate, la analiza şi tratarea riscurilor, alegerea mijloacelor de diminuare a riscurilor şi până la recomandări de aplicare a măsurilor de securitate sub aspect general sau pentru anumite tipuri de organizaţii [9].

În lumea unei concurențe între diferite companii informația prezentată trebuie să corespundă următoarelor cerințe fundamentale [7, p. 54]:

- *confidențialitate,* accesul la informație nu poate fi făcut decât cu autorizare adecvată;
- *integritate, acuratețea și completitudinea* informației și a modului în care este prelucrată;
- *disponibilitate,* utilizatorii autorizați trebuie să aibă acces la informație de fiecare dată când au nevoie.

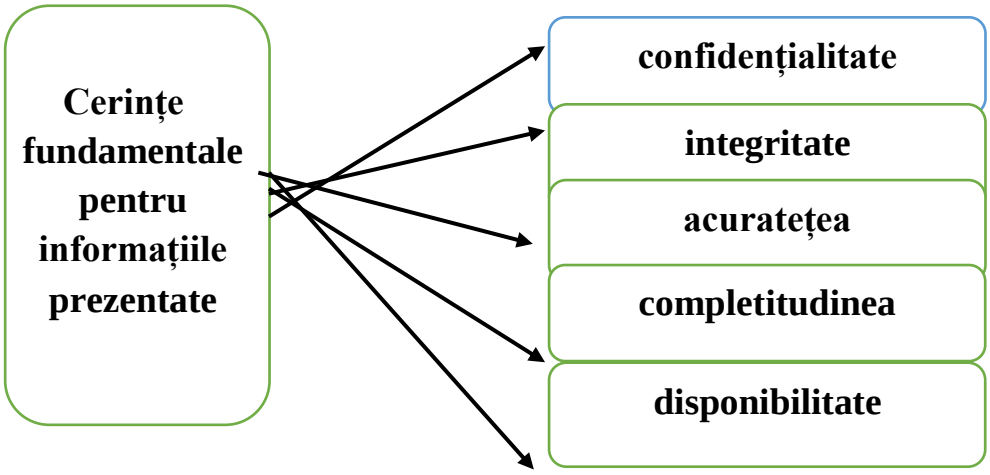


Figura 1. Cerințe fundamentale pentru informațiile prezentate
Sursa: Elaborată de autor

Pentru o monitorizare mai eficientă a sistemului de securitate informațională este necesar de lua măsuri pentru actualizarea politicilor de securitate, pentru protecția *sistemelor de comunicații și informații,* care includ [5]:

- Sistemele informaționale și protecția rețelelor;
- Internetul;
- Elemente tehnologice ale rețelelor de comunicații electronice,
- Elemente tehnologice ale rețelelor mobile de comunicații,
- Elemente tehnologice ale rețelelor de televiziune și radiodifuziune.

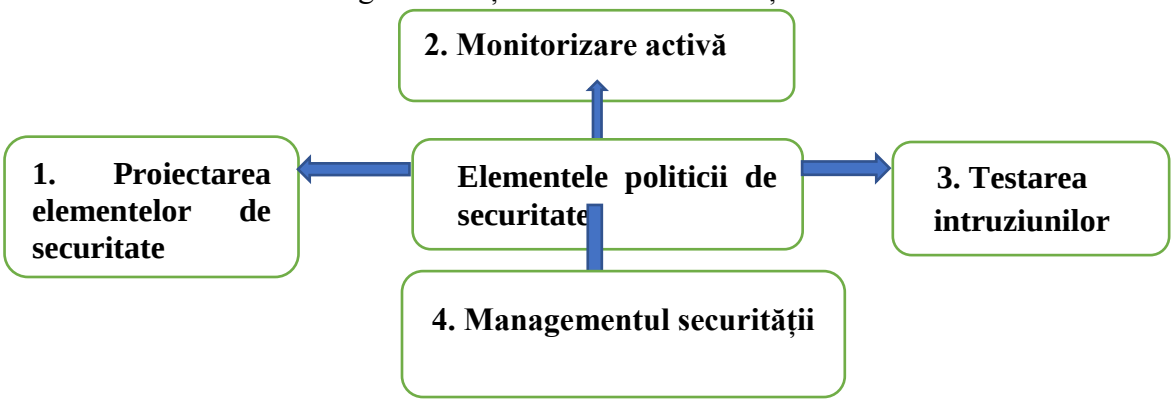


Figura 2. Principalele elemente ale politicii de securitate informațională
Sursa: Elaborat de autor în baza sursei [1].

În practica securității informaționale este necesară de a aplica o monitorizare și testare permanentă a infrastructurii și a mediului cu privire la diferite vulnerabilități și luarea măsurilor necesare și actualizarea politicilor de securitate (figura 2):

Securitatea informațiilor poate fi obținută prin implementarea unor instrumente de control, incluzând diferite politici, procese, proceduri, funcții software și hardware. Aceste instrumente de control trebuie să fie implementate, supravegheate, revizuite și perfecționate, pentru a se asigura atingerea obiectivelor de securitate ale companiei. Deci, când există amenințări asupra vulnerabilității companiei, pot apărea și riscurile asupra securității informației pe care o prezintă entitatea. Securitatea informației ar putea reduce aceste riscuri prin protejarea companiei împotriva diferitor amenințări și vulnerabilități și prin reducerea impactului asupra resurselor ei [13].

STANDARDELE INTERNAȚIONALE PRIVIND SECURITATEA INFORMAȚIEI

În practică internațională, privind gestiunea securității informaționale, au fost elaborate și implementate un șir de standarde internaționale dedicate managementului securității informației, care se numește ”Seria ISO/IEC 27000”, care au obiectivul principal de a ajuta companiile să păstreze siguranța informațiilor [9;10].

Securitatea informaţiei este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei. Din acest motiv fiecare entitate trebuie să-și elaboreze Politica de Securitate. Obiectivul politicii de securitate este să ofere managementului instituţiei sprijinul necesar asigurării securităţii informaţiilor din cadrul organizaţiei. Conținutul politicii de securitate trebuie adus la cunoştinţă tuturor angajaţilor.

METODE DE ASIGURARE A SECURITĂŢII INFORMAȚIONALE

Printre principalele metode de protecţie a mijloacelor de păstrare şi transmitere a informaţiei, a sistemelor informaţionale putem enumera [6, p.157]:

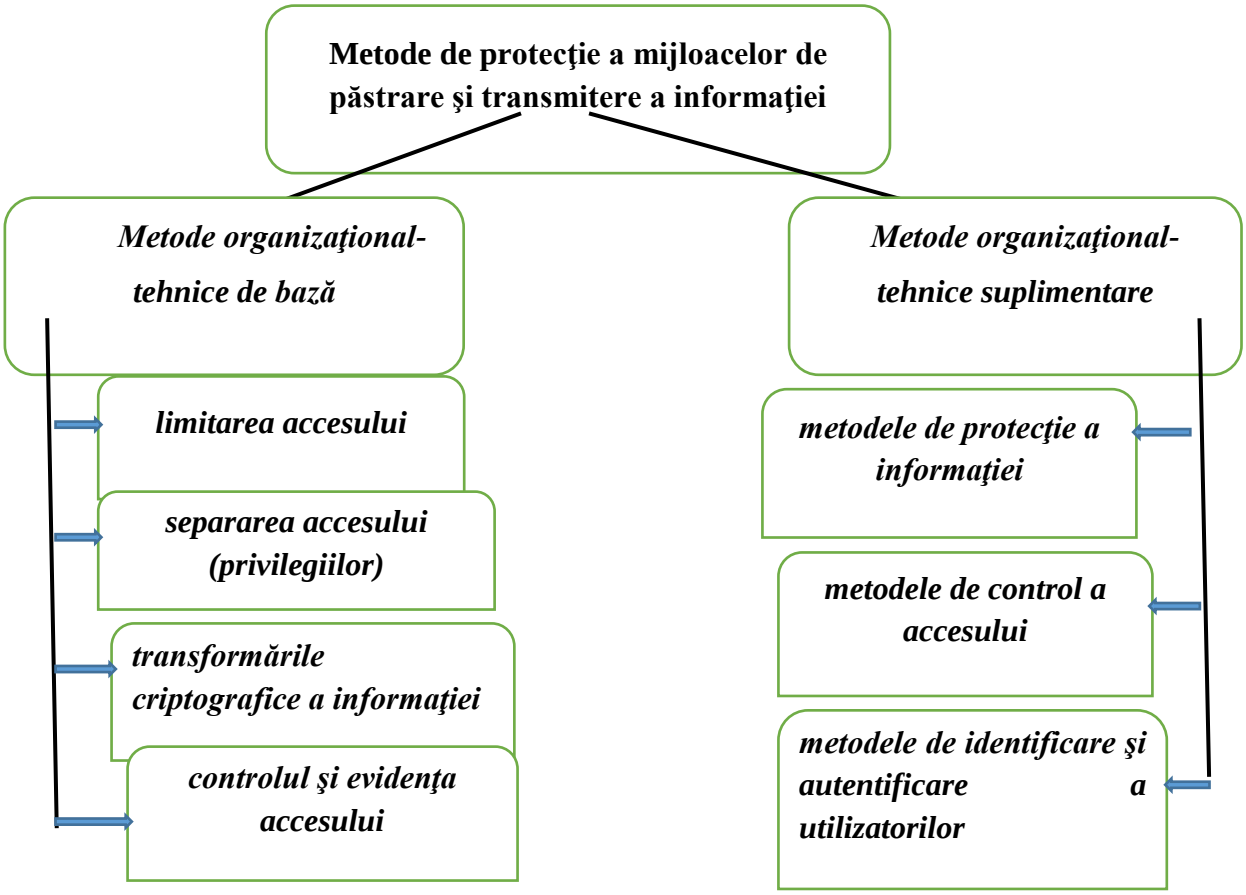


Figura 3. Metode de protecţie a mijloacelor de păstrare şi transmitere a informaţiei
Sursa. Elaborat de autor în baza sursei

Protecția datelor este o problema multilaterala si complexa,care cuprinde o serie de sarcini importante. Problema securității informaționale se agravează permanent din cauza pătrunderii mijloacelor tehnice de prelucrare si transfer de date, si mai ales a sistemelor de calcul,in toate domeniile societății.

În vederea asigurării unui sistem de protecție și dezvoltare a spațiului informațional în condițiile globalizării și liberei circulații a informațiilor, în Moldova, a fost adoptată *Strategia de securitate informațională* pentru anii 2019-2024. Strategia prezintă o evaluare a situației actuale în domeniul securității informaționale, enumeră performanțele înregistrate și trasează noi tendințe de dezvoltare a societăţii informaţionale [11].

Printre principalele activități ale securității informaționale, în *Strategia de securitate informațională* pentru anii 2019-2024 sunt prevăzute următoarele măsuri[11]:

- ✓ *determinarea politicii privind modalitatea de raportare, stocare și prelucrare a informațiilor* aferente incidentelor și amenințărilor la adresa securității informaționale;
- ✓ *desfășurarea acțiunilor de sensibilizare și informare a societății* privind amenințările, vulnerabilitățile și riscurile securității cibernetice;
- ✓ *dezvoltarea capacităţilor de rezilienţă cibernetică și ridicarea nivelului de cultură* în domeniul TIC;
- ✓ *desfășurarea exercițiilor și antrenamentelor de consolidare a capacităţilor de reacţie la atacuri cibernetice*, inclusiv de blocare a atacurilor cibernetice simulate;
- ✓ *organizarea și efectuarea atelierelor de lucru în domeniul securității cibernetice*.
- ✓ *sistematizarea, analiza și evaluarea datelor statistice* la capitolul securității cibernetice;
- ✓

CONLUZII

În concluzie putem constata, că la etapa actuală când tehnologiile informaționale au pus amprenta pe toate domeniile de activitate, este necesar de luat măsuri de protecție și de implementat programe de securitate informaționale, deoarece dependența de informații este tot mai mare.

În actualul mediu geopolitic și geostrategic, date fiind amenintarile interne, externe și cele transnationale, statul, prin activitățile de informații, protejează cetățenii, contribuind la menținerea stabilității interne și la consolidarea mediului internațional de securitate.

Măsurile de protecție ar trebui să asigure protecția informațiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informației gestionată de sistemele informatice în noul context tehnologic.

Managementul riscurilor în sistemele informaționale impune utilizarea unor soluţii care să aibă în vedere diferite tipuri de incidente şi ameninţări care pot proteja informaţiile sensibile, precum şi obiectivele propuse, aria securităţii şi apărării sistemelor informaţionale din perspectiva implementării „Strategiei de securitatea naţională a Republicii Moldova” trebuie să devină o soluţie completă de securitate a informaţiilor care ar proteja datele şi resursele informatice.

Asigurarea prevenirii riscurilor și combaterii amenințărilor în adresa securității informaționale este una din sarcinile de bază ale statului.

BIBLIOGRAFIE

1. IT Governance Institute: Guidance for Boards of Directors and Executive Management. 3rd Edition, 2000, www.ITgovernance.org and www.isaca.org accesat 18.02.2022
2. Legea Republicii Moldova privind accesul la informaţie, Nr. 982, din 11 mai 2000. În: Monitorul Oficial al Republicii Moldova nr.88-90 din 25.07.2000.
3. Managementul Riscurilor - risks are everywhere. http://www.managementul-riscurilor.ro/ Accesat 18.09.2022
4. Mihai I. Securitatea informațiilor. Editura Sitech, 2012, 317 p.
5. McAfee.Protecting Critical Infrastructure. https://www.mcafee.com/enterprise/enus/about/public-policy/critical-infrastructure.html Accesat 28.09.2022
6. Rusnac A. Aspecte ale teoriei securităţii, Chişinău, 2005, 216 p.
7. Stanciu V., Tinca A. Securitatea informației. Principii și bune practici. Ediția a doua, 2015
8. Standardul de securitate ISO/IEC 27002. https://standardizare.wordpress.com Accesat 12.10.2022
9. SR/ISO 27002 Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației. Camera de Comerț, Industrie și Agricultură Timiș. https://www.cciat.ro/cciat_ASRO_-_CZI_Timi%C8%99_(standarde), accesat 12.10.2022
10. SR EN ISO/IEC 27001:2018. https://standardizare.wordpress.com/2018/04/13/, accesat 14.09.2022
11. Strategia securității informaționale a Republicii Moldova pentru anii 2019–2024. În: Monitorul Oficial Nr. 13-21 art. 80 din 18-01-2019
12. https://www.securitatea-retelelor.ro/sisteme-de-tip-ids-ips. Accesat 23.10.2022
13. https://ibn.idsi.md/sites/default/files/imag_file/410-413_1.pdf Accesat 23.10.2022

Acest studiu este realizat în cadrul Proiectului demarat la inițiativa Departamentului Contabilitate și Informatică Economică a USM ”*Armonizarea tratamentului contabil al Republicii Moldova în vederea sporirii calității informației prezentate în situațiile financiare*” (2022-2023)