1. Arhitectura programului de securitate

Elaborarea programului de securitate al unei USE – *organizații, companii, firme* – presupune *structurarea lui, definirea politicilor, standardelor, normelor și procedurilor de securitate.* Politicile, standardele, normele și procedurile constituie fundamentul programului de securitate al unității social economice (USE). Toate acestea, clar formulate, servesc proceselor de management, control și auditare a ASI. Arhitectura generală a PSI trebuie să ia în considerare *riscurile* și *contramăsurile* necesare pentru a le reduce sau a le preveni. La elaborarea PSI se va ține cont de interesele USE:

- Valorile/resursele informaționale ce trebuie protejate;
- Mijloacele de protecție și acțiunile necesare;
- Riscurile aferente și reevaluarea amenințărilor ținând cont de protecția implementată;
- Impactul, consecințele amenințărilor.

Pentru construcția propriului sistem de securitate a informațiilor, orice organizație trebuie să analizeze nivelul actual atins și dinamica dezvoltării tehnologiilor informaționale, amenințările așteptate la adresa securității informațiilor, sursele acestor amenințări și factorilor care contribuie la aplicarea acestora, având în vedere *declararea sistemică a scopurilor, obiectivelor și principiilor* pentru atingerea obiectivelor cerute de securitate.

Toate acestea sunt reflectate în **Programul de securitate informațională al USE** și integrate într-un sistem unitar de securitate, care constă dintr-un set de (a) măsuri organizatorice, (b) juridice, (c) de inginerie software și hardware de protecție, bazate pe metode moderne de previziune, analiză și modelare a situațiilor în continuă schimbare.

Cadrul normativ intern al USE necesar pentru realizarea PSI, poate fi recomandat oricărei organizații, ținându-se cont de:

1. Documentele primului nivel, *Politica (*informală*)* a *organizației*, prezintă *reguli, principii, norme* de ASI. De regulă, sunt determinate scopurile, conținutul și principalele direcții de activitate pentru ASI *(un exemplu a se vedea în Anexa 1)*. Politica se aplică de obicei tuturor unităților și tuturor angajaților organizației.

De regulă, Politica informală a securității informației unei USE reflectă *propriile drepturi, drepturile persoanelor juridice, fizice și drepturile statului în accesarea, distribuirea și utilizarea informației* pentru a asigura protejarea resurselor informaționale și a informației confidențiale. Astfel, PSI protejează informația contra potențialelor atacuri, pagube, pierderi precum și asigură o reputație sigură a organizației, încredere față de parteneri, colaboratori și utilizatori.

2. Documentele de nivelul doi conțin prevederi detaliate, numite *Politici particulare (private, speciale)* de securitate a informațiilor pentru anumite zone, tipuri de tehnologii și organizare. De exemplu, *politici pentru utilizarea Internetului, e-mail-ului, accesarea de la distanță a sistemului* etc. Aceste politici stabilesc domeniul de operare, obiectivele, scopul și cerințele de operare, precum și activitățile persoanelor fizice responsabile de implementarea setului de activități din domeniul relevant al securității informațiilor. *Numărul politicilor private depinde de valorile protejate și tipurile de activități necesare pentru ASI.*

3. Documentele nivelului trei conțin *Cerințe operaționale de securitate,* aplicate procedurilor operaționale pentru ASI: *reguli și parametri care stabilesc modalitățile de implementare și executare a anumitor tipuri de lucrări în cadrul proceselor asociate proceselor tehnologice*. Suplimentar, aceste documente pot conține diferite restricții privind îndeplinirea anumitor acțiuni legate de implementarea măsurilor de protecție în procesele tehnologice utilizate, așa ca *sarcini tehnice, reglementări, proceduri, instrucțiuni (*diverse dispoziții, seturi de reguli, cerințe pe care acest funcționar ar trebui să le respecte în cadrul activității sale).

4. Documentele nivelului patru conțin dovezile activităților desfășurate pentru ASI: reflectă rezultatele (intermediare și finale) ale activităților de ASI, includ o varietate de rapoarte, protocoale etc., necesare pentru activitățile de monitorizare, care certifică implementarea activităților d ASI în modul reglementat.

Politica de securitate poate fi descrisă într-un mod formal sau informal. O descriere formală a politicii de securitate se face în cadrul *modelelor formale de securitate (pct. 3),* care pot fi definite ca descrieri abstracte a comportamentului unei întregi clase de sisteme, fără a lua în considerare detaliile specifice ale implementării acestora.

În concluzie, principalele prevederi ale Programului de

securitate a informațiilor includ:

- Definiția securității informațiilor, lista componentelor sale;
- Regulamentul privind obiectivele de management, sprijinirea obiectivelor și principiilor securității informațiilor;
- Politici speciale de securitate, principii și standarde de construcție a politicii pe domenii;
- Consecințele încălcării politicii de securitate și altele.

Politica globală de securitate informațională definește politica de ansamblu a organizației și responsabilitățile respective. Iar **politicile speciale** sunt componente esențiale ale programului de securitate, care, de regulă trebuie să răspundă la cinci obiective majore:

1. ***Prevenirea*** accesului neautorizat la valorile patrimoniale ale organizației;
2. ***Asigurarea*** că politicile, standardele și normele sunt în concordanță cu intențiile organizației privind protejarea valorilor patrimoniale informaționale;
3. ***Detectarea*** intrușilor din sistem și lansarea arsenalului de contramăsuri corespunzătoare;
4. ***Investigarea*** capacității de a folosi tehnici adecvate pentru obținerea informațiilor despre posibilii intruși din sistem;
5. ***Continuitatea*** – garantarea funcționării neîntrerupte prin existența unui plan de acțiune în cazul dezastrelor, dezvoltat și testat în organizație.

2. Politica generală și politici particulare de securitate

Politica generală de securitate a informației are ca obiectiv orientarea generală a managementului și sprijinul lui pentru securitatea informației în conformitate cu cerințele afacerii, legislația în vigoare și actele normative aplicabile, incluzând o analiză a posibilelor amenințări și alegerea contramăsurilor. PSI este una dintre cele mai importante și vitale documentele companiei.

Conducerea USE elaborează și aprobă un document întitulat „*Politica (generală) a securității informației”,* care trebuie comunicat tuturor angajaților și terțelor părți relevante *(Figura 1).*

De regulă, politica de securitate:

a) Este revizuită anual sau oricând apar schimbări semnificative la nivelul SiF sau al reglementărilor aferente;
b) Este exprimată sub formă de narațiune concisă;
c) Necesită aprobarea și susținerea managementului superior;
d) Ar trebui să fie disponibilă tuturor angajaților responsabili de securitatea informațională.

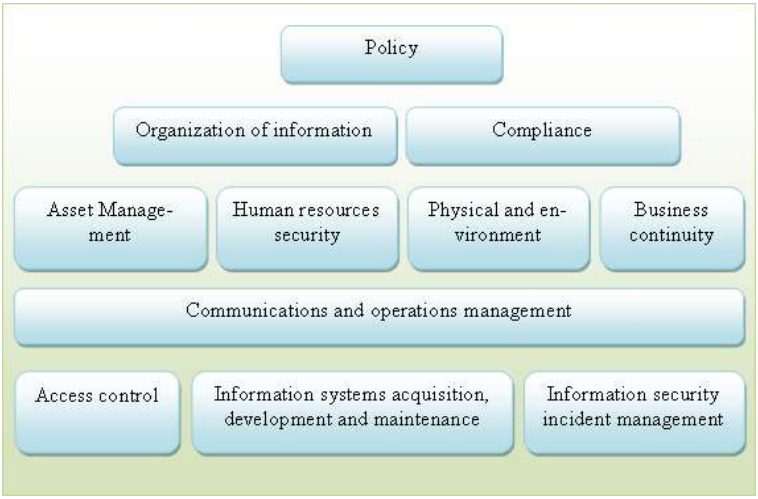

Fig. 1. Componente majore ale Politicii de securitate

Politica de securitate ar trebui să conțină:
a) O definiție a securității informaționale, obiectivelor sale generale și domeniilor de aplicare;
b) O declarație cu privire la intenția managementului, care sprijină obiectivele și principiile securității informaționale;
c) O extindere a politicilor de securitate specifice, conform principiilor, standardelor inclusiv cerințelor:
    - de conformitate cu cerințele legale și contractuale;
    - de educație și instruire în domeniul securității;
    - de prevenire și detectare a virușilor;
    - de planificare a continuității afacerii.
d) O definiție a responsabilităților generale și specifice pentru toate aspectele securității informaționale și

e) O explicație a procesului de raportare a incidentelor de securitate suspectate.

Pentru descrierea specificațiilor tehnice ale cerințelor de securitate politicile de securitate operează cu trei termeni, definiți în continuare, *Modelul politicii, Ținta securității, Profilul protecției*

Modelul politicii de securitate este o declarație succintă a proprietăților sau principiilor securității, ca un sistem sau ca un tip generic de sistem. Punctele sale esențiale vor fi consemnate în scris, pe cel mult o pagină, iar documentul respectiv prevede scopurile protecției unui sistem, agreate de întreaga comunitate sau de linia managerială a clienților. Un astfel de model constituie *baza de pornire a analizelor formale matematice.* Practica arată: pentru analiza unui număr semnificativ de resurse, acțiuni și obiecte informaționale, inclusiv pentru automatizarea procedurilor, ar fi bine de utilizat modelarea, care simulează situația reală, descrie acțiunile reale având în vedere caracteristicile acestora. Modelul PSI va ține cont de *resursele informaționale, amenințări, obiectele amenințate, scopurile atacatorilor/ a intruşilor, surse de amenințări etc. (Figura 2).*

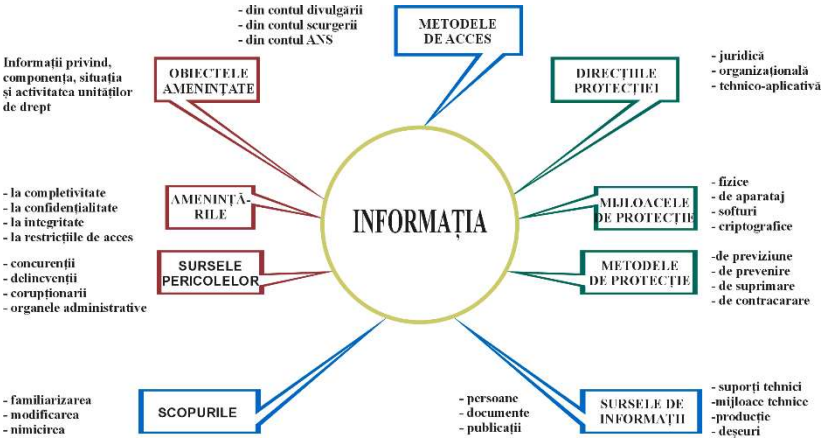

Fig. 2. Model conceptual al informației ca obiect de protecție

Ținta securității este o descriere mult mai detaliată a mecanismelor de protecție oferite de o anumită variantă de implementare, precum și a modului în care ele concură la atingerea

obiectivelor de control ale sistemului. Ținta securității formează baza testării și evaluării produsului implementat.

Profilul protecției exprimă o cale independentă de implementare, care să permită evaluări comparative ale produselor sau versiunilor lor.

O altă piatra de temelie a politicii de securitate este **determinarea răspunderii,** care impune studierea detaliată a aspectelor legate de *repartizarea responsabilităților* și de *delimitarea responsabilităților*. Responsabilitatea pentru securitatea informațională ar trebui, în mod normal, atribuită unei funcții de administrare a securității. La clienții mai mici, această funcție poate fi un post part-time, deținut de un membru al personalului, cu numele de administrator/specialist în securitatea informației. Adesea, această funcție poate fi externalizată, practică frecventă pentru cloud computing. Clienții mai mari ar fi de așteptat să aibă personal/ subdiviziuni dedicate pentru ASI.

Implementarea politicilor de securitate trebuie pornită de la vârful piramidei manageriale, unde se află *top managerii*. Aceștia au misiunea de a formula *Declarația politicii organizației*. Aceasta este o declarație/formulare generală, care descrie:

a) Importanța informației și resurselor informaționale pentru atingerea obiectivelor strategice ale organizației;
b) Formularea clară a sprijinului oferit SiF de către TIC;
c) Angajamentul managerilor de niveluri superioare de a autoriza sau coordona activitățile de definire a *standardelor, procedurilor și normelor de securitate de pe nivelurile inferioare.*

În afara *declarației politicii de securitate* la nivelul top managerilor, mai există *politici obligatorii, politici recomandate și politici informative*.

Politicile obligatorii de securitate sunt cele pe care USE sunt obligate să le implementeze ca *efect al acordurilor, regulamentelor* sau al *altor prevederi legale*. De regulă, aici se încadrează *instituțiile financiare, serviciile publice* sau orice alt tip de organizație care servește interesului public. Aceste politici sunt foarte detaliate și au elemente specifice, în funcție de domeniul de aplicare.

De regulă, politicile obligatorii au două scopuri de bază:

- asigurarea că USE urmează procedurile standard sau

politicile de bază din domeniul ei de activitate;

- de a oferi încredere USE că aceasta urmează standardele și politicile de securitate din domeniul ei de activitate.

Politicile recomandate, prin definiție, nu sunt obligatorii, dar sunt puternic susținute, cu prezentarea consecințelor foarte dure în cazul înregistrării eșecurilor. *O organizație este direct interesată ca toți angajații ei să considere aceste politici ca fiind obligatorii*. Cele mai multe politici se încadrează în această categorie. Ele sunt foarte clar formulate la toate nivelurile. Cei mai mulți angajați vor fi riguros controlați prin astfel de politici, definindu-le r*olurile* și *responsabilitățile* în organizație.

Politicile informative au scopul de a informa utilizatorii interesații de aceste politici, fie din interiorul organizației fie partenerii externi, dar fără a înainta careva cerințe specifice, lăsând acțiunile la discreția lor.

Toate politicile de securitate au șase elemente comune:

1. ***Declararea domeniului de aplicare*** – prezentarea intenției vizate de politică, care va scoate în relief și legăturile existente cu întreaga documentație a organizației. Formularea trebuie să fie cât mai scurtă și, de regulă, plasată la începutul documentului.
2. ***Declararea așteptărilor top-managerilor*** **–** specifică scopul global al politicii, la fel se include la începutul documentului și are dimensiunea unui singur paragraf.
3. ***Responsabilitățile*** **–** specifică persoanele implicate în asigurarea bunei funcționări a politicilor pe domenii/secțiuni distincte.
4. ***Consecințele*** **–** prezintă eventualele pierderi dacă politica nu va fi respectată.
5. ***Monitorizarea*** **–** specifică modul în care se controlează/ auditează respectarea și actualizarea continuă a politicii.
6. ***Excepții*** **–** menționează cazurile excepționale și modalitățile de tratare a lor; de regulă, au o durată limitată de aplicare.

Pe nivelul inferior al politicilor de securitate se află trei elemente de implementare a politicii: *standardele, normele și procedurile.* Ele conțin detaliile politicii, cum ar fi posibilitățile de implementare, ce standarde și proceduri să fie întrebuințate. Ele sunt făcute publice la nivel de organizație, prin manuale, Intranet, cărți, cursuri ș.a.

De cele mai multe ori, standardele, normele și procedurile sunt tratate laolaltă. Însă aceasta nu este cea mai inspirată idee, tratarea separată a lor fiind justificată de următoarele argumente:

- Fiecare dintre ele servește unei funcții diferite și are propria audiență; chiar și distribuția lor fizică este mai lejeră;
- Controalele securității pe linia confidențialității sunt diferite pentru fiecare tip de politică;
- Actualizarea și întreținerea politicii ar deveni mai anevoioase, prin prisma volumului documentației, dacă s-ar trata nediferențiat.

Politica de securitate este un „document viu" care trebuie actualizat în permanență, simultan cu schimbarea tehnologiilor, angajaților, atacurilor, riscurilor etc.

2.1. Standarde de securitate

Standardele specifică utilizarea anumitor tehnologii, într-o viziune uniformă. De regulă, standardele sunt obligatorii și sunt implementate la nivel de unității. Elementele principale ale unui standard de securitate informațională includ:

- ***Scopul și aria de aplicare*****,** prin care se oferă o descriere a intenției standardului (realizarea unui tip de server pe o anumită platformă);
- ***Roluri și responsabilități*** la nivel de corporație pe linia definirii, execuției și promovării standardului;
- ***Standardele cadrului de bază*****,** prin care sunt prezentate declarațiile de pe cel mai înalt nivel, aplicabile platformelor și aplicațiilor;
- ***Standardele tehnologiei*** conțin declarațiile și descrierile aferente (configurația sistemului sau serviciile nesolicitate de sistem);
- ***Standardele administrării*** reglementează administrarea inițială și în timpul exploatării platformei și aplicațiilor.

În afară de standardele deja menționate, există diverse *standarde naționale* și *internaționale, de jure* și *de facto,* care sunt legate, direct sau indirect, de gestionarea riscurilor informaționale bazate pe TIC.

Standardul ISO/IEC 27000 a fost rezervat pentru o familie de standarde de management al securității informațiilor, derivate din standardul britanic BS 7799/ISO-17999. În RM multe standarde din această serie au fost deja publicate; altele se află în diferite stadii de dezvoltare. O prezentare cuprinzătoare și discutarea acestor standarde este furnizată de ISO-27001.

În cadrul ISO/IEC 27001:2005 este concepută selectarea măsurilor de securitate adecvate, care să protejeze activele informatice și să ofere încredere părților interesate în cadrul standardului. Standardul specifică cerințele pentru s*tabilirea, implementarea, operarea, monitorizarea, revizuirea, menținerea și îmbunătățirea unui sistem de securitate informațională documentat*. Aplicarea sa în practică este adesea combinată cu standardele aferente, cum ar fi BS 7799-3: 2006, care oferă îndrumări suplimentare pentru a susține cerințele din ISO/IEC 27001: 2005.

ISO/IEC 27005:2011 oferă orientări pentru gestionarea riscurilor de securitate a informațiilor. Acesta susține conceptele generale specificate în ISO/IEC 27001 și este conceput pentru a sprijini implementarea satisfăcătoare a securității informațiilor bazată pe o abordare a managementului riscului.

ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls. Second edition, 2016, http://www.iso27001security.com/html/27002.html/.

ISO/CEI 13335: *Information technology-Guidelines for the* management *of* IT-Security, cuprinde recomandări cu privire la analiza riscului pentru companii (Common Criteria);

Alte standarde de securitate în rețea, adoptate de Institutul de Standardizare din Moldova (ISM) (http://www.standard.md)/ includ[1]:

1. SMV ISO/CEI 18028-2:2010. Tehnologia informației. Tehnici de securitate. Securitatea rețelei IT. Partea 2: Arhitectura

[1]*Abrevierie utilizate de către ISM: SM – Standard moldovan; SMV – Prestandard moldovan; EN – Standard european; ISO – Standard al Organizației Internaționale de Standardizare; CEI – Standard internațional al Comisiei Electrotehnice Internaționale; GOST – Standard interstatal; RFC – Request For Comment – memorandum publicat de către Internet Engineering Task Force; OSI – Open System Interconnection, arhitectura de rețea pe 7 niveluri, potrivită pentru proiectarea oricăror rețele.*

securității rețelei.

2. SMV ISO/CEI 18028-3:2010. Tehnologia informației. Tehnici de securitate. Securitatea rețelei IT. Partea 3: Securizarea comunicațiilor între rețelele care utilizează gateway-uri de securitate.
3. SMV ISO/CEI 18028-4:2010. Tehnologia informației. Tehnici de securitate. Securitatea rețelei IT. Partea 4: Securizarea accesului de la distanță.
4. SMV ISO/CEI 18028-5:2010. Tehnologia informației. Tehnici de securitate. Securitatea rețelei IT. Partea 5: Securizarea comunicațiilor în cadrul rețelelor care utilizează rețele virtuale private.
5. SM GOST ISO 7498-2:2010. Tehnologia informației. Interconectarea sistemelor deschise. Model de referință de bază. Partea 2. Arhitectura securității informației.

2.2. Normele de securitate

Normele sunt oarecum asemănătoare standardelor, referindu-se la metodologiile sistemelor securizate, doar că normele sunt acțiuni recomandate, nu obligatorii. Sunt mult mai flexibile decât standardele și iau în considerare naturile diverse ale sistemelor informaționale. Adesea, normele specifică modalitățile de dezvoltare a standardelor sau garantează aderența la principiile generale ale securității.

Elementele principale ale unei norme de securitate informațională sunt:

- Scopul și aria de aplicare, descriindu-se intenția urmărită prin regula respectivă;
- Roluri și responsabilități pe linia definirii, execuției și promovării normei;
- Declarații de orientare: este un proces pas-cu-pas de promovare a tehnologiilor respective;
- Declarații de exploatare: se definesc obligațiile zilnice, săptămânale sau lunare pentru o corectă exploatare a tehnologiei respective.

Ca exemple de norme pot servi clauzele standarde internaționale și bune practici de ASI, întrunite în ITIL [.], CoBiT [.].

2.3. Proceduri/aspecte practice de securitate

Procedurile prezintă pașii detaliați ce trebuie să fie parcurși pentru execuția unei activități. Ele descriu acțiunile concrete pe care trebuie să le efectueze personalul. Prin proceduri se oferă cele mai mici detalii pentru implementarea *politicilor, standardelor* și *normelor.*

Realizarea propriei politici de securitate presupune acoperirea a 10 domenii diferite, inclusiv:

1. *Funcționarea neîntreruptă/continuă a USE*
2. *Controlul accesului în sistem*
3. *Dezvoltarea și întreținerea SiF*
4. *Securitatea fizică și a mediului*
5. *Maleabilitatea (capacitatea, ușurință de adaptare)*
6. *Securitatea personalului*
7. *Organizarea securității*
8. *Managementul resurselor informatice și al exploatării lor*
9. *Clasificarea și controlarea valorilor patrimonial*
10. *Politica de securitate*

2.4. Conținutul politicilor specifice de securitate

Nu există două USE care să aibă politici de securitate identice. Serviciile de securitate sunt dependente de contextul concret, timp, adesea sunt contradictorii, inegale ca amploare și necesita aplicare specifică. Adică, nu există rețete/soluții unice de securitate, fiecare USE își asigură securitatea în funcție de mărime, semnificația informațiilor, posibilitățile de finanțare etc.

Institutul *SANS* (http://sans.org), *cea mai de încredere și cea mai mare sursă de formare în domeniul securității informațiilor din lum*e, în colaborare cu liderii industriei IT, oferă **ghiduri de dezvoltare a diferitelor componente ale politicii de securitate** pentru organizații. De exemplu, *Declarația de autoritate și domeniul de aplicare; Politica de utilizare acceptabilă a serviciilor și tehnicii de calcul și măsurile de securitate adecvate angajaților pentru a proteja resursele corporative; Politica de identificare și autentificare; Politica de acces la Internet; Politica de acces la distanță; Politica de tratare a incidentelor; Definirea nivelului minim de asigurare a securității și a măsurilor de atingere* și altele.

2.5. Modele formale de securitate informațională

Cele mai multe modele de securitate funcționează cu termenii „entitate”, „subiect”, „obiect” .

Entitate – orice componentă protejată a SiF.

Subiect – o entitate activă care poate solicita și folosi resurse pentru a efectua operațiuni de calcul (de exemplu, un utilizator uman, un proces, o entitate SiF, notată cu s_i).

Obiect – o entitate pasivă utilizată pentru a stoca sau a prelua informații (de exemplu, un fișier de date, notat cu o_i).

Se presupune, de asemenea, existența unui **monitor de securitate** – subiect activat cu orice referire la obiecte și care poate distinge (pe baza unor reguli) și permite procesarea autorizată și respinge procesarea neautorizată, de exemplu accesul.

Accesul este interacțiunea dintre subiect și obiect, ca rezultat al transferului de informații între ele. Există două tipuri fundamentale de acces: **citirea** *(r, de la read)* **–** o operație, rezultatul căreia este transferul informațiilor de la obiect la subiect; **înregistrarea** *(w – de la write)* – o operație, rezultatul căreia este transferul de informații de la subiect la obiect. Dar pot fi definite și alte operații, de exemplu **e – executare***,* **o - posesie** *(de la own = proprietar),* **∅ –** mulțimea vidă/interzicerea oricăror operații.

În literatura de specialitate se disting două clase principale de modele ale politicii formale de securitate: *modele multinivel (discreționare, selective, mandatate)* și *modele multilaterlae*, succint examinate în continuare.

2.5.1. Modele de securitate informațională multinivel

Baza politicii de securitate multinivel este controlul caracterizat prin identificarea tuturor subiectelor și obiectelor de securitate și drepturilor de acces ale subiectului la obiectul sistemului, determinate pe baza unor reguli externe referitoare la sistem:

- Trebuie identificate toate subiectele și obiectele;
- Se specifică un set liniar de etichete de confidențialitate;
- Fiecărui obiect i se atribuie o etichetă de securitate care determină *nivelul său de secret*;

- Fiecărui subiect i se atribuie o etichetă de securitate care determină nivelul de încredere în acesta - *nivelul său de acces*;
- Decizia de a permite subiectului să acceseze obiectul se face pe baza tipului de acces și comparării etichetei subiectului și a obiectului.

Schematic, sistemul multinivel al securității poate fi reprezentat ca în *Fig. 3,* fiind divizat în straturi prin linii orizontale, prin care se realizează o delimitare netă între diferite categorii de informații din sistem *(de exemplu, publice, confidențiale, secrete, strict secrete*). Această delimitare asigură certitudinea accesării informațiilor dintr-o anumită clasă doar de subiecții *care au autorizația de același nivel sau mai mare*.

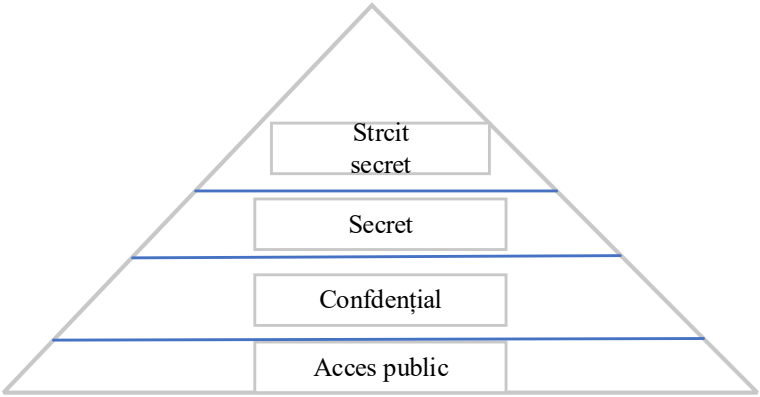

Fig. 3. Model de securitate multinivel

Acuma politicile de control a accesului pot fi foarte clar definite: informațiile vor circula doar de jos în sus; de sus în jos nu pot să circule decât dacă o persoană autorizată le declasifică. Cel mai des, politica de securitate multinivel este descrisă în termenii modelului Bell-LaPadula, unul dintre cele mai cunoscute modele al politicilor de securitate multinivel. Sistemele ce le adoptă sunt numite și „sigure multinivel" sau MLS (Multi Level Secure). Proprietatea de bază a acestor sisteme este aceea că informațiile pot circula în jos.

Formal, modelul Bell-LaPadula a introdus trei principii:

- Principiul securității simple, prin care nu-i este permis nici unui proces să citească date aflate pe un nivel superior lui.

Este cunoscut și ca *Nu citi deasupra (No Read Up, NRU);*

- Principiul * (stea): nici un proces nu poate să scrie date pe un nivel aflat sub el. Este cunoscut și ca *Nu scrie dedesubt (No Write Down, NWD);*
- Principiul securității discreționare – introduce o matrice de acces pentru a specifica controlul accesului discreționar. Este cunoscut și ca *Trusted Subject (subiect de încredere). Pentru detalii a se vedea ....*

Adesea, regulile de control discreționar al accesului sunt specificate în ***matricea de acces*** *(Tabelul 1)*. Într-o astfel de matrice, rândurile corespund subiecților sistemului, coloanele – obiectelor, elementele matricei descriu drepturile de acces pentru perechea corespunzătoare „subiect-obiect".

Tabelul 1

Exemplu de matrice a accesului

	o_1	o_2	o_3	o_4
s_1	rwe	∅	rw	Rw
s_2	E	rwe	r	∅

Acest tip de control al accesului este folosit în sistemele de operare datorită relativității ușoare de implementare. În acest caz, regulile de control a accesului sunt descrise prin intermediul listelor de control al accesului *(Control List Access, ACL).* ACL este asociată cu obiectul protejat și păstrează o listă cu subiecții și permisiunile lor pentru acest obiect.

Unul dintre cele mai cunoscute modele discreționare este modelul **Harrison-Ruzo-Ulman**, numit adesea **modelul matriceal**. Funcționarea sistemului rezumă în modificările aduse matricei de acces. Modelul definește 6 operații primitive: „a crea", „a distruge" obiectul și subiectul, „a crea", „șterge" dreptul de acces al subiectului la obiect. Descrierea acestora este prezentată în *Tabelul 2*.

Tabelul 2

Operații elementare ale modelului Harrison-Ruzo-Ulman

Operația	Rezultatul operației
„a crea” subiectul **s’**, unde s’$\notin$**S**	**S’**=**S**$\cup${s’}; **O’**=**O**$\cup${s’}; **M’**[s,o]= **M**[s,o] pentru orice s$\in$**S,** o$\in$**O**; **M’**[s’,o]= $\varnothing$ pentru orice o$\in$**O’**, **M’**[s,s’]= $\varnothing$ orice s$\in$**S’**
„a crea” obiectul **o’**, unde o’$\notin$**O**	**S’**=**S**; **O’**=**O**$\cup${o’}; **M’**[s,o]= **M**[s,o] pentru orice s$\in$**S,** o$\in$**O**; **M’**[s,o’]= $\varnothing$ pentru orice s$\in$**S’**
„a distruge” **s’**, unde s’$\in$**S**	**S’**=**S**\{s’}; **O’**=**O**\{s’}; **M’**[s,o]= **M**[s,o] pentru orice s$\in$**S’,** o$\in$**O’**;
„a distruge” **o’**, unde o’$\in$**O**	**S’**=**S**; **O’**=**O**\{o’}; **M’**[s,o]= **M**[s,o] pentru orice s$\in$**S’,** o$\in$**O’**;
„a crea” regula r’$\in$**R** în **M**[s’,o’], unde s’$\in$**S,** o’$\in$**O**	**S’**=**S**; **O’**=**O**; **M’**[s,o]=**M**[s,o] pentru s$\neq$s’,s$\in$**S’**, o$\neq$o’, o$\in$**O’**; **M’**[s’,o’]=**M**[s’,o’] $\cup${r’}
„a sterge” regula r’$\in$**R din M**[s’,o’], unde s’$\in$**S,** o’$\in$**O**	**S’**=**S**; **O’**=**O**; **M’**[s,o]=**M**[s,o] pentru s$\neq$s’,s$\in$**S’**, o$\neq$o’, o$\in$**O’**; **M’**[s’,o’]=**M**[s’,o’]\ {r’}

Starea inițială a sistemului este descrisă de mulțimea de drepturi/reguli de acces **R,** mulțimea de subiecți **S**, mulțimea de obiecte **O** (**S$\subseteq$O,** cu puterile mulțimilor **|S| = i, |O| = j, i $\leq$ j),** matricea de acces $\mathbf{M_{i\times j}}$ (elementul matricei care corespunde subiectului ***s*** și obiectuli ***o*** este notat **M[s,o]** și este o submulțime a setului de reguli). Starea finală (după operație) este **S', O', M', R** (setul de reguli nu se modifică).

Din operațiile primitive pot fi realizate comenzi. **Comanda** constă din două părți: starea în care este executată și secvența de instrucțiuni:

command C (x_1, …, x_k)*:*
    if $r_1 \in M[x_{s1}, x_{o1}]$ *and …* $r_m \in M[x_{sm}, x_{om}]$ *then*
    α_1;
    …
    α_n;
end,

unde $\mathbf{r_1, ..., r_m \in R}$ sunt reguli de acces, $\alpha_1, ..., \alpha_n$ - succesiuni de operații primitive.

De exemplu, comanda de creare a unui fișier *f* de subiectul *s* cu setul de drepturi de acces *citit, scris, proprietar:*

```
command «a crea fișier» (s, f)
    «a crea» obiect f;
    «a crea » regula de deținere own в M[s,f];
    «a crea » regula de citire read в M[s,f];
    «a crea » regula de scriere write в M[s,f];
end.
```

După cum arată rezultatele analizei acestui model de securitate, construirea unui algoritm pentru verificarea securității sistemelor conform politicii discreționare nu poate fi rezolvat în cazul general.

2.5.2. Modele ale securității informaționale multilaterale

Deseori, în realitate, preocupările noastre xe referă nu la prevenirea curgerii în jos a informațiilor, ci către stoparea fluxurilor între diferite compartimente. În astfel de sisteme, în locul frontierelor orizontale s-au creat altele verticale, conform *Figurii 4.*

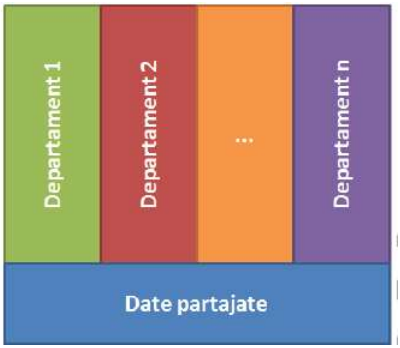

Fig. 4. Model de securitate multilateral

Acest control al fluxurilor informaționale laterale este unul organizațional, așa cum este cel al organizațiilor secrete, pentru păstrarea în taină a numelor agenților care lucrează în alte țări, fără să fie cunoscuți de alte departamente speciale. La fel se întâmplă și în

companii pentru separarea verticală a compartimentelor conform funcțiilor îndeplinite (producție, comercială, personal-salarizare etc.).

Există cel puțin trei modele diferite de implementare a controlului accesului și de control al fluxurilor informaționale prin modelul securității multilaterale:

Compartimentarea, folosită de comunitatea serviciilor secrete;

Zidul chinezesc, folosit la descrierea mecanismelor utilizate pentru prevenirea conflictelor de interese în practicile profesionale;

BMA (British Medical Association), dezvoltat pentru descrierea fluxurilor informaționale din domeniul sănătății, conform cu etica medicală.

Compartimentarea și modelul rețea

Ani mulți acest model a servit ca practică standard, în SUA și guvernele aliate, pentru restricționarea accesului la informații, prin folosirea cuvintelor-cod pentru decriptarea mesajelor criptate și a clasificărilor. Cercul persoanelor cu acces la mesajele decriptate fiind foarte redus, numărul autorizărilor pentru informații de pe cel mai înalt nivel de clasificare era mult mai mare. Prin folosirea cuvintelor-cod se creează o puternică subcompartimentare, chiar a categoriei strict secret și deasupra ei.

Cuvintele-cod sunt folosite pentru crearea grupurilor de control al accesului printr-o variantă a modelului Bell-LaPadula, numită modelul rețea. Clasificările, împreună cu cuvintele-cod, formează o rețea, conform *Fgurii 5.*

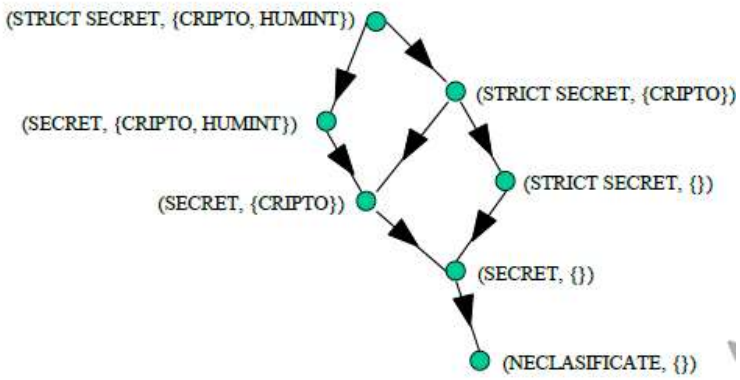

Fig. 5. Model rețea cu etichete de securitate

Potrivit modelului, o persoană autorizată să aibă acces la informații SECRETE nu poate accesa informații SECRETE CRIPTO, dacă nu are și autorizație pentru CRIPTO.

Ca un sistem să răspundă acestor cerințe, va trebui ca problemele clasificării informațiilor, ale autorizării persoanelor și ale etichetelor ce însoțesc informațiile să se transfere în politica de securitate pentru a defini țintele securității, modul de implementare și evaluare.

Modelul zidului chinezesc

Modelul a fost realizat de Brewer și Nash. Numele provine de la faptul că firmele care prestează servicii financiare, cum sunt băncile de investiții, au normele lor interne pentru a preveni conflictul de interese, norme numite de autori zidul chinezesc. Aria de aplicare este, însă, mai largă. Se poate spune că toate firmeleprestatoare de servicii au clienții lor și pentru a-i păstra se află într-o veritabilă competiție. O regulă tipică este următoarea: „un partener care a lucrat recent pentru o companie dintr-un anumit domeniu de activitate nu poate să aibă acces la documentele companiilor din acel domeniu", cel puțin pentru o perioadă controlată de timp. Prin aceasta, caracteristica modelului zidului chinezesc constă într-un mix de libertate de opțiune și de control obligatoriu al accesului: oricine este liber să lucreze la orice companie, dar îndată ce a optat pentru una, se supune restricțiilor ce operează în domeniul respectiv de activitate.

Modelul zidului chinezesc introduce principiul separării obligațiilor de serviciu: un utilizator anume poate să prelucreze tranzacțiile A sau B, nu amândouă. Așadar, putem spune că modelul zidului chinezesc aduce elemente noi pe linia controlării accesului

Modelul BMA (British Medical Association)

În domeniul medical sunt confruntări serioase privind tocmai sistemele de securitate a datelor pacienților. În efortul multor țări de a introduce carduri inteligente cu datele medicale personale, se înregistrează o puternică opoziție din partea publicului. Acesta invocă vulnerabilitatea individului prin trecerea informațiilor despre anumite boli foarte grave, purtate până acum pe brățara de la mână, pe cartela inteligentă, ceea ce va face ca atunci când se va afla în avion, în țări străine, să fie foarte greu sau chiar imposibil să i se citească

informațiile respective. O altă problemă se referă la păstrarea secretului datelor personale sau a unei părți dintre acestea.

Cea mai mare temere vine din cauza proliferării practicilor de inginerie socială, putându-se afla cu multă ușurință date personale din baze de date medicale.

Scopul modelului politicii de securitate BMA este acela de consolidare a principiului consimțământului pacientului și de a preveni accesul prea multor persoane la datele personale din bazele de date ce le conțin. Totul s-a rezumat la un nou sistem de codificare. Politica BMA se bazează pe nouă principii, formulate foarte pe scurt astfel:

- controlul accesului,
- deschiderea înregistrărilor, c
- controlul modificărilor din liste,
- consimțământul și notificarea clientului,
- persistența,
- marcarea accesului pentru a servi ca probă în justiție,
- urmărirea fluxului informațiilor,
- controlul agregării informațiilor,
- încrederea în sistemele informatice.

Rezumat

În SIC, informațiile constituie cea mai importantă resursă a organizației care adaugă valoare organizației. Ca urmare, informațiile trebuie protejate și securitatea informațiilor devine unul dintre cele mai fierbinți subiecte și una dintre cele mai prioritare sarcini a sistemului managerial al organizațiilor.

Doar pe termen scurt (de exemplu, în timpul transportării) securitatea presupune îndeplinirea atributelor de *accesibilitate, integritate, disponibilitate, confidențialitate.* Pentru protecția valorilor organizațiilor și asigurarea continuității serviciilor pe termen lung sunt necesare și alte măsuri:

- **preventive** (instruirea *utilizatorilor*, coduri de *conduită* etc.);
- **protective** (echipamente și *dispozitive* securizate; *reglementări*)*;*
- **de reacție/combatere** *(*crearea și *specializarea* organismelor

abilitate de lege; cooperare între sectorul public și cel privat; *cooperare* internațională);

- **de revizuire** *și* perfecționare *continuă* (adaptarea la noile *tehnologii*, viruși etc.).

Cele mai bune practici ale SMSI sunt descrise în Standardele „ISO/IEC 27001:2005 Sistemul de Management al Securității Informației" (fost BS 7799-2) și „ISO/IEC 27002:2005, Corecția 1:2007. Cod practic pentru Managementul Securității Informației" (fostul standard britanic BS 7799-1, ulterior ISO/IEC 17799) și ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls. Second edition, 2016, (http://www.iso27001security.com/html/27002.html/)

Totuși, la crearea SMSI, este necesară luarea în considerare nu doar a cerințelor stabilite în standarde, ci și specificul organizației, programul și politicele prestabilite de securitate.