Concepte şi descriptori ai funcţiilor de securitate utilizaţi în Sistemele Integrate de Informatică şi de Comunicaţii (S.I.I.C.)

Drd. ing. & Psih. Gheorghiţă PESCARU

Rezumat. *Conceptul de securitate capătă noi semnificaţii semantice şi noi viziuni, pe măsură ce tehnologia informaţiei şi sistemele de comunicaţii se dezvoltă şi avansează. Nu mai putem vorbi despre securitate dacă nu extindem conceptul la nivel de sistem şi macrosistem. Articolul de faţă îşi propune să abordeze conceptul de securitate considerînd un sistem format din trei componente funcţionale: componenta „comunicaţii", componenta „informatică" şi componenta „informaţii" care circulă între (sau prin) celelalte două.*

Cuvinte cheie: *securitate, informaţii, comunicaţii, informatică*

Abstract. *While information tehnology and communications systems are developing and advancing, the security concept is getting new semantics and visionals. We cannot speak anymore about security if we don't extend the concept at system and macrosystem level. The present paper is aiming to approach security concept by considering a system containing 3 functional components: the „communications" component, the „informatic" component and the „information" passing betwen the previously ones.*

Keywords: *security, information, communications, informatic*

1. Introducere. Securitatea şi buna funcţionare a unui S.I.I.C. Calitatea informaţiei.

Într-o epocă a informaţiei, buna funcţionare şi atacurile asupra sistemelor informaţionale şi de comunicaţii sînt deja fapte curente în viaţa cotidiană. Îngrijorătoare este însă conturarea unei ameninţări „strategice tehnice". Atât mediul natural cît şi mijloacele hardware şi software care există în prezent pot cauza daune serioase bunurilor informaţionale ale unui Sistem Integrat de Informatică şi de Comunicaţii, S.I.I.C., putînd compromite nu numai buna sa funcţionare dar şi integritatea informaţiei vitale. În prezent, simpla existenţă a formelor şi a mijloacelor prin care se pot produce diverse agresiuni, cuplate cu multitudinea motivelor şi oportunităţilor care există, reflectă multiple vulnerabilităţi. Aceste circumstanţe cer acţiuni în interesul unui S.I.I.C., printr-o atitudine mult mai analitic „pro-activă" decît defensivă. Informaţia a îmbunătăţit în mod efectiv eficienţa tuturor aspectelor legate de atacul informaţional, de la logistică la comandă, control, comunicaţii, calculatoare, informaţii, precum şi supravegherea şi securitatea acestora. Componentele funcţiilor de securitate reprezintă baza cerinţelor funcţionale de securitate exprimate pentru un Sistem Integrat de Informatică şi Comunicaţii (S.I.I.C.). La rîndul lor, cerinţele trebuie să definească comportamentul de securitate aşteptat (prognozat) faţă de

[1] Institutul Naţional de Studii şi Cercetări pentru Comunicaţii.

riscurile şi vulnerabilitățile stabilite ale S.I.I.C. În plus, cerințele de securitate definesc – prin concepte şi descriptori specifici – proprietățile de securitate pe care atît utilizatorii/beneficiarii le pot utiliza în momentul interacțiunii cu S.I.I.C., cît şi răspunsul acestuia față de solicitările utilizatorilor/beneficiarilor (fig. 1).

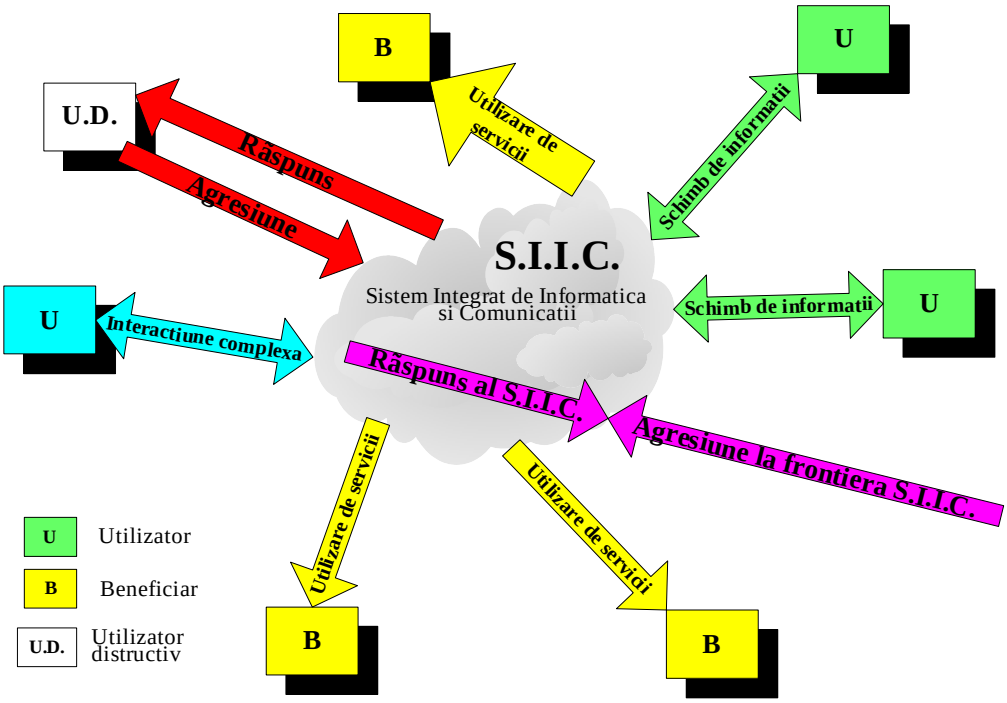

Fig. 1. Interacțiunile dintre un S.I.I.C. şi mediul îmconjurător.

Componentele funcțiilor de securitate pentru un S.I.I.C. **exprimă holistic cerințele de securitate menite a contracara riscurile şi vulnerabilitățile din mediul de funcționare stabilit pentru sistemul S.I.I.C. în ansamblul său.** Ele cuprind premisele de securitate şi politicile de securitate organizaționale sau/şi de sistem folosite.

Politica de Securitate (P.S.) a informațiilor este rezultatul necesității alinierii şi integrării unui S.I.I.C. în noile contexte tehnice, economice şi socio-umane şi **argumentează orientarea resurselor disponibile din S.I.I.C. pentru a satisface cerințele impuse**. Prin Politica de Securitate factorii de decizie ai S.I.I.C. transpun în practică noțiunile şi conceptele articulate într-un mod unitar aplicîndu-le la particularitățile S.I.I.C. În acest context, consider că politica de securitate a informațiilor într-un S.I.I.C. trebuie văzută prin prisma următorilor termeni:

– ***siguranța informațională*** (fig. 2) (a sistemelor, rețelelor informatice şi de comunicații, a mediilor de securitate) ce reprezintă toate măsurile care pot fi luate (împreună sau separat) din punct de vedere **software şi orgware**[1] pentru ca informația legală care circulă prin aceste medii şi sisteme să nu fie modificată, alterată, ştearsă sau citită de utilizatori care nu au dreptul legal de acces la ea;

– ***securizarea informațională*** (fig. 3) (a sistemelor, rețelelor informatice şi de comunicații, a

1 Orgware = ştiința organizării informației şi a fluxurilor informaționale din cadrul unei activități oarecare astfel încît să conțină „**maximum de informație concentrată în minimum de resursă semantică** şi care să conducă la optimul activității respective.

mediilor de securitate) reprezintă toate măsurile de tip **hardware** care pot fi luate astfel încît informația legală care circulă prin aceste sisteme să ajungă la destinație **la timpul şi locul prestabilit**.

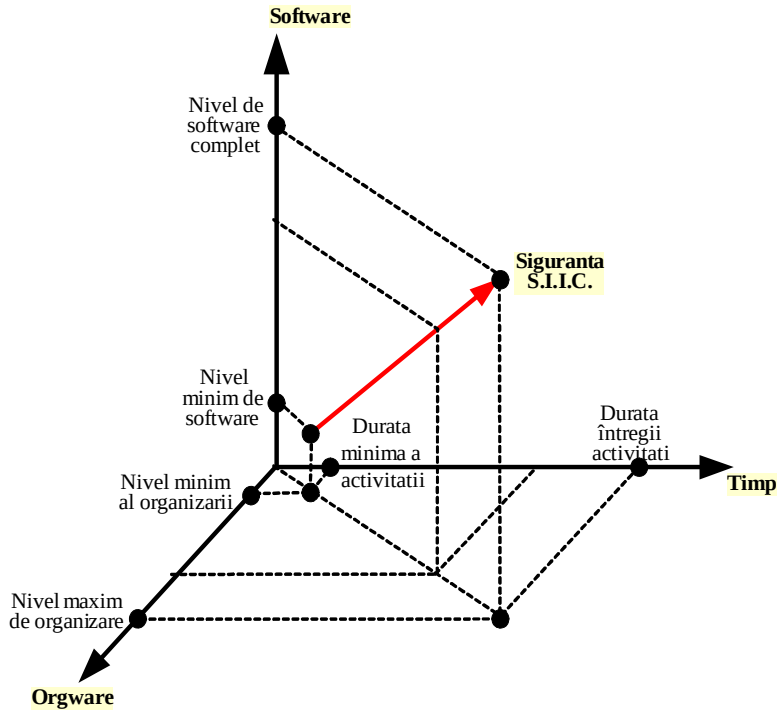

Fig. 2. Reprezentarea vectorului de siguranță.

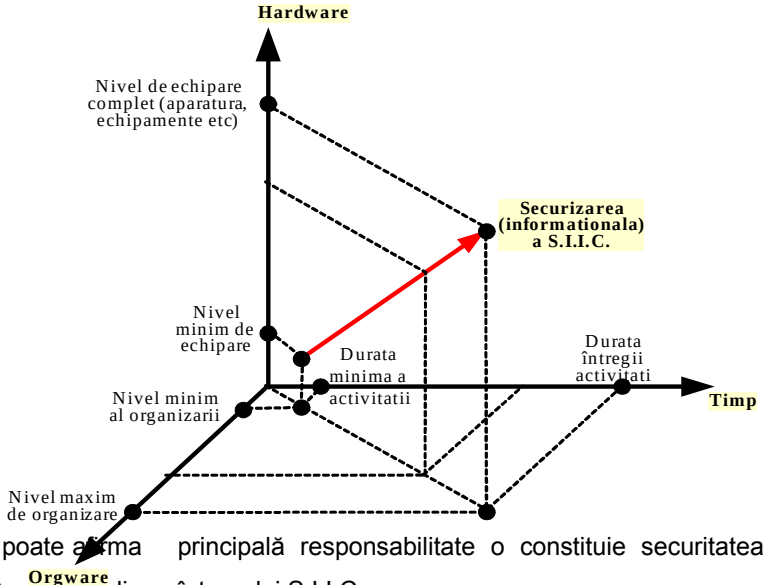

Fig. 3. Reprezentarea vectorului de securizare (informațională) a S.I.I.C.

Avînd în vedere cele de mai sus, se poate afirma că politica de securitate a unui S.I.I.C. consta din totalitatea resurselor hardware, software, firmware şi orgware aparținînd S.I.I.C. care veghează la funcționarea în parametri proiectați ai sistemului. De aceea, pentru realizarea funcțiilor de securitate, un S.I.I.C. va trebui să conțină o entitate de sine-stătătoare a cărei principală responsabilitate o constituie securitatea întregului S.I.I.C.

Componenta de Securitate (notată mai departe cu C.S.) îşi îndeplineşte atribuțiile printr-un „set" de interacțiuni (reguli bine definite) ce formează Domeniul de Control (DC) al C.S. Aceste reguli **cuprind modalități predefinite de acțiune, operare, evidență**

şi interdicții, sesiuni de lucru, perioade de timp, valori maxime şi minime de parametri, admise pentru protejarea resurselor proprii S.I.I.C.

De exemplu, în C.S. sunt stabilite perioadele de interacțiune dintre utilizatori/beneficiari şi S.I.I.C. în cadrul unei/unor sesiuni de lucru de utilizator. Aceste sesiuni de lucru se pot controla în baza unor considerații din Politica de Securitate (P.S.) şi S.I.I.C., ca de exemplu:

– **autentificarea** unui utilizator;
– **momentul din zi** în care accesează S.I.I.C.;
– **metoda** de accesare a S.I.I.C. şi resursa utilizată;
– **numărul de sesiuni** folosite;
– **nivele de acces** permise/interzise.

În acest sens, C.S. foloseşte termenul de Autorizat pentru a semnifica un utilizator care are drepturile şi/sau privilegiile şi/sau interdicțiile necesare pentru a efectua o operație în cadrul S.I.I.C.

Deoarece întreaga funcționare (eficientă) a unui S.I.I.C. se bazează pe o bună administrare (management), C.S. impune ***sarcini separate şi delimitări precise*** ale diverşilor administratori ai S.I.I.C., definind Roluri Administrative (R.A.) pentru fiecare dintre aceştia.

Un rol este un set predefinit de reguli ce stabileşte interacțiunile permise dintre un administrator (manager) şi funcțiile de operare S.I.I.C. ***În P.S. vor fi structurate şi precizate lingvistic, semantic şi tehnic proprietățile şi regulile de securitate ale fiecărui R.A.*** Pe de altă parte, un S.I.I.C. poate cuprinde două clase de entități (resurse proprii):

- ***entități active*** adică entități/resurse ce stau la baza diferitelor acțiuni, operații, sesiuni ce se derulează în interiorul S.I.I.C. şi determină operații asupra Fluxurilor de Informații (F.I.) din S.I.I.C. (de exemplu transport, prelucrare, stocare, arhivare de date) (fig. 4);
- **entități pasive** adică entități/resurse constituite din „containere" de unde pleacă sau unde sunt stocate informațiile şi datele din S.I.I.C.

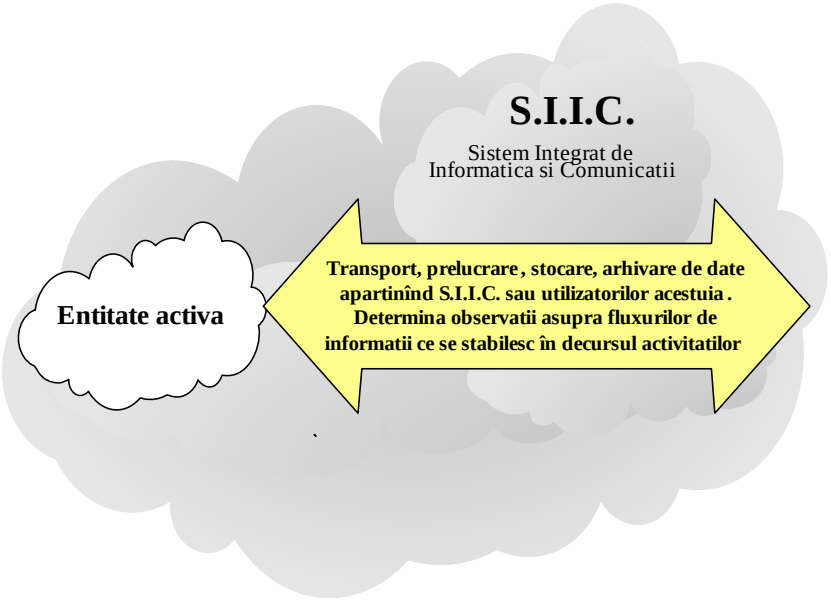

Fig. 4. Interac'iuni dintre un S.I.I.C. şi o entitate activă din interiorul său.

Politica de Securitate a S.I.I.C., P.S., creează şi gestionează reguli şi norme ce se stabilesc în cadrul interacțiunilor dintre utilizatori/beneficiari ai S.I.I.C. şi S.I.I.C. În cadrul P.S. utilizatorii, resursele S.I.I.C. şi

cerinţele funcţionale de securitate deţin ***atribute*** ce conţin date şi informaţii ce permit S.I.I.C. să se comporte corect. De exemplu, unele atribute, cum ar fi numele fişierelor, pot avea diferite scopuri informaţionale (să crească gradul de accesibilitate, user-friendly, al S.I.I.C.) în timp ce altele, cum ar fi informaţiile de control acces, pot fi restrictive prin aplicarea P.S. Aceste atribute din urmă sunt denumite, în general, ***atribute de securitate*** ale S.I.I.C.

În concepţia unei politici de securitate a unui S.I.I.C. agresiunea informaţională poate implica atacuri fizice asupra informaţiei, asupra proceselor informaţionale, asupra infrastructurii proprii sau a celor partenere şi în urma cărora se compromite, se alterează, se produc daune, se întrerupe, se întîrzie, se distruge informaţia (eventual combinaţii ale acestor forme) cu efecte în confuzia şi/sau blocarea proceselor decizionale. Managementul de securitate al unui S.I.I.C. consideră că importanţa şi amploarea agresiunii informaţionale trebuie multiplicată şi prin prisma următorilor trei factori:

– poate avea o precizie mare la un preţ scăzut, ceea ce lărgeşte aria de acţiune a potenţialilor agresori;

– nu necesită o participare directă, fizică, putîndu-se produce la / de la distanţă şi din orice punct geografic;

– se poate desfăşura în mare secret, intenţiile şi urmele acţiunilor putînd fi şterse;

– atunci cînd sînt mai mult decît un incident izolat, agresiuni de acest gen creează o percepţie a vulnerabilităţii, a pierderii controlului, subminînd încrederea autorităţilor şi a societăţii civile în posibilităţile unui S.I.I.C. de a asigura securitatea informaţională.

Această reacţie neliniară între daunele reale suferite de o structură / reţea de comunicaţii constituită într-un S.I.I.C. şi costurile efective ale agresiunilor informaţionale face ca acestea să constituie o provocare specială, creind disproporţii între răspunsurile raţionale (şi tradiţionale) şi eficienţa lor. ***Cum poate, în aceste cazuri, să răspundă un S.I.I.C. unui atac informaţional? De cele mai multe ori nici nu există un consens privind modul de a trata un astfel de atac, chiar şi pentru specialiştii în domeniul securităţii sistemelor integrate.***

Există decidenţi care pot sugera că S.I.I.C-urile (în special cele de însemnătate ridicată) nu sînt vulnerabile la atacurile informaţionale datorită faptului că aceste S.I.I.C-uri pot avea o oarecare cantitate de rezistenţă şi chiar de „elasticitate”. Argumentările sînt bazate pe scoaterea în evidenţă a suprapunerilor şi redundanţelor acestor echipamente şi resursele acestor S.I.I.C-uri şi de aceea se consideră a fi foarte greu, pentru oricine, să distrugă sau să penetreze un set dat de servicii (software, de comunicaţii, transport, stocare etc.). Totodată, anumite lipsuri în interconectarea şi interoperabilitatea sistemelor sînt folosite ca argumente ale imposibilităţii ajungerii potenţialilor agresori în diverse sisteme „mai slabe” din punct de vedere al securităţii informaţionale şi folosirea acestora drept căi de acces pentru a ataca alte sisteme. Este susţinută (chiar greşit) ideea potrivit căreia unele S.I.I.C-uri şi interconexiunile lor sînt dificil de înţeles pentru potenţialii atacatori.

Din punct de vedere al securităţii informaţionale, cinci puncte trebuie subliniate:

• Important nu este dacă o agresiune poate sau nu să distrugă parţial sau în totalitate un S.I.I.C sau un serviciu, ci **dacă sînt suficiente daune pentru a atrage atenţia şi a provoca un comportament de panică** ceea ce poate crea, la rîndul său, o problemă semnificativă de importanţă economică, politică, socială, strategică, de imagine etc. A reduce sau chiar a anula încrederea acordată unui S.I.I.C. ca şi componentă a economiei unei companii, firme etc. reprezintă totuşi o problemă;

• Redundanțele în S.I.I.C.-uri sînt numai parțiale şi, de multe ori, neplanificate şi **neplanificate la nivel macrosistemic**.

• O parte dintre S.I.I.C-uri au fost proiectate şi construite **cu puțină sau chiar fără atenția** cuvenită pentru funcțiile de securitate, fiind astfel mai dificil de protejat şi securizat.

• Deoarece dinamica activității creşte, cresc şi nevoile de interconexiune şi interoperabilitate astfel încît din ce în ce mai multe S.I.I.C-uri sînt interconectate prin „lucrări auxiliare". Aceste modalități compromit în cele mai multe cazuri factorul securitate informațională şi / sau funcțională.

• Lipsa de securitate informațională şi / sau funcțională sau existența unor forme neadecvate ale lor poate conduce la **renunțarea cererii de servicii,** concomitent cu **scăderea nivelului de încredere**.

La nivel de generalitate se poate afirma că informatizarea globală a societății poate duce la punerea accentului pe latura folosirii mult mai intense a intruziunii informaționale ca formă de obținere mai economică, mai eficientă şi pe termen lung a dominației. Această situație, fără a schimba fondul problemelor puse în discuție, le poate îmbogăți radical conținutul şi va determina creşterea bruscă a eficacității în îndeplinirea obiectivelor de securitate informațională şi de funcționare în ansamblu.

2. Calitatea informației (de securitate)

Din punct de vedere al conținutului semantic al domeniului de **securitate integrată a sistemelor**, calitatea informației exprimă **gradul de precizie al sintezei dintre laturile şi însuşirile esențiale ale obiectelor, fenomenelor sau abstractizărilor**. Definiția este absolut necesară la stabilirea nivelului de clasificare al informațiilor într-un S.I.I.C.

Calitatea informației poate fi exprimată de relația:

$$C.I. = \sum_{i=1}^{\infty}(Si + Pi + Ui)$$

în care: **C.I.** reprezintă **calitatea informației**, ca produs cartezian al noțiunilor de semnificat[1] şi semnificant[2] (fig. 5.); S_i este suma tuturor **semnificațiilor** pe care o informație de securitate le poate căpăta în raport cu unul sau mai multe sisteme de gîndire (tehnic, economic, filosofic, socio-uman, etc); U_i reprezintă suma **utilităților** pe care o informație de securitate le poate avea într-un moment de timp dat; P_i reprezintă suma tuturor **ponderilor** pe care o informație de securitate le poate avea într-un sistem de tipul S.I.I.C. Ponderea informației de securitate **arată efectul** pe care aceasta îl poate produce **prin cunoaşterea şi interpretarea ei.**

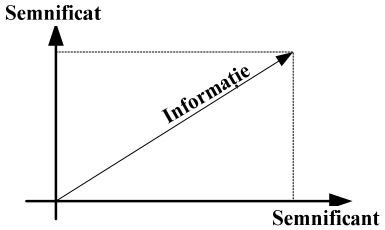

Fig. Relația dintre semnificat şi semnificant.

Demersurile cognitive şi evoluția acestora (pre – acțiune şi conceptualizare a securității informaționale) în concepția P.S. sînt date de algoritmul prezentat mai jos (fig. 6), în care se definesc şi conceptele de „strategie[3]" respectiv „tactică[4]":

Notă. În cadrul politicii P.S. a S.I.I.C. vor fi specificați şi ***coeficienții de importanță*** cu care vor

[1] *Semnificat* = sens al unui cuvînt raportat la cultura din care provine.
[2] *Semnificant* = Este o realizare materială a semnului lingvistic (ex. forma grafică, complex sonor) ce constituie *suportul unui sens atribuit.*
[3] *Strategie* = set de căi şi mijloace puse în aplicare de către factorii de decizie pentru atingerea unui (unor) scopuri declarate prin politica de securitate PS a S.I.I.C.
[4] *Tactică* = Reprezintă decizii privind acțiuni pe termen scurt pentru realizarea unei strategii din cadrul politicii de securitate P.S. a S.I.I.C.

fi ponderate **criteriile de decizie**. Aceşti coeficienţi de importanţă **fac parte din politica decizională** a conducerii unui S.I.I.C.

Obiectivele vizate de politica şi strategiile de securitate integrată sînt legate de:

• circulaţia informaţiei. În atenţie vor fi:

– mediul (mediile[1]) prin care circulă informaţia; în raport cu acestea;

– protocoalele de acces;

– protocoalele de transport;

– protocoalele de protecţie ale mediilor de circulaţie a informaţiei.

Ţinte vizate la circulaţia informaţională:

– accesul neautorizat în (la) mediul de circulaţie al informaţiei;

– distrugerea mediilor de circulaţie a informaţiei (transport, prelucrare, stocare, arhivare a informaţiei).

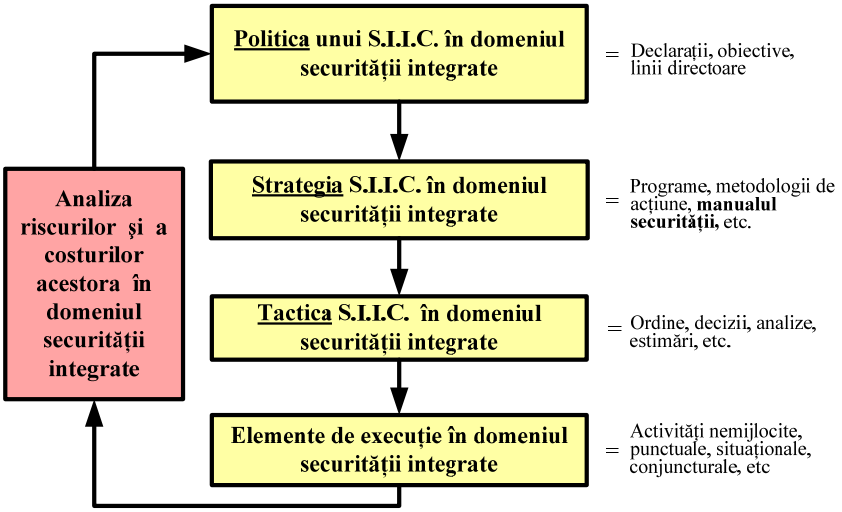

Fig. 6. Algoritm de realizare evolutivă a activităţilor de securitate integrată.

• conţinutul semantic al informaţiei[2]. În atenţie vor fi:

– integritatea informaţiei;

– disponibilitatea informaţiei;

– non-repudierea informaţiei.

Ţinte vizate la conţinutul semantic al informaţiei:

– modificarea conţinutului semantic al informaţiei pentru obţinerea unui sens diferit al acesteia;

– trunchierea informaţiei pentru reducerea cantitativă a acesteia;

– ştergerea informaţiei şi crearea imposibilităţilor de acţiune;

– întîrzierea informaţiei pentru pierderea operativităţii sau refuzul primirii ei.

Prin politica de securitate a informaţiilor, un S.I.I.C. vizează următoarele scopuri:

• *întocmirea şi redactarea propriu-zisă a unui document de sine-stătător*, într-o formă lingvistică adecvată, pentru înţelegerea corectă a tuturor activităţilor desfăşurate în domeniul securităţii informaţionale faţă de pericolele şi ameninţările la care trebuie să facă faţă;

• *asigurarea suportului conceptual şi teoretic* privind activitatea de securitate a informaţiilor care să-i confere, în contextul legislativ actual, capacitatea de

[1] Ne referim aici la mediile specifice activităţii unui S.I.I.C.
[2] Reprezintă totalitatea sensurilor precis determinate ce conduc la claritatea şi precizia deciziilor şi a modurilor de acţiune pentru un eveniment (situaţie) dat(ă).

a-şi proteja identitatea, „bunurile informaționale" şi cele materiale precum şi de a putea răspunde adecvat la orice încercare de prejudiciere a acestora;

- *stabilirea principiilor de interconexiune ale S.I.I.C.* cu alte entități similare ce formează comunitatea operatorilor de comunicații. Sînt stabilite, astfel, şi reguli de cooperare, conlucrare, colaborare şi interese comunitare în domeniul securității integrate pentru cunoaşterea, prevenirea şi contracarare (potrivit domeniilor de competență) a amenințărilor comune şi specifice;
- instituirea unei terminologii clare, precise, de comun acord, care să asigure compatibilitatea cu alte entități cu atribuții în domeniul securității integrate.
- participarea şi dezvoltarea de relații şi cooperări internaționale, schimb de experiență în domeniul securității integrate şi al co-domeniilor acestuia, pentru creşterea nivelului de încredere acordat S.I.I.C

C.S., în procesul de analiză şi stabilire a strategiilor urmărite din P.S. realizează o corelație optimă între metode şi tehnici specifice prin care caută să stabilească, permanent, relații logice cauză → efect față de diferite disfuncții şi vulnerabilități pe de-o parte, şi factori de risc şi amenințări pe de altă parte. Analizele şi strategiile stabilite de C.S. vor fi dependente de:

- nivelul şi amploarea informațiilor protejate (securizate);
- relevanța acestora în cadrul bunei funcționări a S.I.I.C. contribuind la eliminarea incertitudinilor şi avînd ca rezultat obținerea protecției sigure a S.I.I.C.
- elementele de patrimoniu ale S.I.I.C.

3. Definirea unui S.I.I.C

Pentru ca cerințele de mai sus să poată fi puse în practică într-un mod eficient, sînt necesare o serie de etape preliminare în care se va stabili cu maximum de precizie toate informațiile definitorii pentru un S.I.I.C.:

1. **Prima etapă** trebuie să fie clarificarea preliminară, şi probabil pur conceptuală, a definirii generale a S.I.I.C., în măsură să determine ulterior o definire concisă şi neechivocă. Această definiție trebuie să se refere la următoarele :

– tipul serviciilor oferite de S.I.I.C. (servicii de voce, date, multimedia, transport, comunicații, servicii comunicații militare, guvernamentale, urgențe, utilitare etc.) şi, odată cu acestea, a informațiilor care trebuie stocate, procesate sau transmise;

– tipul şi categoria utilizatorilor;

– funcțiile operaționale;

– cerințele operaționale pentru schimbul de informații şi / sau interfețele cu alte S.I.I.C.

Aceste informații sunt necesare nu doar pentru a furniza baza pentru stabilirea cerințelor de securitate şi pentru dezvoltarea inițială a P.S., dar şi pentru a asigura un punct de referință pentru viitor. Un element esențial al acestor informații este că trebuie să includă definirea limitelor S.I.I.C. Această delimitare, într-un mediu de rețea, poate fi greu de definit, dar este fundamentală atunci cînd se ia în considerare interconectarea mai multor rețele S.I.I.C. Rolul S.I.I.C. şi, de aici, conținutul P.S. trebuie definit în termeni fizici, cu ieşiri clar definite către alte S.I.I.C. Cerințele de funcționalitate pentru, de exemplu, un firewall, sistem de pază, porți de acces, trebuie să fie incluse întotdeauna în Strategia de Securitate (S.S.) a S.I.I.C. Pentru stabilirea bazei privind cerințele de securitate, sunt cerute informațiile relevante pentru securitate referitoare la rolul operațional al S.I.I.C. Este esențial să fie creat un punct de referință clar definit care să identifice rolul S.I.I.C, tipul, volumul şi nivelul de clasificare al informațiilor care trebuie stocate, procesate sau transmise şi

numărul şi drepturile de acces ale tuturor utilizatorilor (fig. 7).

2. **A doua etapă** o constituie definirea cerinţelor de securitate. Dat fiind faptul că scopul principal al P.S. este acela de a reprezenta baza pentru protecţia şi buna funcţionare a S.I.I.C., C.S. trebuie să fie consultată cu privire la cerinţele de securitate ale S.I.I.C. privite ca un întreg, furnizîndu-i acesteia informaţii despre ameninţări şi informînd-o dacă unele cerinţe de securitate se situează la nivelul minim prevăzut de standardele de securitate P.S. Aceasta poate da o varietate de interpretări despre ceea ce înseamnă pentru un S.I.I.C să fie sigur.

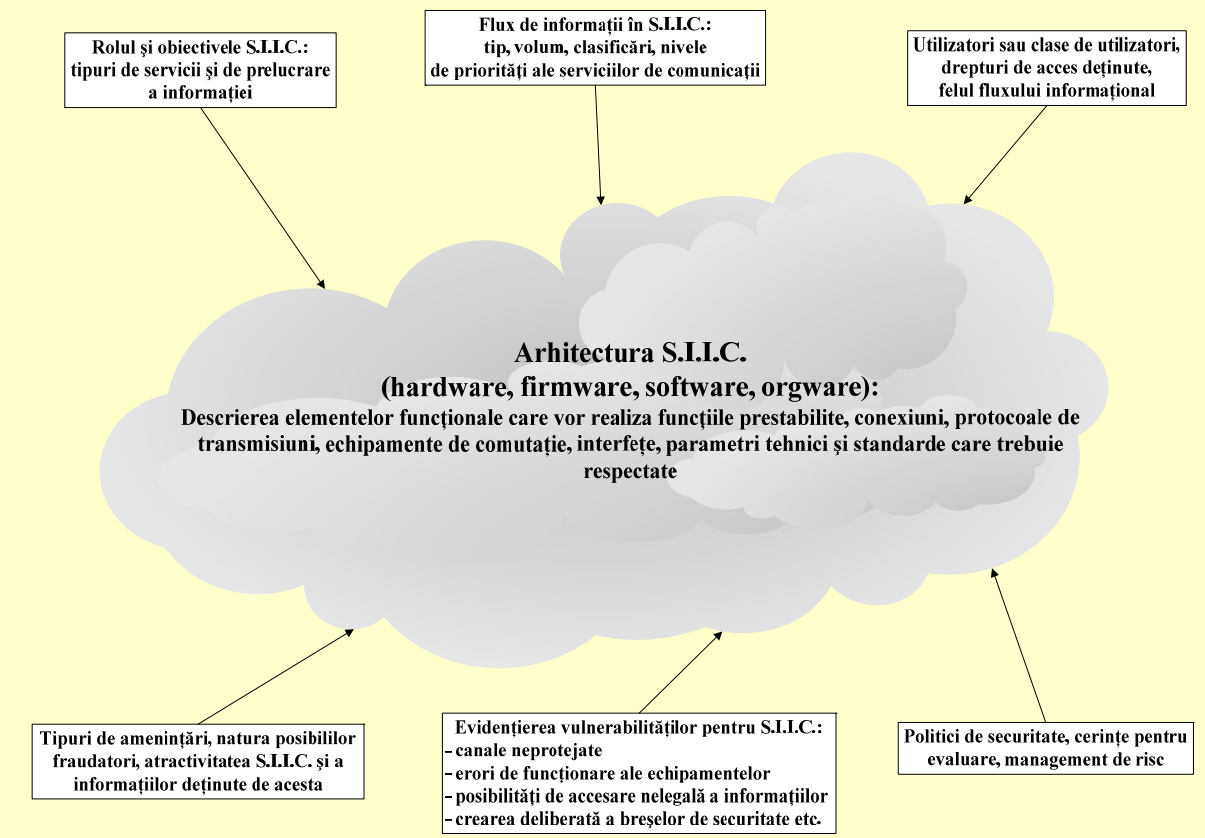

Fig. Informaţii necesare pentru definirea unui S.I.I.C.

3. **A treia etapă** o constituie definirea mediilor de securitate. Termenii acceptaţi de literatura de specialitate[1] şi utilizaţi pentru stabilirea limitelor de responsabilitate privind securitatea unui S.I.I.C. sunt următorii:

– ***mediul de Securitate Globală (MSG)*** - este mediul de securitate fizică generală în care este localizat S.I.I.C. care, în cazul unor reţele de comunicaţii, poate cuprinde un număr de medii globale disjuncte între ele. Această situaţie poate necesita un anumit grad de interpretare şi ea trebuie rezolvată cu soluţii de bază de la caz la caz;

– ***mediul de Securitate Locală (MSL)*** - este mediul de securitate fizică, a personalului, a documentelor şi procedurală, care revine în domeniul de responsabilitate al C.S.;

– ***mediul de Securitate Electronică (MSE)*** - este mediul de securitate al S.I.I.C. însuşi (de exemplu,

[1] Mă refer aici la reglementările O.R.N.I.S.S.

interfețele om-maşină, interfețele interne şi externe, firewall, sistemul de pază şi intrările - ieşirile către alte S.I.I.C.).

Toate măsurile de securitate identificate trebuie să fie aplicabile acestor medii. În unele situații, datorită unor cerințe particulare, este indicat să se adopte mai multe interpretări graduale, ca de exemplu, divizarea Mediului de Securitate Locală (MSL) în zone Clasa I, Clasa II şi administrative sau divizarea Mediului de Securitate Electronică (MSE) în domenii cu diferite nivele de asigurare.

4. **A patra etapă** o constituie definirea măsurilor de securitate. Principiul fundamental al securității este acela că diferitele aspecte ale acesteia (fizice, a software-ului, a personalului, a documentelor, procedurale, etc.) privind confidențialitatea, integritatea şi disponibilitatea, trebuie să fie tratate ca un tot unitar care furnizează un nivel corespunzător de protecție a informațiilor vehiculate, bunurilor şi capabilităților S.I.I.C. Politica de Securitate P.S. asigură o tratare integrală a securității, statuînd nivelul maxim al cerințelor de securitate pentru un S.I.I.C., înainte de stabilirea măsurilor particulare care trebuie să fie luate pentru implementarea cerințelor. Strategia de Securitate aferentă P.S. identifică un set de principii generale de securitate referitoare la controlul accesului, autentificare, evidență, audit, refolosirea obiectelor, integritate, disponibilitate şi schimbul de informații (securitatea comunicațiilor). Măsurile de securitate pentru fiecare dintre acestea trebuie discutate, stabilite şi aplicate în concordanță cu riscurile particulare identificate în cerințele de securitate.

4. Categorii de măsuri de securitate

4.1. Măsuri tehnice de securitate

Măsurile tehnice de securitate vizează capabilitățile de securitate care sunt încorporate în hardware-ul, software-ul, firmware-ul echipamentelor, de exemplu mecanisme de control al accesului, mecanisme de identificare şi autentificare, metode de criptare, software pentru detecția intruziunilor etc.

• **Măsuri tehnice de prevenire**. Au rolul de a opri încercările de încălcare a securității S.I.I.C şi pot asigura:

– identificarea. Oferă posibilitatea de a identifica în mod unic utilizatorii, procesele şi resursele sistemului. Ele constituie totodată şi baza pentru implementarea altor măsuri de securitate, cum ar fi controlul discreționar al accesului, controlul obligatoriu al accesului autorizat, evidența, măsuri pentru care este esențial să fie identificați, atît subiecții, cît şi obiectele;

– autentificarea. Permite verificarea identității unui subiect pentru a se asigura că identitatea pretinsă este cea adevărată. Mecanismele de autentificare includ parole, numere personale de identificare (PIN) şi noi tehnologii de autentificare, ca de exemplu token-uri, smart card-uri, certificate digitale, Kerberos);

– accesul. Oferă posibilitatea specificării şi gestionării ulterioare a acțiunilor permise utilizatorilor unui S.I.I.C. De exemplu, deținătorul informațiilor sau administratorului bazei de date stabileşte cine poate să actualizeze un fişier partajat, accesat de un grup de utilizatori conectați în rețea;

– controlul accesului. Integritatea şi confidențialitatea datelor sunt realizate prin măsuri de control al accesului. Atunci cînd subiectul care solicită accesul a fost autorizat să acceseze anumite procese sau informații, este necesară impunerea controlului discreționar sau obligatoriu al accesului autorizat. Aceste măsuri sunt realizate prin mecanismele de control al accesului implementate în sistem, de exemplu etichete obligatorii pentru nivelul de secretizare al informațiilor, seturi de permisiuni pentru controlul accesului discreționar la fişiere, liste de control al accesului, profilurile utilizatorilor;

– nerepudierea. Are drept scop asigurarea că expeditorii nu pot nega transmiterea informațiilor şi destinatarii nu pot nega primirea lor. Această măsură

are un caracter atît de prevenire cît şi de detecţie. Un exemplu de acest tip de măsuri, aplicate în particular punctelor de transmisie sau recepţie, îl constituie certificatul digital care conţine cheia privată a deţinătorului şi care este cunoscută numai de acesta;

– *comunicaţii protejate.* Permit realizarea securităţii comunicaţiilor, prin asigurarea integrităţii şi confidenţialităţii informaţiilor în timpul transmiterii lor. Pentru asigurarea securităţii comunicaţiilor se pot folosi, de exemplu, metode de criptare a datelor.

• **Măsuri tehnice de detecţie.** Măsurile tehnice de detecţie avertizează asupra încălcărilor sau încercărilor de încălcare a politicii de securitate şi includ măsuri cum ar fi înregistrările de audit, metode de detectare a intruziunilor şi sume de control. Din categoria măsurilor tehnice de detecţie fac parte:

– *auditul.* Aceste măsuri permit înregistrarea evenimentelor importante din punct de vedere al securităţii, al disfuncţionalităţilor în funcţionarea sistemului, precum şi monitorizarea acestora;

– *detecţia intruziunilor şi oprirea lor.* Aceste măsuri de securitate au drept scop atît detectarea breşelor de securitate, de exemplu intruziunile în reţea, activităţi suspecte, cît şi apariţia într-un timp util a unei reacţii (blocarea). Un exemplu de acest tip de măsuri îl constituie software-ul pentru detectarea şi eliminarea viruşilor care, instalat pe servere sau pe staţiile de lucru ale utilizatorilor, detectează, identifică şi înlătură viruşii informatici pentru a asigura integritatea datelor şi a sistemului. Un alt exemplu îl constituie software-ul de tipul „Sistem de Detectare a Intruziunii" (S.D.I.);

– *verificarea integrităţii.* Aceste măsuri permit detectarea încălcărilor sau încercărilor de încălcare a politicii de securitate şi ajută la stabilirea tipului de acţiune corectivă necesară. Ele asigură identificarea punctelor slabe şi a ameninţărilor potenţiale la adresa S.I.I.C, prin analiza integrităţii informaţiilor şi a disfuncţionalităţilor sistemului.

4.2. Măsuri tehnice de restabilire

După producerea unei breşe de securitate, măsurile de restabilire a activităţii S.I.I.C. permit aducerea sistemului la o stare cunoscută ca fiind sigură, prin refacerea resurselor, a serviciilor şi a informaţiilor pierdute. Un exemplu de acest tip de măsuri îl constituie utilizarea capabilităţii de recuperare a datelor, oferită de sistemul de operare de bază.

4.3. Măsuri non-tehnice de securitate

Măsurile non-tehnice de securitate pot fi de natură operaţională sau pot viza managementul securităţii, cum ar fi regulile de securitate, procedurile privind exploatarea operaţională şi procedurile referitoare la securitatea personalului, securitatea fizică şi securitatea mediului de operare.

Măsuri operaţionale de securitate. Politica de securitate a unui S.I.I.C. trebuie să impună un set de măsuri de securitate prin care să se asigure că procedurile operaţionale de securitate care reglementează folosirea bunurilor şi a resurselor sistemului sunt utilizate şi implementate corespunzător, în concordanţă cu scopurile şi funcţionalitatea sa. Managementul securităţii joacă un rol vital în supravegherea implementării politicii şi în stabilirea măsurilor operaţionale corespunzătoare.

Măsurile operaţionale, implementate în concordanţă cu cerinţele de bază de securitate, sunt folosite pentru corectarea deficienţelor operaţionale care pot fi exploatate de surse potenţiale de ameninţare. În această categorie se regăsesc măsurile prezentate în continuare.

Măsuri operaţionale de prevenire. Măsurile operaţionale de prevenire sunt constituite din:

– Controlul accesului la mediile de stocare şi controlul distrugerii acestora, de exemplu controlul fizic al accesului, metode de ştergere a informaţiilor stocate etc.;

– limitarea distribuirii externe a datelor prin folosirea etichetelor de control;

– prevenirea virusării;

– protecția facilităților sistemului prin proceduri pentru vizitatori / utilizatori, sistem cu cartele electronice, controlul biometric al accesului, managementul şi distribuția cheilor încuietorilor, bariere şi garduri etc.;

– încăperi sigure care să adăpostească swich-urile şi cablurile;

– stabilirea politicii pentru realizarea copiilor de siguranță (back-up), de exemplu proceduri privind frecvența realizării copiilor de siguranță pentru date şi sistem, registre de evidență care păstrează toate schimbările bazei de date pentru a fi folosite în diferite scenarii de reluare a activității etc.;

– stabilirea procedurilor privind securitatea facilităților de stocare din afara locației S.I.I.C.;

– protecția dispozitivelor de calcul portabile, a calculatoarelor personale şi a stațiilor de lucru;

– protecția bunurilor sistemului împotriva incendiului, de exemplu cerințe şi proceduri pentru utilizarea stingătoarelor, a sistemelor de stingere a incendiului etc.;

– asigurarea unei surse suplimentare de energie pentru cazuri de urgență, de exemplu cerințe pentru sursele neîntreruptibile de curent, generatoare locale etc.;

– controlul umidității şi temperaturii pentru facilitățile SIC, de exemplu funcționarea aerului condiționat, a sistemului de încălzire, de ventilație etc.

Măsuri operaționale de detecție. Măsurile operaționale de detecție includ următoarele:

– asigurarea securității fizice prin utilizarea senzorilor de detecție a mişcării, monitorizarea prin circuit închis de televiziune, senzori şi alarme etc.;

– asigurarea securității mediului operațional, prin utilizarea detectoarelor de fum şi foc, senzori şi alarme etc.

Măsuri non-tehnice privind managementul securității. Această categorie de măsuri de securitate se axează pe politica de protecție a informațiilor, pe ghiduri şi standarde aplicate practic, prin intermediul procedurilor operaționale, şi pot fi clasificate ca fiind de prevenire, de detecție şi de restabilire. În această categorie intră:

Măsuri non-tehnice de prevenire. Aceste măsuri includ următoarele:

– atribuirea responsabilităților privind securitatea;

– elaborarea şi actualizarea planurilor de prevenire a scurgerilor de informații;

– implementarea măsurilor privind securitatea personalului, incluzînd separarea sarcinilor, privilegii minime şi evidența accesului utilizatorilor la calculator;

– realizarea conştientizării personalului privind securitatea şi pregătirea tehnică pentru asigurarea că utilizatorii S.I.I.C sunt conştienți de regulile privind protecția informațiilor şi a sistemului, precum şi de responsabilitățile lor.

Măsuri non-tehnice de detecție. Măsurile de detecție privind managementul securității constau în:

– implementarea măsurilor privind securitatea personalului, incluzînd verificarea de securitate a personalului, investigații în legătură cu activitatea anterioară, rotația sarcinilor;

– realizarea unor analize periodice a măsurilor de securitate pentru a se asigura de eficiența lor;

– analizarea periodică a înregistrărilor de audit;

– derularea continuă a managementului riscului pentru analizarea şi reducerea riscului.

Măsuri non-tehnice de restabilire. Aceste măsuri permit asigurarea operativității neîntrerupte a S.I.I.C. în timpul situațiilor de urgență şi a evenimentelor neprevăzute şi includ:

– elaborarea planului de măsuri pentru situații de urgență şi pentru continuarea activității;

– constituirea capacităților de răspuns în cazul producerii unui incident pentru recunoaşterea, raportarea şi răspunsul în cazul producerii acelui incident şi refacerea operativității sistemului.

Bibliografie

[1] **Restinian A,** *Patologia informațională*, Editura Academiei Române, Bucureşti, 1997

[2] **Pescaru Gh.** *Considerații privind politica Serviciului de Telecomunicații Speciale în domeniul securității informațiilor* – INFOSEC, S.T.S., Bucureşti, 2006

[3] **Pescaru Gh.** *Studiu privind influența fiabilității echipamentelor, a sistemelor şi a rețelelor de comunicații şi informatică în compunerea securității unei infrastructuri pentru servicii vocale, video şi multimedia*, INSCC, Bucureşti, iunie 2009

[4] **Pescaru Gh.** Studiu de prezentare a aplicațiilor telematice avînd ca suport tehnologii RFID, INSCC, Bucureşti, decembrie 2008

[5] **Ceauşu V.** *De la incertitudine la decizie*, Editura Militară, Bucureşti, 1972

[6] **Mărăcine V.** Decizii manageriale, Editura Economică, Bucureşti, 1998

[7] http://www.ssi.gouv.fr/Secretariat General de la Defence Nationale – Direction Centrale de la Securite des Systemes d'Information, Section 1: Introduction, feb] 2004

[8] **Oprea D.** *Protecția şi securitatea informațiilor,* Editura Polirom, 2007