Clasificarea Informațiilor

Noțiuni introductive, clasificare, declasificare, principii, organizație

Conf. Univ. Dr. Marius Iulian Mihăilescu

m.mihailescu.mi@spiruharet.ro

Facultatea de Inginerie și Informatică
Universitatea Spiru Haret

02.03.2022

Overview

Overview (cont.)

- Protejarea mediilor de stocare a informațiilor
  - Identificarea și marcarea materialelor cu regim special
  - Distrugerea mediilor de stocare a informațiilor
- Clasificarea informațiilor organizațiilor
  - Criterii de clasificare a informațiilor la nivelul organizațiilor
  - Proceduri pentru clasificarea informațiilor
  - Roluri și responsabilități in procesul de clasificare a informațiilor

Clasificarea modernă a informațiilor

- Clasificare = etichetare.
- Se realizează de la cel mai de jos nivel până la cele de nivel inalt.
- Nivelul de jos = informații deschise sau neclasificate
- Nivelul inalt = confidențiale, secrete și strict secrete
- Clasificarea a luat naștere pe baza ideii că informațiile compromise pot conduce la pierderea vieților umane (strict secrete).
- Acces
  - Personalul are drepturi diverse pentru a lucra cu diverse tipuri de informații și categoriile acestora.
  - Un angajat poate să acceseze informațiile respective doar daca are dreptul de a accesa informațiile din categoria respectivă sau din una superioară.

Clasificarea modernă a informațiilor (cont.)

- **Regulă**. Informațiile pot circula in sus - confidențial → secret → top secret. In sens invers (sus ← jos) - dacă persoana autorizată are decizie pentru declasificarea acestora.
- Securitatea națională se bazează pe două strategii fundamentale:
  - ce nu este interzis este permis
  - ce nu este permis este interzis
- Pentru implementarea strategiei de bază se utilizează două tactici fundamentale pentru protejarea informației sensibile:
  - controlul discret al modalităților de acces
  - modalitățile legale ale controlului accesului

Clasificarea modernă a informațiilor (cont.)

- Controlul discret al modalităților de acces
  - Se axează pe cel mai mic privilegiu - implementarea accesului se face cu respect pentru cel mai mic privilegiu - *nici o persoană (indiferent de poziția pe care o are) nu deține drepturi nelimitate pentru a vizualiza informațiile sensibile, iar persoana cu astfel de drepturi trebuie să aibe acces doar la cele care se află in zona lor de activitate*.
  - Implementarea controlului discret se realizează prin utilizarea unei matrici control (vezi Tabelul 1).
  - Fiecare angajat/persoană dintr-o anumită listă și pentru fiecare tip de informație, matricea definește in mod foarte clar ce are dreptul ca fiecare angajat/persoană să facă cu operațiile definite.
  - Operație = execuție, citire, citire/scriere, aprobare.

Clasificarea modernă a informațiilor (cont.)

Table 1: Matrice pentru controlul accesului

Persoană/Angajat	**Operație 1**	**Operație 2**	**Operație 3**
Popescu X	Citire	Citire/Scriere	Aprobare
Ionescu Y	Execuție	Citire	Aprobare
Calinescu Z	Citire/Scriere	Aprobare	Execuție
Stefanescu W	Execuție	Citire/Scriere	Aprobare
Naftanaila K	Citire	Aprobare	Execuție

Clasificarea modernă a informațiilor (cont.)

- Controlul legal al accesului se bazează pe legile existente.
- Legea securității naționale [1]
- Se stabilesc două tipuri de structuri de control:
  - structuri ierarhizate - se referă la catalogarea informațiilor sensibile in patru categorii: *strict secrete*, *secrete*, *confidențiale*, și *neclasificate*.
  - structuri neierarhizate
    - Categoria *Compartimentate* - caracterizate prin nume scurte, sugestive prin evidențierea anumitor aspecte.
    - Categoria *Obiecții* - atenție sporită la naționalitatea celor care vizualizează și au drepturi de operații.

[1] Legea securității naționale Nr. 51/29.07.1991 - http://legislatie.just.ro/Public/DetaliiDocument/1517

Clasificarea informațiilor

- Conceptualizarea informațiilor
  - Din prisma guvernelor
  - Clasificare mai largă: *informații subiective* și *informații obiective*

Clasificarea informațiilor *subiective*

- Ideea de bază a guvernelor - clasificarea cât mai largă a informațiilor:
  - informații *subiective*
  - informații *obiective*

Clasificarea informațiilor *subiective*

- sunt caracterizate ca *secrete reale* sau *operaționale*.
- unice pentru guvern - decide modul in care principalele activități vor fi derulate
- **Regulă**. Cu ajutorul controlului guvernului și protejarea informațiilor de către acesta, pe baza cărora sunt emise și decizii, informațiile in cauză nu pot fi dezvăluite in mod independent de către un adversar.

Clasificarea informațiilor *subiective* (cont.)

- **Caracteristici:**
  - *perceptibilitatea generală* - pregătirea specială nu este necesară cu scopul înțelegerii secretului, ușor de furat și distribuit altora.
  - *schimbarea conținutului* - există șanse foarte mari ca conținutul să fie modificat pe ultima sută de metrii.
  - *perisabilitatea* - după scurt timp, aceste informații devin perisabile, au o viață scurtă, fiind păstrat pentru o perioadă limitată de timp.
  - *dimensiune mică* - exprimarea secretului se va face prin câteva cuvinte, ușor de furat și distribuit altora.
  - *supunerea unui arbitru* - cu scopul de a intra in posesia lor, un adversar le poate fura iar secretul nu poate fi descoperit in mod independent.

Clasificarea informațiilor *obiective*

- definite ca fiind informațiile care dacă sunt descoperite, dezvoltate sau controlate prin mijloace diverse de către guvern, sunt deja cunoscute sau descoperite independent de către o altă entitate/țară.
- Categoria cuprinde *informații științifice* sau *secrete științifice*.
- informațiile obiective nu au control absolut
- sunt caracterizate prin natura lucrurilor/obiectului/a ceea ce cuprinde și nu de secret propriu-zis.

Clasificarea informațiilor *obiective* (cont.)

- **Caracteristici:**
  - *confuzie* - informațiile științifice cuprind și sunt caracterizate prin rapoarte foarte lungi și laborioase, din această cauză ele nu sunt transmisibile ușor.
  - *înțelegere/interpretare* - doar de către oamenii de știință.
  - *supunerea arbitrajului* - alte persoane sunt capabile să afle/determine răspunsul la anumite intrebări științifice, condiția constând in formularea corectă a intrebării respective.
  - *nu există schimbări* - caracter permanent, fiind reprezentate de către o singură valoare.
  - *viață lungă ca și secret* - informațiile respective pot fi descoperite și de către alții intrun mod independent, dar cu cost mare ca și timp, ducând in acest fel la păstrarea secretului pentru mult timp

Informații de natură tehnică - secrete obiective

- nu există o incadrare perfectă in categoria informațiilor subiective sau obiective
- cuprinde proiecte și execuții tehnice (ex.: arme, rachete, explozibil)
- caracteristicile informațiilor tehnice = caracteristicile informațiilor științifice.
- sunt caracterizate prin natura lucrurilor/obiectului/a ceea ce cuprinde și nu de secret propriu-zis.

Secrete comerciale

- includ informații legate de procesele de fabricație, rețelele unui produs, alte informații de natură obiectivă ce pot fi descoperite de către alții in mod independent
- asemnătoare cu informațiile științifice și tehnice

Necesitatea clasificării informațiilor

- Procesul de clasificare al informațiilor se realizează in trei etape:
  - identificarea și stabilirea corespunzătoare motivului și nevoii de clasificare
  - identificarea și determinarea nivelului de clasificare
  - identificarea și determinarea duratei clasificării

Identificarea motivului de de clasificare

- Se realizează pe baza a cinci pași:
  - definirea cu precizie a informațiilor ce urmează a fi clasificiate.
  - stabilirea domeniilor clasificării pentru incadrarea informațiilor
  - identificarea statusului - dacă se află sau nu sub control guvernamental
  - identificarea nivelului de sensibilitate, dacă prin dezvăluirea informațiilor se poate produce daune pentru securitatea națională
  - identificarea clară și concisă pentru nevoia de clasificare a informațiilor respective.

Identificarea nivelului de de clasificare

- Se atribuie un nivel de clasificare - prin acest nivel se evidențiază importanța relativă a informației clasificate
- Legea Nr. 182/2002 privind protecția informațiilor clasificate, informațiile clasificate ca fiind secrete de stat, sunt catalogate și incadrate folosind trei niveluri:
  - **strict secrete de importanță ridicată** - divulgarea fără permisiune produce daune de o gravitate sensibilă securității naționale.
  - **strict secrete** - divulgarea fără permisiune permite producerea de daune grave securității naționale.
  - **secrete** - divulgarea fără permisiune permite producere de daune medii securității naționale

Identificarea duratei clasificării

- Determinarea duratei se realizează folosind una dintre tehnicile de mai jos:
  - perioada de timp măsurată de la data emiterii documentului
  - determinarea evenimentului viitor care apare inaintea procedurii de declasificare
  - in cazul in care data sau evenimentul nu este specificat, documentul care conține informații clasificate urmează să fie marcat, cu scopul identificării instituției originale, care in același timp, va avea rolul și de declasificare al acesteia.

Declasificarea informațiilor clasificate

- presupune reducerea nivelului de clasificare
- informațiile sensibile (strict secrete) primesc nivelul *secret* sau *confidențial*
- informațiile secrete sunt degradate in informații confidențiale
- informațiile confidențiale pot fi declasificate sau mutate pe un nivel superior.
- degradarea și/sau modificarea nivelului de declasificare se realizează de către personalul autorizat și care a realizat clasificarea inițială a informațiilor, de către succesorii acestora, șefii lor sau alți oficiali.

Principiile protejării informațiilor speciale/sensibile

- Sunt 10 principii folosite in protejarea informațiilor speciale/sensibile:

  - *principiul delimitării și identificării autorizării* - repartizarea informațiilor pe structură ierarhică, include compartimentările (catalogarea) pentru regăsirea informației, persoana autorizată este responsabilă cu stabilirea sferei de exercitare și autorizarea folosind criteriul ierarhic al persoanei plus suma tuturor autorizărilor persoanelor aflate in subordinea sa.
  - *principiul securității simple* - informațiia unei categorii care se află in afara autorizării ei, nu trebuie văzută de nici o persoană
  - *principiul stelei* - nici o persoană nu va face modificări pe operațiile dintr-o categorie inferioară la care persoana are acces
  - *Principiile integrității*:
    - *primul principiu* - nici un software nu va accepta informații de la un program inferior lui, respectând linia privilegiilor
    - *al doilea principiu* - nici un software nu va avea posibilitatea să scrie intr-un program superior lui, respectând privilegiile

Principiile protejării informațiilor speciale/sensibile (cont.)

- *principiu etichetării* - etichetarea fiecărui purtător de informații se va face foarte clar, conținând categoria informațiilor ce sunt conținute, in format accesibil unui om, și in format citibil de către echipamentele periferice.
- *principiul clarificării* - schimbarea categoriilor existente este strict interzisă de orice persoană sau procedură
- *principiul inaccesibilității* - informația nu va fi lăsată la dispoziția altor persoane sau procese, se vor respecta normele interne.
- *principiul verificabilității* - se vor realiza inregistrări imposibil de șters, modificat sau orice altă formă de alterare pentru toate activitățile semnificative ce ține de securitate.
- *principiul increderii in software* - atâta timp cât un calculator nu are puterea și posibilitatea să controleze respectarea principiilor anterioare, dar efectuează activități utile, increderea in aplicațiile software va permite identificarea și apariția unor excepții de la regulă, atunci când este cazul.

Principiile protejării informațiilor speciale/sensibile (cont.)

- Asigurarea protecției informațiilor speciale de către sistemele de prelucrare automată a datelor, se poate realiza prin patru moduri de funcționare:
  - *modul dedicat* - informațiile prelucrate de sistem sunt din aceeași categorie, persoanele sistemului au autorizație de acces la categoria respectivă.
  - *modul sistem superior* - informațiile prelucrare de sistem pot să aparțină unor categorii diferite, persoanele implicate in această operație au autorizații care le oferă acces la nivelul cel mai ridicat pentru informațiile prelucrate.
  - *modul controlat* - sistemul poate să controleze informațiile aflate in categorii diferite, persoanele să dețină autorizații diferite, sistemul se va baza pe restricții fizice - aspect ce include respectarea tuturor principiilor securității informațiilor (operațiune foarte dificilă și sensibilă).

Principiile protejării informațiilor speciale/sensibile (cont.)

- *modul securității stratificate* - sistemele prelucrează informații care aparțin diferitelor categorii, personalul are autorizații diferite. Se folosește conceptul de credibilitate al componentelor informatice (hardware, software și firmware) - astfel, prin acest concept, problema *turnului Babel* specifică securității sistemului, asigură realizarea intregului set de princii menționate anterior.

Protejarea mediilor de stocare a informațiilor

- mediile de stocare care conțin informații provenit in urma unor proceduri de prelucrare automată a datelor, trebuie să fie catalogate ca documente ale prelucrării automate a datelor.
- Mediile pot fi: CD-uri, DVD-uri, benzi magnetice, flash disk-uri, circuite electronice, HDD-uri, SSD-uri etc.
- același regim de utilizare ca și la formele tradiționale de prelucrare a datelor/documentelor.
- ștergerea informațiilor clasificate este o operație foarte dificilă și sensibilă.
- autorizarea operațiunilor de prelucrare automată a datelor este făcută de o persoană autorizată care trebuie să verifice existența fișiei de securitate.

Protejarea mediilor de stocare a informațiilor (cont.)

- fișa de securitate conține *categoria persoanei* care execută operația, *categoria informațiilor* prelucrate și instrucțiunile referitoare la statutul informațiilor ce au să rezulte, *durata prelucrării*, *timpul de utilizare a componentelor bazei de date*, *generațiile reținute* (fiu, tată, bunic etc.) - cu scopul restaurării bazei de date in caz de dezastre.

Identificarea și marcarea materialelor cu regim special

- materialele cu regim special trebuie să fie insotite de număr și inregistrate corespunzator cu scopul identificării a ce s-a folosit și ce s-a văzut din ele.
- **marcarea și identificarea in cod mașină** trebuie să se efectueze prin coduri ușor interpretabile aflate pe echipamente, a.i. să se identifice rapid categoria din care parte informațiile prelucrate și care sunt operațiunile la care sunt supuse. poate fi ultimul caracter al numelui fișierului, iar caracterul utilizat să aibă valorile:
  - S - special
  - C - confidențial
  - P - privat
  - R - restricții
  - N - neclasificate

Identificarea și marcarea materialelor cu regim special (cont.)

- **marcarea fizică** - toate suporturile supuse prelucrării automate a datelor.
- **marcarea suporturilor de hârtie** - marcaje prin culori diferite: orange - control special; roz - confidențial; verde - privat; galben - restricții, alb - comun
- **marcarea cutiilor și a carcaselor** - suporturile de memorare sunt păstrate in condiții care impune etichetarea clară a acestora, precum și redactarea fișierelor conținute de suporturile din interior.
- **marcarea benzilor magnetice** - cu etichete lipite chiar pe bandă, fără afectarea prelucrării datelor.
- **marcarea pachetelor cu discuri, HDD-uri, SSD-uri etc.** - cu marker special.
- **marcarea microfilmelor** - pe prima imagine cadru sau pe cutie, cu markerul

Distrugerea mediilor de stocare a informațiilor

- păstrarea se face in camere speciale
- documentele al căror conținut este sub control special se păstrează in seifuri și in locații speciale protejate prin sisteme speciale
- operațiunea de distrugere să urmeze o procedură specială, precum arderea
- arderea se folosește pentru gunoaie informatice adunate in pungi speciale și dedicate.
- la ardere participă cel puțin două persoane, care vor consemna intrun registru special materialele ce se distrug.
- cenușa se imprăștie in așa fel incât să se elimine oricare posibilitate de reconstituire a datelor distruse.
- transformarea in pastă este posibilă doar pentru reziduurile din hârtie.

Clasificarea informațiilor organizațiilor

- la nivel de organizație, informațiile se clasifică folosind mai multe categorii, folosind același principii ca și la informațiile naționale:
- **informații care au nevoie de un control special** - informații cunoscute ca fiind *strict secrete*, la nivel de organizație ele se intâlnesc sub numele de *speciale*, fiind marcate cu **S**
- **informatii confidentiale la nivel de unitate** - notate cu **C**, corespund informațiilor secrete la nivel național.
- **informații private** - notate cu **P**, cuprind informațiile și materialele a căror compromitere duce la prejudicierea statutului unei persoane din unitate sau corporație.
- **informații de uz intern** - notate cu **R** și care nu fac parte din categoriile anterior menționat, dar prezintă un set de restricții in utilizarea lor
- **informații publice** - sau informații neclasificate, fiind notate cu **N**.

Clasificarea informațiilor organizațiilor (cont.)

- la nivel guvernamental, orice fel de informație care nu este incadrată intr-una din categoriile speciale, sub incidența legii accesului liber la informațiile publice, poate fi publicată de orice organ de presă scrisă, video sau audio, cu explicația și motivația că *tot ceea ce nu este interzis este permis*.
- la nivel de organizație, lucrurile stau invers, doar informațiile care sunt specificate *pentru public* pot fi făcute publice, respectând *tot ceea ce nu este permis este interzis*.

Criterii de clasificare a informațiilor la nivelul organizațiilor

- valoarea
- vârsta
- uzura morală
- asocierea cu persoanele

Proceduri pentru clasificarea informațiilor

- identificarea administratorului/custodelui;
- specificarea criteriilor după care vor fi clasificate și etichetate informațiile;
- clasificarea datelor după proprietar, care devine subiect supus auditării efectuate de un superior;
- precizarea și documentarea oricăror excepții de la politicile de securitate;
- precizarea controalelor aplicate fiecărui nivel de clasificare;
- specificarea procedurilor de declasificare a informațiilor sau pentru transferarea custodiei unei alte entități;
- crearea unui program de conștientizare la nivel de organizație despre controalele pe linia clasificării informațiilor.

Roluri și responsabilități in procesul de clasificare a informatiilor

- Singurele roluri in procesul de clasificare le are:
  - proprietarul
  - utilizatorul
  - custodele datelor clasificate

Roluri și responsabilități in procesul de clasificare a informatiilor (cont.)

- poate fi administratorul sau directorul unei organizații.
- Responsabilitățile:
  - intreprinde demersuri pentru stabilirea nivelului de clasificare a informațiilor, care inseamnă, de fapt, cerințele organizației de protejare a acestora;
  - efectuează verificări periodice ale clasificărilor existente, in vederea adaptării la cerințele organizației;
  - delegă responsabilitatea protejării datelor către un custode specializat și autorizat.

Roluri și responsabilități in procesul de clasificare a informatiilor (cont.)

- **Custodele informațiilor** este cel care pestează un serviciu externalizat organizației.
- Obligațiile acestuia sunt:
  - efectuează copii de siguranță periodice și teste de rutină a validității datelor;
  - efectuează restaurări de dare din copiile de siguranță, când este cazul;
  - intreține datele inregistrate, in concordanță cu politicile de clasificare a informațiilor.

Roluri și responsabilități in procesul de clasificare a informatiilor (cont.)

- **Utilizatorul** este considerat orice persoană, operator, angajat, persoană din afară, care folosește informațiile.
- Obligațiile acestuia sunt:
  - de a urma intocmai procedurile de funcționare, definite prin politicile de securitate ale organizației, și să respecte normele publicate privind utilizarea informațiilor;
  - să acorde toată atenția menținerii informațiilor in timpul activității prestate, după cum se stipulează in politicile de utilizare a informațiilor emise de organizația proprietară. Ei trebuie să asigure protejarea impotriva accesului neautorizat la informațiile clasificate;
  - să folosească resursele informaționale ale firmei numai in scopul urmărit de aceasta, nu și in scop personal.

Bibliografie

Recomandări bibliografice pentru aprofundare:

- Popa Sorin Eugen - *Securitatea Sistemelor Informatice*, Capitolul 2 - paginile 16-24, http://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf.
- Suportul pentru CISSP și CISM.