Tema nr.3 Protecția informațiilor prin clasificarea lor

1. Clasificarea informațiilor
2. Copii de rezervă (backup-uri)
3. Sisteme de jurnalizare

Lector univ. R.Bulai

1. Clasificarea informațiilor

- NATO are meritul principal în dezvoltarea sistemului de clasificare a informațiilor.
- Clasificarea este operația de etichetare crescătoare a documentelor sau informațiilor, de la cel mai de jos nivel, unde se situează informațiile **publice** sau **neclasificate,** la cele **confidențiale**, urcînd spre informații **secrete** și **strict secrete** (structura ierarhizată).
- Informațiile **confidențiale**, **secrete** și **strict secrete** sunt denumite ***informații clasificate (sensibile)***.

1. Clasificarea informațiilor

- Există o strînsă legătură între responsabilitățile angajaților și categoriile de informații cu care se dă dreptul de a lucra.
- Un angajat poate citi documentele dintr-o anumită categorie, numai dacă el are cel puțin împuternicirea de accesare a informațiilor din categoria respectivă sau dintr-una superioară.

1. Clasificarea informațiilor

- Organizațiile își protejează informațiile care le oferă avantaje în fața concurenților – secrete comerciale;
- Guvernele își protejează informațiile de apărare națională și de relații internaționale - secrete de stat;
- În ambele ipostaze, informația protejată este atât de importantă, încât ajungerea ei în posesia adversarilor (dușman/concurent) poate să aibă efecte negative asupra intereselor majore (securitatea națională/profitul).
- Informațiile declasificate sau făcute publice pe cale oficială nu mai pot fi reclasificate.

Informații subiective

- Guvernele pornesc de la o altă clasificare: informații *subiective* (operaționale) și *obiective* (științifice, tehnice).
- *Inf.subiective* au următoarele caracteristici: dimensiune redusă, perceptibilitate universală (nu este necesară o pregătire specială pentru al înțelege), conținutul poate fi schimbat, au o viață scurtă.
- Adversarul nu are cum să producă o astfel de informație, dar o poate obține prin spionaj sau dezvăluire neautorizată.

Informații obiective

Inf. științifice sau secrete științifice – care deși sunt descoperite și controlate de un guvern, pot fi deja cunoscute sau pot fi descoperite independent de o altă țară. Caracteristici:

- Sunt confuze, nu se pot transmite cu ușurință;
- Pot fi înțelese numai de oameni de știință;
- Nu sunt supuse schimbării, au caracter etern, valoare unică;
- Pot avea o viață lungă ca secret.

Inf.tehnice - proiecte, metode, un proces, o tehnică, nu sunt fenomene naturale și sunt utilizate in exploatarea inf.științifice.

Etapele clasificării informațiilor

- 1. Stabilirea nevoii de clasificare;
- 2. Determinarea nivelurilor clasificării;
- 3. Determinarea duratei clasificării.

1. Stabilirea nevoii de clasificare;

- Definirea cu exactitate a informațiilor de clasificat;
- Stabilirea dacă informațiile se încadrează într-unul dintre domeniile supuse clasificării;
- Verificarea dacă informațiile se află sub control guvernamental;
- Concluzionarea dacă dezvăluirea inf. poate să conducă la cauzarea daunelor pentru securitatea națională;
- Specificarea precisă a nevoii de clasificare a informațiilor

2. Determinarea nivelurilor clasificării

Un sistem de clasificare eficient trebuie să se bazeze pe niveluri de clasificare definite cu mare claritate. De ex.

- SUA – strict secret, secret și confidențiale;
- România – strict secrete de o importanță deosebită, informațiile strict secrete și inf.secrete;
- R.Moldova???

LEGE Nr. 245
din 27.11.2008**cu privire la secretul de stat**

- Sînt stabilite 4 grade de secretizare a informaţiilor atribuite la secret de stat şi 4 parafe de secretizare corespunzătoare pentru purtătorii materiali de asemenea informaţii:
  a) „Strict secret” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate aduce prejudicii deosebit de grave intereselor şi/sau securităţii Republicii Moldova;
  b) „Secret” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate dăuna grav intereselor şi/sau securităţii Republicii Moldova;
  c) „Confidenţial” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate dăuna intereselor şi/sau securităţii Republicii Moldova;
  d) „Restricţionat” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate fi în dezavantajul intereselor şi/sau securităţii Republicii Moldova sau poate să conducă la divulgarea unei informaţii secretizate cu parafa „Strict secret”, „Secret” sau „Confidenţial”.

- Pentru informaţiile avînd gradul de secretizare „Strict secret” se stabileşte un termen de secretizare de pînă la 25 de ani, pentru informaţiile cu gradul „Secret” – un termen de pînă la 15 ani, pentru informaţiile cu gradul „Confidenţial” – de pînă la 10 ani şi pentru informaţiile cu gradul „Restricţionat” – de pînă la 5 ani.
  (2) Pentru informaţiile despre persoanele care colaborează sau au colaborat confidenţial cu organe ce desfăşoară activităţi de informaţii, de contrainformaţii şi operative de investigaţii se stabileşte un termen de secretizare nelimitat.

3. Determinarea duratei clasificării

Se determină prin una dintre urm. metode:

- Ca o perioadă de timp măsurată de la data emiterii documentului;
- În funcție de un eveniment viitor ce poate să apară înaintea operațiunii de declasificare;
- Documentul va fi marcat, pentru a se indica instituția aflată la originea lui, ce va avea sarcina declasificării.

Clasificarea informațiilor organizațiilor

- *Inform. care necesită un control special (speciale)* sunt notate cu **S** și includ inf. și materialele care ar aduce pierderi de 10% din profitul brut anual – echivalente cu inf. *strict secrete* la nivel național;
- *Inf. confidențiale la nivel de unitate* notate cu **C** și includ inf. și materialele care ar aduce pierderi de 1% din profitul brut anual – echivalente cu inf. *secrete* la nivel național;
- *Informațiile private* notate cu **P** care ar prejudicia statutul unei persoane din organizație – *confidențiale;*
- *Inf. de uz intern* sunt notate cu **R** și reprezintă inf. cu restricții în utilizare;
- *Inf. publice* notate cu **N** sau *pentru public* – inf. neclasificate;
- *Inf. numai pentru domnul/doamna…Numai pentru compartimentul…*

Criterii de clasificare a informațiilor

- *Valoarea* dacă o inf. este valoroasă pentru org. sau concurenți, ea trebuie clasificată – cr. principal;
- *Vârsta* care conduce la stabilirea unei valori diferențiate. Cu cît vechimea e mai mare, cu atît inf. pierd din valoare, interesul pentru ele se pierde;
- *Uzura morală* cînd inf. sunt înlocuite cu altele noi sau în organizație s-au produs schimbări radicale, vechea clasificare este înlocuită cu alta;
- *Asocierea cu persoanele* influențează în funcție de importanța indivizilor care reglementează regimul datelor personale.

Procedurile de clasificare a informațiilor

- Identificarea proprietarului/custodelui (administratorul sau directorul org. care răspunde de averile informaționale încredințate / cel ce prestează un serviciu delegîndu-i-se responsabilități pe linia protejării inf., de obicei specialiști în TI);
- Specificarea criteriilor după care vor fi clasificate și etichetate informațiile (de ob.proprietarul);

Procedurile de clasificare a informațiilor

- 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 sau transferarea custodiei unei altei entități;
- Crearea unui program de conștientizare la nivel de org. dspre controalele pe linia clasificării inform.

Protecția inf.speciale în sistemele de prelucrare automată

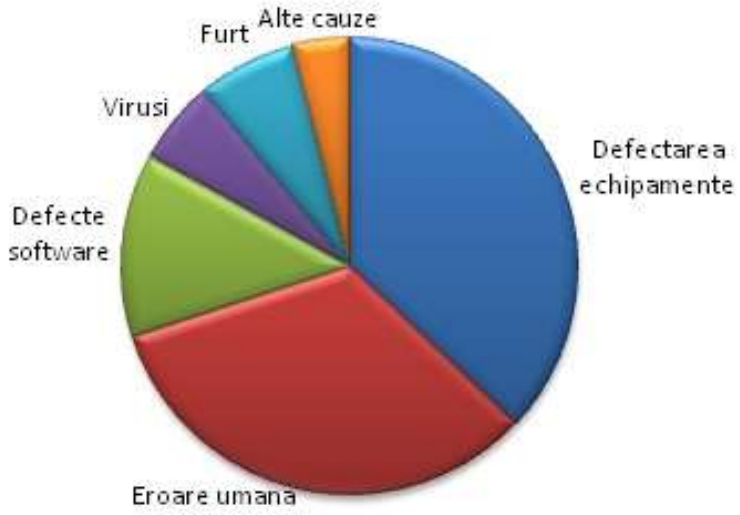
- *Modul dedicat* – toate inf. prelucrate de sistem fac parte din aceeași categorie, iar persoanele sistemului posedă autorizație de acces la categoria respectivă;
- *Modul sistem superior* – inf. pot să aparțină unor categorii diferite, iar persoanele sistemului posedă autorizări de acces la nivelul cel mai înalt;
- *Modul controlat* – inf. din categorii diferite și persoanele au autorizații diferite, dar sistemul se va baza pe restricții fizice prin care să se respecte toate principiile SI;
- *Modul securității stratificate* - inf. din categorii diferite și persoanele au autorizații diferite, dar conceptul credibilității componentelor informatice (hardware, software și firmware – soft din ROM) rezolvă problema.

2. Copii de siguranță (backup-uri)

- **Copiile de siguranţă (*backup*)** sunt necesare pentru a permite **recuperarea datelor şi aplicaţiilor** în cazul unor evenimente cum ar fi: dezastre naturale, defecţiuni ale discurilor de sistem, spionaj, erori de introducere a datelor, erori de funcţionare a sistemului etc.
- Crearea unei copii de rezervă poate fi realizată cu unul din programele: Cobian Backup, Acronis True Image, Norton Ghost, Paragon Backup&Recovery, **FBackup** etc.

2. Copii de siguranță (backup-uri)

- Studii de specialitate facute de diverse organizatii privind cauzele primare ale pierderii datelor indica ca surse primare defectarea echipamentelor si eroarea umana.



Defectarea echipamentelor

Primul motiv care cauzează pierderea datelor, prin:

- defectarea fizica a discurilor,
- scurt circuite,
- probleme cu sursa de alimentare a calculatorului,
- defecte cauzate de uzura echipamentelor.

- Spre exemplu rata de inlocuire in garantie raportate de marii producatori de hard discuri este de 0.6-0.9% dar studii paralele indica cifre precum 2-4%.
- Garantia însă inseamna schimbarea sau repararea discului fara costuri suplimentare, **insa nici un producator nu isi va asuma recuperare datelor**.

Eroarea umana

Este a doua cea mai des intalnita cauza, dar careia i se da cea mai mica importanta sau este cel mai des trecuta cu vederea. Ex.:

- stergeri accidentale a fisierelor,
- formatari accidentale,
- erori facute de administratorii sistemelor (totusi eroarea vrem sau nu vrem este umana),
- utilizare incorecta, cauzate de scapari,
- pierderea dispozitivelor de stocare mobile.