FEAA
FACULTATEA DE ECONOMIE
ŞI ADMINISTRAREA AFACERILOR
UNIVERSITATEA "AL. I. CUZA" IAŞI

Specializarea:

**Informatică economică**

**Anul 3, ZI**

**Dumitru Oprea**



# PROTECŢIA ŞI SECURITATEA SISTEMELOR INFORMAŢIONALE

**SUPORT DE CURS**

2017

# Cuprins

# Prefaţă

Informaţia, a treia formă de manifestare a Existenţei Fundamentale, la confluenţa dintre milenii, a devenit cea mai apreciată comoară a omenirii. Cu mult temei, s-a făcut afirmaţia de către japonezi că fericiţii stăpâni ai informaţiei de la sfârşitul secolului XX vor fi şi stăpânii lumii. Nu energiile controlate de om, oricât de puternice ar fi ele sau efectele lor, nu aurul şi alte averi materiale, sub orice formă ar exista acestea, ci informaţia va fi semnul puterii. Aşadar, nu sceptrul de aur, ci aureola informaţională. Câtă dreptate au avut egiptenii, în urmă cu mii de ani, spunând că omul e frumos când mintea-i e regină. În acest sens, poate că merită să descifrăm şi mesajul de suflet al lui Gabriel Garcia Marquez. Iată ce ar face marele scriitor, dacă Dumnezeu i-ar mai dărui o bucăţică de viaţă: *„Aş da valoare lucrurilor mărunte, dar nu pentru ce valorează ele, ci mai curând pentru ceea ce ele semnifică …; de-abia acum înţeleg că pentru fiecare minut în care închidem ochii pierdem şaizeci de secunde de lumină. Aş merge în timp ce alţii ar sta pe loc, aş rămâne treaz în timp ce toţi ceilalţi ar dormi. Aş asculta în timp ce alţii ar vorbi …”*. Doamne, cât respect pentru lumina minţii, care este informaţia. Şi cum să nu fie protejată pe măsură!?!

În sprijinul afirmaţiilor noastre vin preocupările privind protecţia şi securitatea informaţiilor, care datează de mii de ani. Cu riscul de a intra în contradicţie cu unele periodizări anterioare, putem afirma că semnalele oferite de diferite popoare de-a lungul timpului ne conduc la concluzia că fenomenul globalizării sistemelor de protecţie şi securitate a informaţiilor începe în urmă cu peste zece mii de ani. Ne referim la primul protocol de securitate a informaţiilor, realizat de mesopotamieni, devenit ulterior, la o altă scară, standard internaţional. Peruvienii, prin quippos-urile lor, au făcut acelaşi lucru, în urmă cu şase mii de ani. Egiptenii, acum cinci mii de ani, indirect, au introdus conceptul de clasificare a informaţiilor, interzicând preoţilor să scrie pe pământul reavăn, din dorinţa de a nu se face publice informaţiile cu caracter secret. De asemenea, de multe mii de ani, informaţiile sensibile au fost ascunse privirilor curioase, de cele mai multe ori rău intenţionate, prin operaţiunea de camuflare a lor, sau au fost plasate printre informaţiile obişnuite, prin steganografie, sau au fost codificate, criptate – pentru a le face accesibile doar persoanelor autorizate. Acestor tehnici li s-au adăugat multe altele, cu acelaşi scop, tăinuirea informaţiilor secrete.

Acum, la începutul mileniului trei, prea multe nu s-au schimbat pe planul operaţiunilor de protejare şi securizare a informaţiilor, ci doar tehnicile şi mediile de lucru, firesc, sunt altele. Până şi tradiţionalul sistem bazat pe un calculator central a devenit desuet, vorbindu-se în orice colţ al planetei despre Internet, Intranet, Extranet, despre includerea în structura lor a calculatoarelor personale (PDA), a diverselor generaţii de telefonie şi multe altele, inclusiv despre reţeaua reţelelor, ceea ce dă noi dimensiuni spaţiului cibernetic. Pe planul globalizării, o tendinţă este evidentă, a preocupărilor comune, public-privat, pentru securizarea spaţiului cibernetic global, îndeosebi după 11 septembrie 2001. Dependenţa de informaţie este tot mai mare, chiar periculoasă. Sunt state care depind total de informaţiile oferite de componentele spaţiului cibernetic naţional. Blocarea acestuia timp de câteva ore poate să conducă la instaurarea haosului în ţara respectivă, afectând, în bună măsură, şi securitatea sistemului informaţional global planetar.

Prin diferite niveluri de detaliere, cam toate aspectele menţionate mai sus îşi găsesc un tratament adecvat în cartea de faţă. Tocmai datorită acestui lucru, ea poate fi utilă şi accesibilă, integral sau în parte, mai multor categorii de cititori. Printre ei, cu siguranţă, se vor afla elevi şi studenţi, profesori şi cercetători, specialişti din diferite domenii, dar şi omul de rând.

Tuturor cititorilor, indiferent de grupul de apartenenţă, le mulţumim anticipat pentru exprimările de păreri sau pentru propunerile de îmbunătăţire a ediţiei de faţă.

Autorul
Iaşi, 2016

CAPITOLUL I

# Cadrul general al protecţiei şi securităţii sistemelor informaţionale

Orice material publicat sub titlul „Protecţia şi securitatea informaţiilor”, la o analiză mai atentă, este destul de derutant, întrucât în lumea afacerilor s-ar putea vorbi cu mai multă uşurinţă despre ... insecuritatea datelor decât despre securitatea lor. Mai mult, nici nu se pune problema că uneori şi prea multă informatizare este dăunătoare. Din momentul conştientizării utilizatorilor de avantajele folosirii calculatoarelor, o mulţime de organizaţii au declanşat un imens proces de retehnologizare informaţională, raportând cu satisfacţie ce investiţii masive au făcut în tehnica de calcul. Sunt şi cazuri de informatizare cauzate de „modă”, fără să fie luate în seamă riscurile acestui proces.

În acest spirit, capitolul de faţă doreşte să-şi convingă cititorii că:

- averile informaţionale sunt foarte importante în activitatea organizaţiilor mai mici şi mai mari, iar preocupările pe linia asigurării securităţii lor, deşi există din cele mai vechi timpuri, s-au intensificat o dată cu dezvoltarea tehnicii de calcul;
- există o gamă largă de pericole şi vulnerabilităţi asociate acestor averi, iar ea se extinde simultan cu dezvoltarea tot mai rapidă a tehnologiilor informaţionale şi de comunicaţii;
- securitatea averilor informaţionale este o componentă de bază a ecuaţiei succesului organizaţional şi o problemă mai degrabă umană decât tehnică, posibil de rezolvat cu mijloace ieftine.

## 1.1 Scurtă istorie modernă a (in)securităţii informaţiilor

Investind în tehnică sume colosale, firesc, oamenii au început să folosească metode adecvate de păstrare a ei în camere speciale, cu uşi încuiate prin sisteme sofisticate, bazate pe cifru, ferind, ca şi până acum, noua avere de privirile curioşilor. S-a tratat, deci, tehnica de calcul ca şi seifurile ce păstrau banii şi bijuteriile de familie, uitându-se un amănunt foarte important, şi anume că noile averi sunt nu cele materiale, ci imateriale, cu forme speciale de utilizare, şi cu valori intrinseci, invizibile de cele mai multe ori, iar căile de protejare folosite până acum devin ineficiente sau insuficiente. Mai clar, informaţia, căci ea reprezintă noua avere, devine o resursă de nebănuit a organismelor economico-sociale. Alături de capital şi oameni, informaţia este una dintre averile deosebite ale firmei.

Insecuritatea, amintită anterior, rezidă şi din faptul că orice persoană care dialoghează cu calculatorul unei firme, fie prin multitudinea tipurilor de reţele, fie prin sistemele de poştă electronică (e-mail) sau prin intermediul dischetelor, CD-urilor, DVD-urilor, USB-urilor, al benzilor magnetice sau al altor suporturi de informaţii, aduse din afara unităţii, sau prin scrierea unor programe cu rol special, poate să facă următoarele lucruri: să copieze fişierele importante ale altor firme, să influenţeze evidenţele altora pentru a le cauza pierderi, să reprogrameze calculatoarele incluse în configuraţia sistemelor de producţie pentru a provoca avarierea utilajelor sau pentru producerea accidentelor umane (inclusiv uciderea lor), să şteargă programe sau fişiere şi multe altele.

Dacă ne raportăm la dinamica fantastică din domeniu, ne dăm seama de creşterea constantă a riscului la care se expun beneficiarii noilor tehnologii informaţionale, platformele de lucru generând, la rândul lor, noi medii de utilizare. Se pot puncta câteva momente esenţiale, pe planul evoluţiei tehnologiilor folosite, cu impact asupra sistemelor de securitate, şi încercăm să efectuăm o grupare a lor pe generaţii, astfel:

- generaţia I, securitatea sistemelor bazate pe calculatoare mari, de sine stătătoare;

- generaţia a II-a, securitatea sistemelor distribuite;
- generaţia a III-a, securitatea microcalculatoarelor, inclusiv a reţelelor locale;
- generaţia a IV-a, securitatea Internetului;
- generaţia a V-a, securitatea comerţului şi afacerilor electronice;
- generaţia a VI-a, securitatea comerţului şi afacerilor mobile;
- generaţia a VII-a, securitatea globală a lumii virtuale, a întregului spaţiu cibernetic.

Dintr-un alt punct de vedere, al elementelor prelucrate şi al produselor oferite utilizatorilor, am putea vorbi de o altă sistematizare evolutivă, după cum urmează:

- securitatea datelor;
- securitatea datelor şi informaţiilor;
- securitatea datelor, informaţiilor şi cunoştinţelor.

Prin această ultimă prezentare, am intenţionat să suprindem trecerea de la societatea preocupată de creşterea performanţelor prin colectarea mai rapidă a datelor, la societatea informaţională a zilelor noastre, până la societatea ce se conturează în mileniul III, a cunoaşterii.

Analiza locurilor de amplasare a echipamentelor folosite pentru atingerea scopurilor prelucrării, implicit ale securizării, ne va conduce, în timp, spre spaţii tot mai extinse: centre de prelucrare automată a datelor, puncte de amplasare a terminalelor clasice, birouri şi case ale utilizatorilor, clădiri izolate şi/sau grupate – componente ale reţelelor locale, metropole, ţari, grupuri de ţări, ajungând, prin world-wide-web (www), la întreaga planetă.

Dacă, din curiozitate, veţi accesa *www.attrition.org*, veţi afla cât de vulnerabile sunt până şi site-urile marilor corporaţii. În fiecare an, site-uri ale unor companii celebre (Pepsi Cola UK, Egypt Air, U.S.A. Government National Oceanic and Atmospheric Administration, McDonald's etc.) suferă atacuri de diverse naturi.

Soluţia? Măsuri dure de securitate luate pe cont propriu sau prin apelarea la firme care vă asigură împotriva unor astfel de incidente. Liderul mondial absolut îl veţi găsi la adresa *www.counterpane.com*. El vă protejează împotriva pierderilor din cauza hackerilor de până la 1 milion dolari, cu o asigurare de 20.000 dolari anual; cu 75.000 dolari vă asigură anual pierderile de până la 10 milioane dolari; pierderile până la o sută de milioane dolari pot fi asigurate prin sume negociabile.

Oricum, calculatoarele, pe zi ce trece, devin o parte tot mai intimă a vieţii noastre, a tuturor. Despre aspectele securităţii sistemelor informaţionale, pe plan mondial, s-au scris o mulţime de cărţi, s-au ţinut conferinţe sau seminarii internaţionale, dar s-a făcut încă puţin pentru transpunerea lor în practică. Mulţi cred că n-au nevoie de ea sau consideră că necazurile se pot ţine doar de alţii.

Soluţia problemei nu este de natură tehnică, atât timp cât cu mijloace tehnice reduse ca performanţă se pot efectua pagube imense. În mod asemănător, trebuie pusă şi problema securităţii, ea fiind uşor de realizat cu mijloace ieftine. Securitatea sistemelor informaţionale este, în primul rând, o problemă umană, nu tehnică, şi se impune a fi tratată ca atare. Trebuie să se înţeleagă faptul că securitatea sistemelor informaţionale este o componentă de bază a ecuaţiei succesului firmelor. De multe ori, conducerea se interesează doar de reducerea cheltuielilor generale, neglijând aspectele atât de importante ale protejării averii informaţionale. Totuşi, în ultimul timp, se constată o schimbare a opticii manageriale.

Preocupări deosebite pe linia securităţii datelor, îndeosebi a celor prelucrate automat, sau a sistemelor electronice de calcul, în toată complexitatea lor, au apărut încă din anii 1960. Între timp, s-au creat organisme naţionale şi internaţionale, cu un astfel de obiectiv. Au apărut numeroase cărţi, inclusiv cursuri universitare, cu teme apropiate, cum ar fi *Criptografia şi securitatea datelor*, curs predat din anii 1970 la Universitatea George Washington, *Securitatea datelor şi informaţiilor şi contabilitatea analitică*, la universităţile din Delaware şi Ohio. Rezultate remarcabile a înregistrat şi Universitatea din Ontario de Vest, din Canada. Ulterior, în Europa, reţeaua specialiştilor în securitatea sistemelor informaţionale s-a extins din Anglia în

Olanda, Belgia, Suedia, Germania, cuprinzând întreaga arie a ţărilor puternic dezvoltate. În numeroase ţări se predau cursuri universitare care conţin tematici apropiate ca formulare, dar toate au un obiectiv comun: securitatea informaţiilor în sistemele de prelucrare automată a datelor. Ca efect, în universităţi se creează diverse grupuri de iniţiaţi în domeniu, cei mai reprezentativi fiind experţii sau realizatorii de sisteme expert pentru verificarea securităţii, analiza riscului şi evaluarea potenţialelor pagube, sau producătorii de software specializat în auditarea sistemelor informaţionale.

Din anul universitar 1999/2000, la Georgetown University, se predă cursul *Războiul informaţional şi securitatea* pentru studenţii din diverse domenii, cum ar fi cei de la politici internaţionale, de la administraţie publică, administrarea afacerilor, comunicare, ştiinţe exacte şi în toate domeniile socio-umane.

În ultimul timp, chiar se poate vorbi de o mare gamă a specializărilor în foarte complexa problemă a securităţii sistemelor. Până şi legislaţia multor state, începând cu anii 1970, a suferit modificări substanţiale, pe care vom încerca să le redăm succint într-un viitor capitol.

La nivel internaţional, semnificativă este constituirea, încă din 1960, a **IFIP** (International Federation for Information Processing = Federaţia Internaţională pentru Prelucrarea Informaţiilor), creată sub auspiciile UNESCO, care reuneşte cadrele didactice şi alţi specialişti preocupaţi de prelucrarea informaţiilor, în număr de peste 3500. Din ea fac parte organizaţii din 58 de ţări sau regiuni. Activitatea tehnică a IFIP este coordonată prin 14 comisii tehnice, fiecare dintre ele având un număr diferit de grupuri de lucru, care se ocupă cu aspecte concrete ale unui anumit domeniu de activitate. În total, sunt 101 de grupuri de lucru.

Comisiile tehnice[1] sunt:

TC1 – Bazele ştiinţei calculatoarelor
TC2 – Software: teorie şi practică
TC3 – Educaţie informatică
TC4 - neatribuită
TC5 – Aplicaţii în tehnologia informatică
TC6 – Sisteme de comunicaţii
TC7 – Modelarea şi optimizarea sistemelor
TC8 – Sisteme informaţionale (comisia cea mai puternică), cu 7 grupuri de lucru:
- WG8.1 Evaluarea şi proiectarea sistemelor informaţionale
- WG8.2 Interacţiunea sisteme informaţionale – organizaţie
- WG8.3 Sisteme de sprijinire a procesului decizional
- WG8.4 Afaceri electronice (E-Business: cercetare şi practică multidisciplinară)
- WG8.5 Sisteme informaţionale în administraţia publică
- WG8.6 Difuzia, transferul şi implementarea tehnologiilor informaţionale
- WG8.7 – neatribuit
- WG8.8 Carduri inteligente, tehnologie, aplicaţii şi metode
- WG8.9 Sisteme informaţionale ale întreprinderilor

TC9 – Relaţia calculatoare - societate
TC10 – Tehnologia sistemelor electronice de calcul
TC11 – *Protecţia şi securitatea în sistemele de prelucrare a informaţiilor*, cu următoarele grupuri de lucru:
- WG11.1 Managementul securităţii informaţiilor
- WG11.2 Securitatea sistemelor omniprezente (*Pervasive Systems Security*)
- WG11.3 Securitatea datelor şi aplicaţiilor

[1] Potrivit www.ifip.org, ianuarie 2011. Recomandăm site-ul pentru informarea privind domeniile actuale de interes, principalele evenimente profesional-academice şi personalităţile din zona IT.

WG11.4 Securitatea reţelelor şi sistemelor distribuite
WG11.5 Integritatea şi controlul sistemelor – dizolvat în 2007
WG11.6 Managementul identităţii
WG11.7 Tehnologii informaţionale: Abuzurile şi cadrul legal
WG11.8 Educaţia în domeniul securităţii informaţiilor
WG11.9 Criminalistică în mediul digital (*Digital Forensics*)
WG11.10 Protecţia infrastructurilor critice
WG11.11 Managementul încrederii (*Trust Management*)
WG11.12 Aspecte umane ale securităţii şi asigurării informaţionale
WG11.13 Cercetări în domeniul securităţii sistemelor informaţionale

TC12 – Inteligenţa artificială
TC13 – Interacţiunea om-calculator
TC14 – Utilizarea informaticii în divertisment (*Entertainment Computing*)

Pentru a ne edifica asupra rolului unor astfel de organizaţii, vom face o descriere succintă a grupurilor de lucru din comisia tehnică *TC11 – Protecţia şi securitatea în sistemele de prelucrare a informaţiilor*, evidenţiind scopul înfiinţării şi obiectivele urmărite de fiecare dintre ele.

**Comisia TC11** a fost înfiinţată în 1984.

*Scopul* ei este de creştere a siguranţei şi încrederii în informaţiile prelucrate automat, precum şi cel de constituire a unui forum al responsabililor cu securitatea şi al altor specialişti care activează în domeniul securităţii sistemelor de prelucrare a informaţiilor.

Obiectivele urmărite sunt:

- stabilirea unui cadru comun de referinţă pe linia securităţii, pentru organizaţii, specialişti şi publicul interesat;
- promovarea protecţiei şi a securităţii ca o componentă esenţială a sistemelor de prelucrare a informaţiilor.

*Grupul de lucru WG11.1 – Managementul securităţii informaţiilor*, înfiinţat în 1985 şi revizuit în 1992.

*Scopul*: crearea unui cadru managerial pe linia securităţii sistemelor informaţionale ale organizaţiilor, identic celui din domeniul financiar-contabil.

Aspectele urmărite se încadrează într-o paletă foarte largă, de la cele simple, ale securităţii informaţiilor (cum sunt responsabilităţile de nivel superior pe linia documentaţiei privind politicile de securitate), până la aspecte foarte tehnice (cum ar fi analiza riscului, reconstituirea sistemelor după dezastre şi alte instrumente tehnice) – toate concepute pentru sprijinirea procesului de management al securităţii informaţionale.

*Obiectivele* grupului sunt:

- studierea şi promovarea metodelor de sensibilizare a factorilor de decizie pe linia acordării unei importanţe deosebite valorii informaţiilor, considerându-le la fel de importante ca şi valorile patrimoniale, obligându-i să ia toate măsurile necesare pentru protejarea noilor valori;
- studierea şi promovarea metodelor şi căilor de măsurare şi evaluare a nivelului securităţii dintr-o organizaţie şi sensibilizarea conducerii despre importanţa acestora;
- cercetarea şi realizarea de noi căi de identificare a ameninţărilor şi vulnerabilităţii sistemelor din orice organizaţie;
- cercetarea şi realizarea influenţei noilor echipamente şi produse software asupra managementului securităţii informaţionale;
- studierea şi dezvoltarea mijloacelor şi căilor pentru a veni în sprijinul managerilor cu securitatea informaţiilor, prin evidenţierea eficienţei muncii lor şi a calităţii controlului exercitat în unitate;
- fixarea standardelor pe linia securităţii informaţiilor.

*Grupul de lucru WG11.2 – Securitatea sistemelor omniprezente*, constituit în 1985 sub numele „Securitatea sistemelor mici", a fost revizuit în 1992 şi 1995 şi redefinit sub denumirea curentă în 2009.

*Scopul* său este să identifice metodele şi problemele din domeniul securităţii informaţiilor, în particular al celor privind sistemele omniprezente - definite ca fiind sistemele ce includ calculatoarele personale, reţelele locale, dispozitivele mobile, etichetele RFID[2], nodurile de senzori şi alte configuraţii similare, conectate wireless, în care nu există echipamente anume pentru administrarea securităţii, iar utilizatorul final este singurul ce se ocupă de protecţia sistemului.

*Grupul de lucru WG11.3 – Securitatea datelor şi aplicaţiilor*, creat în 1987 şi revizuit în 2001.

*Scopul*:

- să promoveze pe o scară cât mai largă înţelegerea riscului la care se expun societăţile bazate pe sistemele de operare ale bazelor de date cărora le lipsesc măsurile adecvate pe linia securităţii şi intimităţii datelor;
- să încurajeze aplicarea tehnologiilor existente pentru îmbunătăţirea securităţii sistemelor bazelor de date.

*Obiective*:

- promovarea tehnologiilor care sprijină definirea cerinţelor pe linia securităţii pentru sistemele bazelor de date;
- proiectarea, implementarea şi exploatarea sistemelor bazelor de date care să aibă incluse şi funcţii de securitate;
- asigurarea că sistemele bazelor de date implementate satisfac şi cerinţele de securitate.

*Grupul de lucru WG 11.4 – Securitatea reţelelor*, constituit în 1985, revizuit în 1992, 1997 şi 2003.

*Scopul*:

- să studieze şi promoveze procesele acceptate internaţional care să permită echipelor de conducere şi specialiştilor să înţeleagă deplin responsabilităţile ce le revin pe linia exploatării cu încredere şi în condiţii de securitate a reţelelor informaţionale, care vin în sprijinul organizaţiilor, clienţilor acestora sau publicului larg;
- să studieze şi promoveze educaţia şi instruirea pe linia aplicării principiilor, metodelor şi tehnologiile de securitate a reţelelor.

*Obiectivele* sunt:

- promovarea stărilor de încredere şi înţelegere a aspectelor privind reţelele din punct de vedere al securităţii sistemelor informaţionale;
- asigurarea unui forum pentru discuţii, înţelegerea şi clarificarea tuturor aspectelor ce ţin de securitatea reţelelor;
- studierea şi identificarea aspectelor manageriale, procedurale şi tehnice ale securităţii reţelelor;
- studierea şi descrierea riscurilor apărute în contexul includerii sistemului informaţional într-un mediu bazat pe reţele;
- promovarea tehnologiilor şi practicilor care să asigure controlul securităţii reţelelor, să facă posibilă definirea cerinţelor securităţii reţelelor şi, în general, să avanseze constituirea cadrului de bază pentru o securitate eficientă a reţelelor;
- să contribuie, în măsura în care este fezabil şi posibil, la standardizarea internaţională a securităţii reţelelor.

[2] Radio Frequency IDentification

În noul context, aspectele securităţii depăşesc frontierele organizaţiei, întrucât se intră în legătură cu o mulţime de alte sisteme externe, regăsite prin reţelele locale, metropolitane sau internaţionale. În aceste reţele se includ conectările dial-up (telefonice) sau de alte tipuri care permit angajaţilor să lucreze de acasă, dar şi conexiunile ce-i permit organizaţiei să efectueze operaţiuni bazate pe legături reciproce, astfel încât acestea să aibă loc în cadrul acordurilor EDI sau ale comerţului electronic.

*Grupul de lucru WG11.6 – Managementul identităţii* a fost creat în 2006.

*Scopul*:

- să promoveze, prin educaţie şi cercetare, conştientizarea şi înţelegerea următoarelor concepte: managementul identităţii (aplicaţii şi metodologii, securitatea documentelor optice şi electronice, rolul şi funcţiile actuale şi potenţiale ale biometriei), metodele şi tehnicile care sprijină evaluarea unor tehnologii biometrice particulare (aspecte operaţionale şi legale ale biometriei, impactul său asupra societăţii) şi managementul identităţii naţionale (printre altele, şi rolul acestuia în combaterea fraudei, terorismului şi delictelor internaţionale).

*Obiectivele grupului*:

- stabilirea şi promovarea unui lexic comun pentru problemele legate de managementul identităţii, astfel încât întreaga comunitate interesată să vorbească aceeaşi limbă;
- propunerea, definirea şi elaborarea de metodologii şi aplicaţii ale managementului identităţii, care să răspundă standardelor formulate de responsabilii cu deciziile din sectorul public şi privat;
- propunerea, definirea şi elaborarea tehnologii de securitate ale documentelor optice şi electronice, care să răspundă standardelor formulate de responsabilii cu deciziile din sectorul public şi privat;
- propunerea, definirea şi elaborarea de metodologii şi tehnologii biometrice, care să fie încorporate în managementul identităţii (naţionale) şi care să răspundă standardelor formulate de responsabilii cu deciziile din sectorul public şi privat;
- promovarea, prin educaţie şi cercetare, a unei largi înţelegeri a aspectelor sociale şi operaţionale legate de managementul identităţii naţionale în general şi de tehnologiile menţionate mai sus în particular.

*Grupul de lucru WG 11.7 – Tehnologii informaţionale: Abuzurile şi cadrul legal aferent*, constituit în 1990, revizuit în 1992 şi 2001. În prezent, a fuzionat cu grupul de lucru WG 9.6.

*Scopul*:

- să analizeze ameninţările existente şi în curs de apariţie pe linia tehnologiilor informaţionale, precum şi a riscurilor la care se expun oamenii, organizaţiile şi societatea;
- să analizeze principiile securităţii;
- aspecte ale impactului tehnologiilor informaţionale asupra cadrului legal existent, ce poate fi învechit faţă de noul mediu;
- să analizeze mijloacele, cadrul legal, standardele etice, procedurile manageriale, precum şi alţi factori sociali aplicabili în domeniul tehnologiilor informaţionale;
- să identifice soluţii posibile;
- să depisteze noi consecinţe legale, sociale şi organizaţionale ale dezvoltării şi utilizării sistemelor tehnologiilor informaţionale.

*Obiectivele* grupului sunt:

- consolidarea relaţiilor de cooperare dintre comunităţile tratate în comisiile „Calculatoarele şi societatea” şi „Securitatea informaţiilor” pe problematica folosirii inadecvate a tehnologiilor informaţionale şi cadrul legal;
- dezvoltarea echipelor orientate spre studierea:

– ameninţărilor prezente din domeniul tehnologiilor informaţionale şi cadrul legal adecvat;
– riscul la care sunt expuşi oamenii şi organizaţiile din cauza acestor ameninţări;
– responsabilităţile oamenilor şi organizaţiilor pe linia legalităţii utilizării tehnologiilor informaţionale;
– riscul înregistrării unor nesincronizări între prevederile legale, tehnice şi manageriale;
– impactul tehnologiilor informaţionale asupra cadrului juridic existent;

- să propună şi/sau să evalueze prevederile legale pe linia combaterii ameninţărilor la care sunt expuse tehnologiile informaţionale.

*Grupul de lucru WG 11.8 – Educaţia în domeniul securităţii informaţiilor*, constituit în 1991.

*Scopul*:

- să promoveze educaţia şi instruirea pe linia securităţii informaţiilor la nivel de universitate, guvern şi întreaga economie.

*Obiective*:

- crearea unui centru de resurse internaţionale pentru schimbul de informaţii privind educaţia şi instruirea în securitatea informaţiilor;
- realizarea de modele de cursuri de securitate a informaţiilor la nivel de universităţi;
- încurajarea facultăţilor şi universităţilor să includă modele de cursuri adecvate pe linia securităţii informaţiilor, la nivel universitar şi postuniversitar, prin disciplinile de informatică, sisteme informaţionale şi servicii publice;
- realizarea de module de securitate a informaţiilor care să poată fi integrate în planurile de învăţământ ale şcolilor de afaceri şi/sau în cursurile introductive de informatică la nivel de facultăţi şi universităţi;
- promovarea unui modul adecvat despre securitatea informaţiilor pentru facultăţi, universităţi, economie şi organizaţii guvernamentale;
- colectarea, transmiterea şi difuzarea de informaţii privind cursurile de securitate a informaţiilor prin intermediul organizaţiilor private în folosul întregii economii;
- colectarea şi difuzarea periodică a bibliografiei cărţilor de securitate a informaţiilor, articolelor, rapoartelor şi altor suporturi educaţionale.

*Grupul de lucru WG 11.9 – Criminalistică în mediul digital (Digital Forensics)*, format în 2004.

*Scopul:*

- să promoveze, prin educaţie şi cercetare, conştientizarea şi înţelegerea:

- metodelor şi tehnicilor ştiinţifice capabile să stabilească circumstanţele producerii unui incident informatic (ce, când, cum s-a întâmplat, cine a fost autorul şi care au fost consecinţele incidentului), în vederea iniţierii unei acţiuni legale;
- aspectelor legale şi operaţionale ale tehnologiilor noi, capabile să ajute dezvoltarea de asemenea metode şi tehnici.

*Obiective:*

- stabilirea şi promovarea unui lexic comun pentru problemele legate de criminalistica în mediul digital, astfel încât întreaga comunitate internaţională să vorbească aceeaşi limbă;
- propunerea, definirea şi elaborarea de tehnologii care să sprijine tribunalele şi alţi factori de decizie din mediul civil şi militar prin probe digitale credibile;
- promovarea, prin educaţie şi cercetare, a unei înţelegeri cât mai ample a aspectelor legale, operaţionale şi sociale legate de criminalistica în mediul digital;
- sprijinirea cooperării între comunităţile internaţionale, pentru a le implica în discuţii academice privind cercetarea în domeniul criminalisticii digitale şi a aplicaţilor acesteia.

*Grupul de lucru WG 11.10 – Protecţia infrastructurilor critice*, apărut în 2006.

*Scopul:*

- sprijinirea colaborării între ştiinţă, tehnologie şi politică, pentru a dezvolta şi implementa soluţii sofisticate şi practice în acelaşi timp, care vor duce la securizarea averilor informaţionale în sectoarele critice. Grupul doreşte să întărească protecţia infrastructurii informaţionale la toate nivelurile – local, regional, naţional şi internaţional – prin cercetare, dezvoltare şi educaţie.

*Obiective:*

- identificarea aspectelor de securitate informaţionale comune sectoarelor infrastructurii;
- stabilirea interdependenţelor dintre infrastructuri şi importanţa asigurării securităţii lor;
- identificarea principiilor şi tehnicilor de securitate care pot fi aplicate pentru protecţia infrastructurilor critice;
- dezvoltarea de soluţii mixte de protecţie a infrastructurilor, care să înglobeze metode ştiinţifice, tehnici de inginerie şi politici publice.

*Grupul de lucru WG 11.11 – Managementul încrederii*, constituit în 2006.

*Scopul:*

- realizarea unui forum pentru investigarea interdisciplinară a încrederii ca mod de asigurare a siguranţei şi credibilităţii infrastructurii de calcul globale. Disciplinele implicate provin atât din zona tehnică, cât şi din domenii ca dreptul, ştiinţele sociale şi filosofia.

*Obiective:*

- semantici şi modele pentru securitate şi încredere;
- arhitecturi, mecanisme şi politici pentru managementul încrederii;
- încrederea în comerţul electronic, serviciile electronice şi e-guvernare;
- încredere şi intimitate (în colaborare cu WG 11.7);
- managementul identităţii şi încrederii (în colaborare cu WG 11.6);
- aspecte sociale şi legale ale încrederii (în colaborare cu WG 11.7).

Despre grupurile de lucru WG11.12 - *Aspecte umane ale securităţii şi asigurării informaţionale* şi WG11.13 *Cercetări în domeniul securităţii sistemelor informaţionale* nu există, deocamdată, informaţii detaliate pe site-ul IFIP.

În 1974, s-a înfiinţat Institutul pentru Securitatea Calculatoarelor (*Computer Security Institute* – CSI –, cu site-ul *www.gocsi.com*) pentru formarea şi perfecţionarea continuă a specialiştilor în securitatea informaţiilor, a calculatoarelor şi a reţelelor.

În anul 1990, Comitetul pentru Informaţii, Calculatoare şi Politici de Comunicaţie ale Organizaţiei pentru Cooperare şi Dezvoltare Economică (OECD) a constituit un grup de experţi pentru a pregăti ghidul securităţii sistemelor informaţionale. În octombrie 1992, s-a realizat *Ghidul pentru securitatea sistemelor informaţionale*, iar, în noiembrie 1992, cele 24 de ţări membre ale OECD l-au aprobat. Obiectivul de bază l-a constituit crearea unui cadru de bază care să înlesnească dezvoltarea şi introducerea mecanismelor, practicilor şi a procedurilor pentru asigurarea securităţii sistemelor informaţionale. Ghidul se adresa tuturor sistemelor informaţionale din sectorul public şi privat, supuse jurisdicţiei naţionale, prin enunţarea a nouă principii de bază: responsabilitate, conştientizare, etică, multidisciplinaritate, proporţionalitate, integrare, oportunitate, reevaluare periodică, democraţie.

De asemenea, la nivelul anului 1990, Consiliul Cercetării Naţionale al SUA, printr-un raport special, *Computer at Risk* (CAR), prezenta starea securităţii sistemelor informaţionale din SUA şi recomanda şase seturi de acţiuni. Prima recomandare se referea la crearea şi promulgarea *principiilor general acceptate de securitate a sistemelor* (Generally Accepted System Security Principles, GASSP). Recomandarea pentru crearea GASSP a condus la înfiinţarea, la sfârşitul anului 1992, a *Fundaţiei Internaţionale pentru Securitatea Informaţiilor*.

În 1997, comitetul GASSP, care era format din experţi în securitatea informaţiilor din zece ţări, inclusiv SUA, a lansat GASSP, versiunea 1.0, care conţine nouă principii de bază, referite

ca principii universale, bazate pe principiile OECD. În acelaşi timp, Institutul Naţional de Standarde şi Tehnologie din SUA a emis un raport cu aceleaşi nouă principii, aplicabile la nivelul organismelor guvernamentale federale.

Menţionăm şi faptul că, până în anul 1994, a existat *Comitetul Coordonator pentru Controlul Multilateral al Exporturilor* (*Coordinating Committee for Multilateral Export Controls, COCOM*), cu scopul instituirii unui regim comun de control al exporturilor la nivelul celor 17 ţări membre. Acestea erau Australia, Belgia, Canada, Danemarca, Franţa, Germania, Grecia, Italia, Japonia, Luxemburg, Marea Britanie, Norvegia, Olanda, Portugalia, Spania, Statele Unite ale Americii, Turcia. Ca membri asociaţi erau Austria, Coreea de Sud, Elveţia, Finlanda, Irlanda, Noua Zeelandă, Polonia, Singapore, Slovacia, Suedia, Taiwan şi Ungaria – în total 12 ţări. Scopul principal îl constituie restricţionarea exporturilor spre anumite ţări, cum ar fi Libia, Irak, Iran, Coreea de Nord – considerate a fi ţări ce sprijină mişcările teroriste. Exporturile spre alte ţări erau permise, însă pe bază de licenţe.

În 1991, *COCOM* a adoptat *Nota Generală privind Software-ul* (*General Software Note, GSN*), prin care s-a permis exportul de masă al softului criptografiat, inclusiv cel din domeniul public, la nivelul ţărilor membre. De asemenea, erau acceptate exporturile criptografice folosite pentru autentificare, inclusiv produsele folosite pentru criptarea parolelor. Toate ţările membre au respectat Nota, cu excepţia SUA, Marea Britanie şi Franţa.

În iulie 1996, 31 de ţări au semnat Acordul Wassenaar privind Controlul Exporturilor de Arme Convenţionale, Bunuri şi Tehnologii cu Dublă Întrebuinţare. Acesta a fost semnat şi de România, Rusia, Republica Cehă, iar ulterior, de Bulgaria şi Ucraina. Prevederile privind criptografia au fost preluate de la *COCOM*.

Deci, dacă de peste patru decenii sunt preocupări pe linia securităţii informaţiilor prelucrate în sistemele de prelucrare automată, prin cursuri universitare, cărţi, simpozioane ş.a., dacă pe plan internaţional există atâtea organisme care se ocupă de problematica menţionată, considerăm firească abordarea şi la noi, cu mai multă seriozitate, a *Protecţiei şi securităţii informaţiilor*.

Identificaţi câteva repere istorice (la nivel statal, academic sau organizaţional) privind protecţia şi securitatea informaţiilor în România.

## 1.2. Particularităţi ale securităţii sistemelor informaţionale

Odată cu trecerea spre prelucrarea masivă a datelor cu ajutorul calculatoarelor electronice, ca urmare a volumului mare al investiţiilor şi a transferării „grijii” informaţiei către sistemele electronice de calcul, s-a pus într-un alt context problema protejării noilor averi, fizice şi informaţionale. Totul trebuie pornit de la schimbarea opticii privind gestiunea fizică a noilor averi, dar şi de la valorificarea pe multiple planuri a datelor memorate, încercându-se să se obţină alte dimensiuni ale funcţiei de informare a conducerii, prin utilizarea informaţiilor arhivate şi păstrate în alte condiţii.

În vederea obţinerii noilor performanţe, datele prelucrate sunt supuse unor operaţiuni suplimentare în faza de culegere, astfel încât să poată fi valorificate ulterior pe mai multe planuri. Preluarea datelor din două sau mai multe documente operative în unul sau mai multe fişiere, având suportul de înregistrare specific noii variante de prelucrare, constituie o îndepărtare vizibilă de modul tradiţional de păstrare a documentelor primare, de gestionare a lor, şi duce la apariţia mai multor persoane care pot accesa aceleaşi date. Mai mult, prin agregarea înregistrărilor anterioare, pot rezulta chiar noi informaţii.

Cum noile resurse fizice ale sistemelor de calcul sunt destul de scumpe, se constată o tendinţă de centralizare a prelucrărilor de date, din motive de economie, dar, în acelaşi timp,

sporeşte grija asigurării securităţii lor, întrucât riscul pierderii lor sau al consultării neautorizate este şi mai mare. Într-un astfel de caz, nu trebuie uitat principiul dominant al prelucrării automate a datelor, GIGI (Gunoi la Intrare, Gunoi la Ieşire), conform căruia o eroare strecurată într-un sistem integrat se propagă cu o viteză inimaginabilă, în zeci sau sute de locuri din sistem, generând, la rândul ei, o multitudine de erori în rapoartele ce se vor obţine ulterior.

Alt element, deosebit de important, îl constituie factorul uman. Dacă în vechile sisteme erau uşor de controlat locurile de păstrare a informaţiei, acum, într-un mediu puternic informatizat, persoanele cu atribuţii de urmărire a modului de realizare a securităţii datelor au o misiune mult mai dificilă. Se pot înregistra două cazuri: fie că nu pot intui căile prin care datele pot fi accesate pe ascuns, în vederea sustragerii sau modificării lor, fie că nu reuşesc să descopere de unde şi cine, cu ajutorul unui calculator aflat la distanţă de locul păstrării datelor, are acces neautorizat în sistem. Surpriza poate veni tocmai de la persoanele care lucrează cu cea mai mare asiduitate la anumite aplicaţii. Loialitatea excesivă, în acest caz, poate da de gândit.

Prin trecerea la prelucrarea automată a datelor (p.a.d.) s-au schimbat şi suporturile informaţiei, precum şi mijloacele de lucru, situaţie în care apar noi aspecte, şi anume:

*Densitatea informaţiei* este mult mai mare în mediul informatic decât în sistemele clasice, bazate pe hârtie. Prin utilizarea discurilor optice sau a stick-urilor USB, zeci de volume, însumând zeci de mii de pagini de hârtie, pot fi introduse cu multă uşurinţă într-un buzunar. CD-urile, DVD-urile, cardurile, memoriile flash, hard-discurile portabile şi alte suporturi moderne pot fi astfel subtilizate discret, cu eforturi minime dar cu efecte distructive majore.

*Obscuritatea sau invizibilitatea* constituie o altă problemă, întrucât conţinutul documentelor electronice şi al rapoartelor derivate stocate pe suporturile enumerate mai sus nu poate fi sesizat pe cale vizuală la un control de rutină. De multe ori, cei puşi să controleze nu au pregătirea informatică şi nici echipamentele necesare pentru a observa o eventuală sustragere de fişiere.

*Accesibilitatea* datelor din sistemele de calcul este mai mare, cel puţin pentru o nouă categorie de infractori, catalogaţi „hoţi cu gulere albe”, făcându-se trimitere vădită la nivelul de cultură, în primul rând informatică, al acestora.

*Lipsa urmelor* eventualelor atacuri criminale constituie un alt element îngrijorător al noului mediu de lucru. Ştersăturile din vechile documente pentru schimbarea sumelor, precum şi adăugările de noi înregistrări „cu creionul” nu mai există, modificările în fişierele electronice sunt efectuate cu multă lejeritate şi foarte greu de depistat ulterior.

*Remanenţa suporturilor*, după ce au fost şterse, poate constitui o cale sigură de intrare în posesia informaţiilor memorate anterior. Se cunosc numeroase programe de restaurare a fişierelor şterse.

*Agregarea datelor*. Puse laolaltă, datele capătă altă valoare decât cea avută prin păstrarea lor în mai multe locuri separate unele de altele. Uneori, informaţiile de sinteză sunt valorificate prin programe speciale în vederea obţinerii, tot cu ajutorul calculatorului, a strategiei şi tacticii firmei într-un anumit domeniu. Edificator este cazul benzilor magnetice ale firmei IBM, care conţineau direcţiile de cercetare pe următorii 15 ani, intrate în posesia unei firme dintr-o ţară concurentă.

*Necunoaşterea calculatoarelor*. Pentru foarte multe persoane, îndeosebi de vârstă înaintată, calculatorul este investit cu forţe supraomeneşti, ceea ce le conferă o încredere oarbă în datele obţinute prin intermediul lui. De asemenea, din motive de nepricepere, aceşti anagajaţi pot fi victime uşoare ale corupătorilor ... informatizaţi.

*Progresul tehnologic*. Rezultatele cercetărilor tehnico-ştiinţifice se transformă zi de zi în tehnologii din ce în ce mai performante de accesare a datelor. Nu acelaşi lucru se poate spune şi despre progresele înregistrate în domeniul securităţii datelor.

*Comunicaţiile şi reţelele*, devenind tot mai performante, au extins aria utilizatorilor, atât din punct de vedere numeric, cât şi al dispersiei în teritoriu, întregul spaţiu terestru fiind accesibil

reţelelor foarte mari. Odată cu noile progrese, şi aria utilizatorilor rău intenţionaţi s-a mărit, precum şi variantele de furt informatizat.

*Integrarea puternică a sistemelor* apare ca o consecinţă a îmbunătăţirii formelor de comunicaţie şi a proliferării reţelelor de calculatoare. Pe acelaşi canal de comunicaţie sunt transmise tot felul de date. În plus, introducând o dată eronată în sistem, de la un banal punct de vânzare, ea pătrunde cu rapiditate în zeci de fişiere şi, implicit, aplicaţii ale firmei. Comerţul şi afacerile electronice au deschis şi mai mult apetitul „specialiştilor" în fraudă.

*Apariţia utilizatorilor finali informatizaţi* constituie un veritabil succes, dar sporeşte şi riscul pierderii datelor importante din calculatorul principal al companiilor.

*Standardele de securitate*, în pofida atâtor altor domenii în care se înregistrează mutaţii vizibile în intervale scurte de timp, nu se concretizează în forme general valabile şi, cât timp un lucru nu este interzis prin reguli scrise, el ori se consideră că nu există, ori se trage concluzia că este permis.

Totuşi, efortul uman pentru protejarea, asigurarea sau securizarea sistemelor s-a accentuat în mod vizibil. În tabelul 1.1 am redat numărul de site-uri care tratează concepte specifice temei discutate, la nivelul lunilor aprilie 2002 şi ianuarie 2011, folosind motorul de căutare Google. După cum se observă, se detaşează net conceptele: *internet security, network security, information security, computer security, data protection, digital signature, e-security* – în ordinea numărului de apariţii în site-uri.

În concluzie, odată cu dezvoltarea noilor sisteme informaţionale şi cu transferarea către acestea a secretelor firmelor, trebuie văzut în ele, în acelaşi timp, ajutorul numărul unu, dar şi elementele cele mai tentante pentru noii criminali. Hardul şi softul pot fi manevrate cu multă uşurinţă de către om. În acest caz, ca şi în altele intrate în obişnuinţa cotidiană, „inteligenţa" calculatorului lasă de dorit, putându-se spune că tot omul (a)sfinţeşte ... calculatorul, motiv esenţial pentru sporirea preocupărilor tuturor specialiştilor din domeniul securităţii sistemelor informaţionale.

*Tabel nr. 1.1 – Numărul site-urilor ce tratează concepte specifice protecţiei şi securităţii sistemelor informaţionale*

| Nr. crt. | Conceptul căutat cu Google | 2002 | 2011 |
|---|---|---|---|
| 1. | **computer security** | **534.000** | **8.890.000** |
| 2. | **information security** | **439.000** | **13.600.000** |
| 3. | **data security** | 305.000 | **2.860.000** |
| 4. | **data protection** | **495.000** | **12.700.000** |
| 5. | information protection | 36.700 | 714.000 |
| 6. | information assurance | 36.500 | 839.000 |
| 7. | data assurance | 569 | 90.900 |
| 8. | **computer protection** | 7.720 | **2.160.000** |
| 9. | computer data protection | 171 | 39.900 |
| 10. | computer assurance | 1.820 | 11.800 |
| 11. | network assurance | 590 | 181.000 |
| 12. | network protection | 12.800 | 253.000 |
| 13. | **network security** | **615.000** | **14.700.000** |
| 14. | **internet security** | **758.000** | **82.200.000** |
| 15. | internet protection | 19.100 | 284.000 |
| 16. | internet assurance | 169 | 36.600 |
| 17. | computer vulnerability | 1.140 | 34.600 |
| 18. | data vulnerability | 908 | 9.230 |
| 19. | information vulnerability | 713 | 22.100 |
| 20. | network vulnerability | 6.910 | 408.000 |
| 21. | internet vulnerability | 1.320 | 48.000 |
| 22. | **digital signature** | 217.000 | **1.940.000** |

| Nr. crt. | Conceptul căutat cu Google | 2002 | 2011 |
|---|---|---|---|
| 23. | digital protection | 1.790 | 42.500 |
| 24. | e-signature | 11.800 | 600.000 |
| 25. | **e-security** | 140.000 | **1.490.000** |
| 26. | e-protection | 5.600 | 349.000 |

Propuneţi alte concepte relevante pentru domeniul protecţiei şi securităţii informaţionale şi completaţi tabelul de mai sus cu numărul paginilor oferite ca răspuns de motorul de căutare Google pentru ele.

### 1.2.1 Vulnerabilitatea microcalculatoarelor

Odată cu lansarea IBM-ului în producţia de microcalculatoare, în 1981, acest domeniu a înregistrat progrese uluitoare. Dacă la început nu au fost luate în seamă, acum s-a ajuns ca un microcalculator de câteva sute de dolari să efectueze ceea ce, cu doar câteva zeci de ani în urmă, efectuau doar calculatoarele mari, de milioane de dolari.

Apariţia milioanelor de utilizatori a dus la constituirea unei adevărate bresle de specialişti în „butonat" – a se citi apăsarea tastelor –, cu destul de puţine cunoştinţe despre teoria sistemelor informaţionale şi cu nici o teamă de implicaţiile posibile ale unui sistem fără securitate. De la utilizatorii izolaţi s-a trecut la constituirea de reţele puternice, care au împânzit orice colţ al organizaţiilor. Următoarele trepte au constat în depăşirea graniţelor firmei, ale oraşului, respectiv ale ţării. S-a creat, astfel, posibilitatea ca sistemele bazate pe calculatoare mari să fie accesate din sute sau mii de locuri, afectând substanţial integritatea, confidenţialitatea şi accesibilitatea datelor.

Datorită microcalculatoarelor, se poate spune că s-a înregistrat un progres colosal pe linia domeniilor de aplicabilitate ale informaticii. Ele rezolvă rapid şi ieftin o mulţime de probleme de planificare tehnico-economică, de exploatare, de administrare, procesare de texte, comunicaţii şi alte facilităţi de lucru în reţea. În aceste condiţii, microcalculatoarele aduc şi noi forme de manifestare a slăbiciunii sistemelor electronice de calcul şi a vulnerabilităţii lor. Hazardul joacă un rol din ce în ce mai mare, astfel:

1. De la bun început ele au fost concepute mult mai prietenoase decât vechile sisteme, deci destul de tentante în a fi utilizate şi de copiii şi de funcţionarii fără prea multe cunoştinţe tehnice, aceasta concretizându-se în:
   a) *apariţia numeroaselor eşecuri sau erori în operaţiunea de creare a copiilor de siguranţă* – de exemplu, realizarea lor pe suportul intern de memorare al aceluiaşi microcalculator, chiar pe aceeaşi partiţie de disc;
   b) *eşecuri în controlul accesului sistemului*. Sistemele de protecţie prin parole nu se folosesc la toate microcalculatoarele, iar când există nu sunt folosite corespunzător, parolele fiind cunoscute de mai mulţi utilizatori, şi nu numai atât, ele aflându-se scrise pe o bucată de hârtie, lipită pe colţul monitorului sau pe masa de lucru;
   c) *tratarea tuturor datelor la fel*, omiţându-se cele de o importanţă deosebită, care ar trebui să aibă cu totul alt regim;
   d) *greşeli în păstrarea şi utilizarea resurselor sistemului*. Discurile de orice tip, casetele, benzile sunt împânzite prin toată unitatea, prin toate birourile, putând fi folosite sau sustrase cu multă uşurinţă de alte persoane. Un suport din afară poate fi introdus printre cele deja existente, strecurându-se astfel şi viruşii distructivi. Hârtia de imprimantă (de regulă cea care conţine mici greşeli sau a doua copie a unei lucrări efectuate în două exemplare), benzile tuşate ale acesteia (riboanele), celelalte „resturi" sunt accesibile noilor „scormonitori în gunoaie informatice", cu scopul de a găsi „un colţ de pâine" printre informaţiile conţinute de aceste materiale;

e) *scrutarea cu uşurinţă a sistemului*. Deseori, din pură curiozitate, un coleg, un prieten, un copil venit în vizită la biroul părinţilor, având cunoştinţe limitate despre calculatoare, încep să „se joace" cu tastele unui microcalculator pornit, situaţie în care se pot distruge date foarte importante. Mai periculos este cazul în care „joaca" are un scop anume;

2. Calculatoarele nu mai sunt doar la dispoziţia specialiştilor, ci şi a altor persoane, care nu cunosc prea multe lucruri despre alte tipuri de sisteme. Odată cu apariţia microcalculatoarelor, problemele de instruire informatică se pun într-un alt mod;
3. Prin politica de instaurare a unor restricţii în utilizare, apelându-se la sistemul parolelor multiple, din faza de iniţializare a sistemului până la accesul la căi şi fişiere, se reduce dramatic viteza de prelucrare, deci scade productivitatea sistemului;
4. Fiind plasate în aproape toate birourile, iar condiţiile de păstrare puternic diversificate, riscul defectării este diferit de la un birou la altul;
5. Resursele întregului sistem fiind împrăştiate prin toate colţurile unităţii, securitatea tradiţională a sălii calculatorului unic dispare, aceasta având ca rezultat:
   a) documentaţia sistemului, softul, manualele de utilizare sunt ineficient folosite sau în condiţii de risc sporit;
   b) pierderea cheilor de deschidere a PC-urilor le poate face inutilizabile o perioadă de timp;
   c) softul de aplicaţii se realizează în mod haotic, ducând uneori la lucrul în paralel la aceeaşi problemă, neexistând o evidenţă centralizată a preocupărilor;
   d) parolele nu se înregistrează, deci nu poate fi vorba de un control al lor;
   e) manualele de utilizare sunt păstrate neglijent, iar când sunt necesare nu mai sunt de găsit;
6. Actele cu scop de fraudă pot fi săvârşite cu mai multă uşurinţă şi de către mai multe persoane, ceea ce diminuează eficienţa controlului;
7. Prin preluarea de către calculator a activităţilor prestate anterior de mai multe persoane, posibilitatea de furt, fără complotul mai multor angajaţi, devine mult mai lejeră;
8. Persoanele care în condiţiile prelucrării clasice aveau grija şi posibilitatea de a lucra doar într-un domeniu, destul de limitat, pot să-şi extindă aria „cunoaşterii" asupra întregii baze de date a unităţii;
9. Pe suporturile cu capacitate de memorare foarte mare, fiind ascunse datele deosebit de importante, acestea erau mai greu de găsit, în schimb, pe un disc optic sau video disc operaţiunea este mult mai uşoară;
10. Sistemele de operare ale microcalculatoarelor nu dispun de aceleaşi performanţe de protecţie precum sistemele mari;
11. Slaba securitate, însoţită de facilităţile de lucru în reţea, conduce la sporirea posibilităţilor de accesare neautorizată a sistemului;
12. Datele pot fi preluate pe un PC fie din reţea, fie din calculatorul mare şi tipărite sau transferate pe diverse tipuri de discuri, cu scopul sustragerii lor;
13. Resursele locale ale unui PC pot fi folosite de către utilizatorii lor pentru a ataca reţeaua sau calculatorul central;
14. Prin dimensiunile lor reduse şi greutatea mică, PC-urile sunt uşor de mutat dintr-un loc în altul, ceea ce sporeşte riscul defectării lor;
15. Posibilitatea defectării sau întreruperii temporare a sursei de alimentare cu energie electrică este mult mai mare decât în cazul unei singure săli a calculatoarelor.

Pornind de la elementele de vulnerabilitate a microcalculatoarelor prezentate mai sus, identificaţi elemente similare de vulnerabilitate a calculatoarelor portabile şi, respectiv, a telefoanelor mobile folosite în organizaţii.

## 1.2.2 Forme de manifestare a pericolelor în sistemele informaţionale

Datelor supuse prelucrării automate trebuie să li se asigure cel puţin aceleaşi condiţii de protecţie ca şi celor prelucrate manual. Totuşi, din cauza creşterii riscului prin informatizare, aşa cum rezultă din descrierea sumară a vulnerabilităţii noilor sisteme, se impun şi unele măsuri suplimentare de realizare a protecţiei, situaţie în care utilizatorii trebuie să cunoască în detaliu natura noilor ameninţări. Literatura de specialitate le grupează în diverse moduri. Oricum, ele pot fi sintetizate în trei mari categorii:

- ameninţări cauzate de incidente ivite în sistem;
- factori naturali, bazaţi pe hazard;
- ameninţarea sistemelor prin acţiunea voită a omului.

### 1.2.2.1 Ameninţări cauzate de incidente ivite în sistem

Realitatea a demonstrat că există următoarele cauze care pot afecta securitatea sistemelor:

1. *Apariţia unor defecţiuni la echipamentele sistemului*. De multe ori micile defecţiuni, în special cele cu o perioadă de manifestare foarte scurtă, sunt mai greu de detectat şi reparat decât cele catastrofale. Având un caracter imprevizibil, pentru ele nu se pot stabili anumite măsuri de prevenire. Mai grav este atunci când ele nu au forme sesizabile în momentul producerii, iar datele eronate apar mult mai târziu, făcând reconstituirea celor originale foarte anevoioasă sau chiar imposibilă;
2. *Apariţia inevitabilelor erori umane*, conform dictonului „errare humanum est”, conduce la luarea elementarei măsuri preventive de reducere substanţială a intervenţiei umane în procesul de prelucrare a datelor cu ajutorul calculatorului electronic. Cauzele erorilor pot fi: indiferenţa cu care se exercită o anumită operaţiune, slaba instruire, entuziasmul excesiv, înţelegerea greşită a modului de funcţionare a sistemului. Erorile pot să aparţină operatorilor, dar, şi mai grav, programatorilor. Riscul cel mai mare provine din posibilitatea perpetuării modului eronat de exercitare a operaţiunilor sau a programării. Soluţiile constau în introducerea în soft a mai multor teste de validare a introducerilor de date, iar, pe linia programării, apelarea la standardizare sau la utilizarea sistemelor CASE (Computer Aided Software Engineering);
3. *Funcţionarea defectuoasă a softului*. Chiar şi atunci când se apelează la un întreg arsenal de metode de testare a lui, softul poate păstra anumite vicii ascunse, care să producă erori inimaginabile. Este cazul programelor foarte mari, de milioane de linii sursă, care, practic, sunt tot mai greu de controlat. Edificator este cazul unui academician rus care a demisionat dintr-o importantă funcţie informatică din ministerul apărării, întrucât spunea că pericolul producerii unor grave incidente, cu efecte nebănuite asupra securităţii omenirii, devine tot mai mare, din cauza imposibilităţii controlării programelor. Multitudinea ramificaţiilor din program poate să ducă la „scurt-circuitarea” lor, generând căi imprevizibile de execuţie, concretizate în luarea unor decizii surprinzătoare;
4. *Întreruperea sistemului de alimentare cu energie sau funcţionarea lui în afara parametrilor tehnici admişi*. În această categorie intră şi “căderea” legăturilor de comunicaţie, precum şi a altor utilităţi necesare sistemului.

### 1.2.2.2 Factorii naturali, bazaţi pe hazard

Calculatoarele sunt sisteme deosebit de sensibile. Deseori sunt comparate cu creierele umane, deci asemănarea poate continua. Dacă pe creier se depun mici cheaguri de sânge, el funcţionează eronat sau poate să-şi înceteze exercitarea funcţiilor sale. „Cheagurile” calculatoarelor pot fi: exces de umiditate, exces de căldură, praf, fire de păr, scrum de ţigară ş.a. Nu sunt de neglijat diversele insecte, îndeosebi muşte, ţânţari, păianjeni, gândaci, viespi, viermi. Cel mai mare pericol îl reprezintă „mouse”-ul, dar de data aceasta cel adevărat, adică micuţul şoricel.

Tot în această categorie intră cutremurele, vijeliile, furtunile, inundaţiile şi alte forme de dezlănţuire a naturii.

#### 1.2.2.3 Ameninţarea sistemelor prin acţiunea voită a omului

Ca orice avere, şi cea informaţională stârneşte tentaţii umane, iar regula decalogului, care îndeamnă să „nu furi", nici în acest caz nu este respectată. S-au constituit, în timp, grupuri de „specialişti" care exploatează slăbiciunile sistemelor. Cel mai grav este faptul că unii realizatori de sisteme sunt şi cei mai periculoşi duşmani ai propriilor creaţii, fiind un fel de „Kronoşi" ai vremurilor noastre, devorându-şi propriii lor „copii", adică sistemele. Motivele atacurilor pot fi destul de variate: de la spionajul industrial, militar, până la cele mai meschine interese. Atacurile pot fi deliberate sau accidentale, deschise sau mascate (ascunse).

1. *Spionajul şi serviciile secrete* acţionează, de regulă, în domeniul militar, dar îşi fac simţită prezenţa şi în industrie, comerţ, învăţământ, cercetare ş.a. Căile de obţinere a informaţiilor variază de la banalele apeluri telefonice, până la sofisticatele metode tehnice de captare a datelor. Microfonul ascuns într-o cameră este deja o formă de primitivism, întrucât au proliferat tehnici de-a dreptul miraculoase de captare.
2. *Duşmanii, nedreptăţiţii şi neloialii dintre angajaţii firmei*. Această categorie nu apelează la tehnici prea performante, deoarece, desfăşurându-şi activitatea în interiorul sistemului, pot înfăptui acte criminale cu mijloace mult mai simple. Motivaţia lor poate să fie un câştig personal sau o răzbunare. Mai grav este cazul când o terţă persoană din sistem, investită cu autorizarea unor operaţiuni, în mod involuntar, contribuie la înfăptuirea atacului.
   Trecerea spre PC-uri, culturalizarea informatică a utilizatorilor constituie reale ameninţări pentru sistemele informaţionale. Cu banii plătiţi de firmă, întrucât efectuează atacul în timpul programului de lucru din birou, angajaţii devin duşmanii cei mai periculoşi ai unităţii. Tot în această categorie sunt încadraţi şi greviştii.
3. *Vandalii şi huliganii* au la dispoziţie forme noi de manifestare, renunţând la bâte şi pietre, dar apelând la spargeri informatice, la viruşi ş.a. Mai periculoşi sunt cei strecuraţi în unitate pe principiul calului troian. Zicala „Doamne, spune-mi duşmanul care mi-e prieten, căci pe celălalt îl ştiu eu" trebuie să devină un adevărat crez pentru conducerea unităţilor.
4. *Utilizatorii* pot să contribuie substanţial la pierderile informatizate, îndeosebi prestând activităţi nestandardizate şi neautorizate. Pe primul loc se află jocurile pe calculator, care, pe lângă faptul că înseamnă folosirea resurselor firmei în scop personal şi irosirea timpului de lucru, chiar dacă este o simplă distracţie, devin cea mai sigură sursă de „importare" a viruşilor. Pe locul doi se află softul tentant, de ultimă oră, necumpărat de firmă, dar aflat în posesia unui „prieten". Deşi este „procurat" cu intenţii vădit benefice firmei, se transformă în altceva.
   Pentru evitarea acestor cazuri, se impun: instruirea personalului, controlarea şi supravegherea permanentă a lui, precum şi interzicerea utilizării altor materiale decât a celor aflate în posesia legală a unităţii.
5. *Organizaţiile subversive şi teroriste* şi-au găsit noi căi de înfăptuire a obiectivelor. Există chiar organizaţii care îşi propun, în mod declarat, abolirea calculatoarelor. Din nou, cei mai periculoşi sunt angajaţii unităţii care aparţin acestor grupuri. Formele lor de manifestare pot fi foarte inteligente, dar şi foarte violente. Se pare că viruşii cei mai periculoşi sunt realizaţi de astfel de grupări.
6. *Ziariştii*, în intenţia de a realiza articole de senzaţie, pe principiul „scopul scuză mijloacele", scurmă în „Berevoieştiul informatic" sau chiar în locurile, aparent, bine tăinuite.
7. *Publicul larg*, din pură curiozitate informaţională sau din dorinţa de a-şi verifica aptitudinile informatice, atentează la integritatea multor sisteme.

8. *Adolescenţii*, deşi fac parte din categoria anterioară, au forme specifice şi rezultate deosebite în atacarea sistemelor. De cele mai multe ori, dispun de cunoştinţe informatice impresionante, care, dacă se cuplează cu accesul la datele folosite de părinţii lor în sistemele informaţionale, devin extrem de periculoşi. Printre ei se află cei mai împătimiţi hackeri, phrackeri şi alte categorii descrise ulterior.
9. *Criminalii* devin noii bogaţi ai zilelor noastre. Unele firme nu raportează pierderile cauzate de atacurile informatice, fie pentru a nu da curaj şi altora să încerce, fiind deja un precedent, fie de teama de a nu fi trase la răspundere că nu au luat cele mai bune măsuri de asigurare a securităţii, fie pentru a nu face un nume prost aplicaţiilor folosite. Cu calculatorul s-au înfăptuit cele mai multe crime perfecte. Cum motivaţia lor este evidentă, furtul, investiţiile făcute de organizaţiile care se ocupă cu o astfel de „activitate" sunt mult mai mari pe linia „cercetării ştiinţifice" decât ale oricărei firme în parte pe linia asigurării securităţii sistemului.

În S.U.A., atacurile sunt abordate printr-un număr mai mic de categorii, în care se regăsesc cele enunţate anterior, după cum urmează:

1. *Atacurile tăinuite ale angajaţilor* (subversive). Aceste atacuri pot duce la distrugerea echipamentelor sau a celorlalte componente ale sistemului, aflarea unor programe secrete sau a căilor de accesare a sistemului, modificarea programelor şi a datelor, inclusiv crearea de drepturi băneşti, distrugerea programelor şi a datelor, furturile bunurilor materiale sau informatice, precum şi folosirea voit eronată a componentelor sistemului, sub formă de sabotaj.
2. *Acţiunile neintenţionate ale angajaţilor* (neglijenţa). Efectul acestor acţiuni poate să se concretizeze în dezvăluirea unor informaţii secrete, modificarea programelor şi a datelor, întreruperea serviciilor, pierderea programelor şi a datelor, precum şi distrugerea echipamentelor.
3. *Evenimentele întâmplătoare*. Astfel de evenimente se pot concretiza în întreruperea funcţionării echipamentelor/sistemelor, modificarea programelor şi a datelor, pierderea programelor şi a datelor, distrugerea echipamentelor.
4. *Atacuri secrete ale persoanelor din afara unităţii*. Scopul lor poate fi aflarea unor informaţii secrete, întreruperea funcţionării sistemelor, modificarea programelor şi a datelor, distrugerea echipamentelor şi a celorlalte componente, furtul averilor informaţionale.
5. *Atacuri deschise din afară* (în forţă). Rolul lor este de întrerupere a funcţionării sistemului sau de distrugere a lui.
6. *Atacurile deschise ale angajaţilor* au un scop identic celor anterioare.
7. *Acţiuni neintenţionate din afara unităţii* (introduceri eronate). Prin astfel de acţiuni se pot produce întreruperi ale funcţionării sistemului, modificări ale datelor sau ale programelor.

În S.U.A., în „topul atacurilor", pe primul loc s-au aflat angajaţii incapabili ai firmelor, urmaţi de cei incorecţi şi de furturile din afară. Relativ recent, s-a extins categoria tinerilor pricepuţi la calculatoare, care, de acasă, pot accesa sistemele mari, considerând acţiunile lor ca un test de isteţime, dar care au devenit din ce în ce mai periculoase. În anii 1998-2001, pe locul întâi s-au aflat atacurile cu viruşi, pe locul doi – utilizarea abuzivă, din interior, a reţelelor locale, iar pe locul trei – furtul de laptopuri.

La nivelul anului 2004, cele mai importante ameninţări asupra securităţii organizaţiilor Fortune 1000 au fost[3]:

1. violenţa la locul de muncă;

[3] *** (The sixth annual Pinkerton survey), *Top Secret Security Threats Facing Corporate America*, www.pinkertons.com

2. crizele de management;
3. fraudele, hoţii cu gulere albe;
4. accesul angajaţilor în zone nepermise;
5. furtul de hardware/software;
6. furtul (în general) comis de către angajaţi;
7. atacurile prin Internet, intranet;
8. prezenţa drogurilor la locul de muncă;
9. lipsa de etică a managerilor;
10. furtul din exterior, vandalismul.

Se observă că 6 dintre cele 10 ameninţări de top proveneau din interiorul organizaţiilor.

Naivitatea angajaţilor care cad victime atacurilor phishing şi dezvăluie informaţii confidenţiale, furtul de laptop-uri care generează furtul de ... identitate, tot din neglijenţa posesorilor calculatoarelor portabile, lipsa de coerenţă a administratorilor care creează conturi de acces şi uită să le schimbe la plecarea angajaţilor din firmă, imposibilitatea de a diferenţia mesajele spam de cele legitime, alături de neutilizarea patch-urilor de securitate sunt, la nivelul anului 2006, potrivit Forrester Research, ameninţările cele mai grave, care au ca numitor comun neglijenţa angajaţilor.

O tendinţă care poate fi extrasă din analiza rapoartelor CSI/FBI din perioada 2003 – 2007 este conştientizarea constantă a necesităţii investiţiilor în securitate la nivelul firmelor analizate, care are ca efect reducerea breşelor de securitate şi implicit a atacurilor. Dintre măsurile adoptate de firme menţionăm training-urile în domeniul politicilor de securitate şi al securităţii reţelelor, auditul sistemelor de securitate, introducerea de măsuri de securitate în reţele (inclusiv criptografie), ca şi la nivelul controlului accesului.

În 2011, Panda Security [4] a menţionat atacuri ca „hacktivism" si cyber-war, malware orientat tot mai mult pe obţinerea de profit, atacuri asupra reţelelor sociale, inginerii sociale şi coduri maliţioase ce au abilitatea de a se adapta, pentru a evita detectarea, ca şi despre creşteri ale ameninţărilor la adresa utilizatorilor de Mac şi eforturi ale infractorilor de a ataca sistemele pe 64 de biţi şi de a exploata noi vulnerabilităţi "zero-day" (semnalate dar neacoperite încă de producător printr-un patch).

- Realizaţi un „top 3" al celor mai distructive incidente care pot afecta securitatea informaţională a unei organizaţii cunoscute de dvs. Motivaţi „nominalizările".
- Realizaţi un „top 3" al celor mai periculoşi atacatori ai unui sistem informatic din cadrul unei organizaţii cunoscute de dvs. Motivaţi „nominalizările".
- Realizaţi un „top 3" al celor mai grave erori umane care pot influenţa securitatea unui sistem informatic din cadrul unei organizaţii cunoscute de dvs. Motivaţi „nominalizările".
- Care este, în opinia dvs., cea mai spectaculoasă ameninţare informatică a zilelor noastre? Argumentaţi.

## 1.2.3 Asigurarea securităţii sistemelor informaţionale

Când se proiectează noi aplicaţii informatice, grija principală a realizatorilor trebuie să o constituie protejarea datelor prelucrate. În orice mediu de lucru, datele trebuie să respecte principiile C.I.A.:

- *Confidenţialitatea* se concretizează în oferirea condiţiilor de păstrare în conformitate cu restricţiile legale descrise de utilizatori şi proiectanţi. Numai persoanele autorizate pot accesa datele sistemului, luându-se măsuri de prevenire a accesului neautorizat;

[4] Corrons, L., director tehnic al Panda Security, citat în Bîrzoi, V., *De unde vor veni principalele ameninţări informatice în 2011*, 16 decembrie 2011, la http://businesscover.ro/de-unde-vor-veni-principalele-amenintari-informatice-in-2011

- *Integritatea*, ceea ce înseamnă că ele trebuie să fie păstrate în forma originală. Datele nu trebuie să fie modificate prin consultare sau pe căi ilegale, nici accidental. De asemenea, ele nu trebuie să fie expuse pericolului distrugerii involuntare. Integritatea este o măsură a corectitudinii datelor şi a asigurării încrederii în ele;
- *Accesibilitatea* se referă la asigurarea accesului la date, pentru cei autorizaţi, în orice moment.

Pentru o organizaţie cunoscută de dvs., realizaţi un clasament al celor mai importante 5 averi informaţionale, precizând pentru fiecare dintre ele dacă este importantă asigurarea confidenţialităţii şi/sau integrităţii şi/sau accesibilităţii. Justificaţi.

Sistemele informaţionale, pe linia asigurării securităţii lor, au multe elemente comune cu celelalte sisteme. Dintre măsurile comune, amintim pe cele organizatorice şi administrative, de personal, de protecţie fizică şi a mediului de lucru.

Particularităţile protecţiei unui sistem informaţional se referă la luarea unor măsuri speciale de apărare a datelor, prin intermediul *echipamentelor* de prelucrare automată a datelor, *softului* de sistem sau de aplicaţii, precum şi al *comunicaţiilor*, dacă se lucrează într-un astfel de mod. Toate acestea vor avea un tratament special.

După prezentarea elementelor vulnerabile din diversele medii informatizate de lucru, putem spune că securitatea, în astfel de sisteme, se referă la:

1. identificarea şi evaluarea elementelor patrimoniale de protejat, astfel încât nimic să nu fie omis, iar valorile deosebite să aibă un tratament special;
2. recunoaşterea de la bun început a vulnerabilităţii şi slăbiciunii sistemelor informaţionale;
3. specificarea tuturor atentatelor posibile asupra sistemelor electronice de calcul, în general, şi asupra unei aplicaţii informaţionale anume, în special;
4. evaluarea potenţialelor pierderi sau riscuri generate de un anumit incident, cu toate consecinţele care decurg de aici;
5. realizarea, implementarea şi consolidarea unor metode de asigurare a securităţii, cu costuri rezonabile, pentru reducerea riscurilor de deteriorare a sistemelor, inclusiv a bazelor de date, la valori minime, asigurându-se obiectivele pentru care au fost realizate sistemele;
6. pregătirea planurilor de reconstituire a datelor pierdute din cauza dezastrelor;
7. controlul şi auditarea periodică a eficienţei măsurilor de asigurare a securităţii sistemului.

Regulile generale, aplicabile tuturor sistemelor de securitate, concretizate în 20 de măsuri preventive, sunt următoarele:

1. Stabilirea autorizărilor;
2. Asigurarea loialităţii şi încrederii personalului;
3. Stabilirea modalităţilor prin care acţiunile de autorizare să fie eficiente;
4. Identificarea mijloacelor materiale prin care să se realizeze protecţia;
5. Inventarierea elementelor de protejat;
6. Gruparea valorilor importante pentru o mai bună protecţie;
7. Stabilirea zonelor de amplasare a valorilor protejate;
8. Apărarea valorilor protejate;
9. Asigurarea verificării bunurilor protejate;
10. Restricţii privind utilizarea bunurilor protejate şi a mecanismelor de protecţie;
11. Controlul accesului la bunurile protejate;
12. Expunerea redusă a bunurilor protejate;
13. Privilegii limitate privind bunurile protejate;
14. Responsabilităţi clare pe linia bunurilor protejate;

15. Consemnarea, în scris, a faptelor care au afectat valorile patrimoniale;
16. Verificarea dublă a tuturor operaţiunilor referitoare la valorile patrimoniale;
17. Elaborarea documentaţiilor de analiză a operaţiunilor cu valori patrimoniale;
18. Cercetarea tuturor neregulilor;
19. Sancţionarea abaterilor;
20. Crearea posibilităţii de redresare, în orice moment, după unele acţiuni care au eşuat.

Fiecare mecanism de protecţie trebuie să realizeze obiectivele pentru care a fost conceput. Eficienţa lui nu trebuie să depindă de prezumţii false privind imposibilitatea atacării sistemului. El trebuie să demonstreze *completitudine*, ceea ce se va concretiza printr-o funcţionare normală la orice eventuală ameninţare, *corectitudine*, prin oferirea răspunsurilor anticipate, îndeosebi atunci când s-ar înregistra intenţii frauduloase sau s-ar produce erori în utilizare. Mecanismul perfect trebuie să fie *cât mai simplu posibil*, precum şi *uşor de întrebuinţat* şi să ofere *un număr cât mai mic de erori sau alarme false*.

*Supravieţuirea* lui este o altă proprietate, stabilindu-se cu o precizie cât mai mare perioada de funcţionare la un anumit nivel asigurat al protecţiei, în condiţii optime de utilizare. De asemenea, trebuie să *ofere soluţii pentru întreruperile de energie, defectarea sistemelor de comunicaţie, variaţii bruşte ale temperaturii ş.a*.

Nu trebuie uitat raportul *cost sistem - eficienţă*.

Care este, în opinia dvs., cea mai importantă regulă generală de securitate pentru o organizaţie? Argumentaţi.

## 1.3 Mecanisme de apărare – prezentare generală

Literatura de specialitate consemnează şapte mecanisme de asigurare a eficienţei securităţii sistemelor informaţionale:

1. *Securitatea fizică* se referă la controlul accesului fizic în sistem şi se va concretiza sub diverse moduri: de la împrejmuiri ale amplasamentelor şi uşi, la lacăte şi sisteme de alarmă, inclusiv crearea cadrului de intervenţie în cazuri de urgenţă.
2. *Securitatea personalului* presupune selecţia, urmărirea, autorizarea şi supravegherea angajaţilor.
3. *Criptarea informaţiilor importante* înseamnă protejarea datelor comunicate la distanţă, făcându-le neinteligibile pentru orice alte persoane decât cele autorizate a le recepţiona.
4. *Studierea tehnicilor specializate ale intruşilor* astfel încât echipamentele acestora să nu poată pătrunde în configuraţia sistemului.
5. *Suprimarea radiaţiilor compromiţătoare* este o operaţiune necesară pentru că echipamentele folosite în centrele de prelucrare automată a datelor produc radiaţii acustice şi electromagnetice, care pot fi interceptate şi analizate. Este cazul consolelor, imprimantelor, cablurilor de legătură, al echipamentelor de vizualizare ş.a.
6. *Securitatea liniilor de comunicaţie* se referă la garantarea comunicării corecte pe liniile care interconectează componentele sistemului, astfel încât intruşii să nu le poată penetra.
7. *Securitatea sistemelor de prelucrare automată a datelor* se ocupă de protejarea datelor din sistem împotriva accesului neautorizat, prin prisma autorizării utilizatorilor şi a protejării datelor, stabilindu-se reguli foarte precise de folosire a lor.

Gradul de confidenţialitate a informaţiei protejate va determina ce mecanisme de apărare să fie folosite, conform figurii 1.1.

| Mecanism de securitate | Categoria informaţiilor | | | |
|---|---|---|---|---|
| | Strict secrete | Secrete | Confidenţiale | Cu restricţii |
| Fizică | X | X | X | X |
| Personal | X | X | X | X |
| Criptografică | X | X | | |
| Tehnică | X | | | |
| Radiaţii | X | | | |
| Linii de comunicaţie | | | X | |
| Sistemul de prelucrare automată a datelor | | | X | X |

**Fig. 1.1 Protecţia informaţiei prin mecanisme specializate**

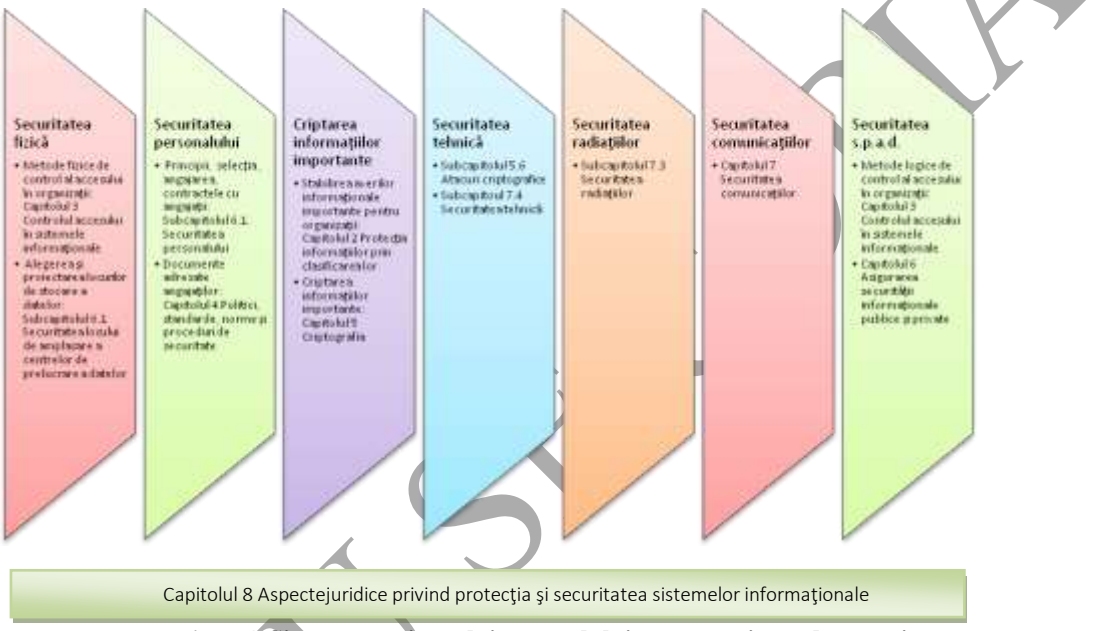


**Fig. 1.2 Sinteza conţinutului manualului pe mecanisme de securitate**

Modul în care mecanismele generale de mai sus sunt tratate în prezentul manual este vizibil în diagrama din figura 1.2.

- Care este, în opinia dvs., cel mai important mecanism de securitate pentru o organizaţie cunoscută de dvs.? Justificaţi, cu exemple.
- Din ce motiv credeţi că nu au fost bifate cu X căsuţele cu fundal mai închis din Figura 1.1?

## Rezumat

Alături de capital şi oameni, informaţia este una dintre averile deosebite ale firmei. Pentru a periclita această resursă importantă, orice persoană care dialoghează cu calculatorul unei organizaţii poate să facă (cel puţin) următoarele lucruri: să copieze fişierele importante ale altor firme, să influenţeze evidenţele altora pentru a le cauza pierderi, să reprogrameze calculatoarele incluse în configuraţia sistemelor de producţie pentru a provoca avarierea utilajelor sau pentru producerea accidentelor umane, să şteargă programe sau fişiere. Din acest motiv, considerăm absolut necesară tratarea cu prioritate de către manageri a problemelor de securitate informaţională.

În funcţie de tehnologiile folosite şi de evoluţia în timp a preocupărilor ce o privesc, securitatea informaţională poate fi abordată prin prisma unui număr mai mare sau mai mic de generaţii. Capitolul 1 prezintă şi câteva repere din istoria modernă a preocupărilor internaţionale pe linia protecţiei şi

securităţii informaţionale, cu dorinţa de a conştientiza cititorii de necesitatea unei discipline de profil în cadrul Facultăţii de Economie şi Administrarea Afacerilor.

În orice mediu de lucru, datele trebuie să respecte principiile C.I.A – Confidenţialitate, Integritate, Accesibilitate. Urmărind acesastă triadă, particularităţile protecţiei unui sistem informaţional se referă la luarea unor măsuri speciale de apărare a datelor, prin intermediul echipamentelor de prelucrare automată a datelor, softului de sistem sau de aplicaţii, precum şi al comunicaţiilor, dacă se lucrează într-un astfel de mod. Măsurile de apărare sunt necesare pentru a contra-pondera pericolele care vizează informaţiile dintr-o organizaţie: incidentele, facotrii naturali, bazaţi pe hazard, atacurile.

Literatura de specialitate consemnează şapte mecanisme de asigurare a eficienţei securităţii sistemelor informaţionale: securitatea fizică, securitatea personalului, criptarea informaţiilor importante, studierea tehnicilor specializate ale intruşilor, suprimarea radiaţiilor compromiţătoare, securitatea liniilor de comunicaţii, securitatea sistemelor de prelucrare automată a datelor, care vor fi tratate pe parcursul capitolelor următoare.

CAPITOLUL II

# Protecţia informaţiilor prin clasificarea lor

Dacă survolăm istoria preocupărilor pe linia securităţii informaţiilor, cu oarecare surprindere, vom constata că ele datează de multe mii de ani. Nu ne propunem să efectuăm o analiză minuţioasă pe această temă, ci doar să redăm câteva momente esenţiale.

Printre obiectivele capitolului de faţă se numără:

- (re)cunoaşterea necesităţii de clasificare a informaţiilor şi a principalelor criterii folosite pentru aceasta;
- familiarizarea cu tipurile de informaţii ce sunt supuse clasificării;
- identificarea principalelor roluri şi responsabilităţi în procesul de clasificare a datelor;
- cunoaşterea modalităţilor de marcare şi distrugere a materialelor cu regim special dintr-o organizaţie.

## 2.1 Forme embrionare de protejare a informaţiilor

Dacă în urmă cu peste 10.000 de ani s-au realizat primele forme de ţinere a evidenţei produselor necesare hranei unei comunităţi umane, făcându-se trimitere la perioada neolitică a Orientului Mijlociu – cam în anii 8500 î.C. –, tot atunci s-au înregistrat şi primele preocupări pe linia securizării informaţiilor păstrate. Produsele obţinute erau evidenţiate prin mici forme realizate din lut, diferenţiate după proprietar, dar, cum recolta se ţinea în comun, în hambarele comunităţii, şi obiectele se păstrau în vase speciale, cu particularităţi date de gestionarul produselor, vase pe care el le sigila după rularea argilei umede, constituindu-se forme asemănătoare unor mingi de mărimi diferite. Când proprietarul voia să-şi ia înapoi ceea ce-i aparţinea, magazionerul spărgea vasul cu însemnele de lut ale acestuia, operaţiune efectuată în prezenţa martorilor. *Acesta este considerat primul protocol de securitate*.

După vreo patru mii de ani, pe teritoriul actualului Peru, s-au realizat forme mai lejere de evidenţă, prin intermediul nodurilor de pe funii sau sfori. La fel de bine, am putea spune că, în urmă cu şase mii de ani, oamenii au început să fie traşi pe sfoară, chiar dacă ea se numea la peruvieni *quippos*. Firesc, trăgea pe sfoară cel ce avea „grija” ei. N-ar trebui să ne punem problema că ele nu se păstrau în condiţii de securitate deplină.

Cu vreo 3000 de ani î.C. s-a inventat *scrierea*. Dar şi aceasta era securizată. Se spune că preoţii egipteni interziceau folosirea scrierii alfabetice pe pământul reavăn, ca, nu cumva, muritorii de rând să aibă acces la invenţiile vremii. Vă amintiţi de celebrul tablou „Şcoala de la Atena”, în care Pitagora demonstrează pe nisip teorema sa. Tragem concluzia că prezenta o informaţie publică.

După altă o mie de ani au apărut *formele echivalente ale actualelor obligaţiuni, avize de expediţie* ş.a. În acelaşi timp, adică în urmă cu circa patru mii de ani, au început să se folosească *lingourile de metal* ca obiecte universale de schimb. Cu 750 de ani î.C. s-au inventat *monedele*, şi procesul evolutiv a continuat, până s-a ajuns la *sistemul de contabilitate în partidă dublă*. Procesul fost surprins în prima carte de acest tip, de Luca Paciolo, în 1494, când, din motive de securitate a operaţiunilor, au fost promovate principiile dublei reprezentări şi dublei înregistrări, deşi acestea apăruseră în anii 1300. După renascentism s-au înfăptuit multiple sisteme de securitate; o bună parte din ele se regăsesc în mai multe capitole ale cărţii de faţă.

Cunoaşteţi şi alte momente istorice relevante în clasificarea informaţiilor? Prezentaţi-le succint, precizând sursa bibliografică.

## 2.2 Începuturile clasificării moderne a informaţiilor

După scurta istorie a preocupărilor vizând securitatea, să ne apropiem de vremurile noastre şi de punctul de vedere al securităţii sistemelor faţă de tipurile de informaţii protejate.

Dacă după cel de-al doilea război mondial au rămas atâtea amintiri neplăcute, se cuvine, totuşi, să recunoaştem şi câteva moşteniri teribile. Ne gândim la cercetarea operaţională, a lui Claude Shannon, transferată din domeniul militar în cel economic, la aportul lui Alan Turing în domeniul tehnicilor de criptare-decriptare a datelor, dar şi la ceea ce ne interesează pe noi mai mult, marcarea documentelor cu regim special. NATO are meritul principal în dezvoltarea acestui sistem, al clasificării. *Clasificare* înseamnă etichetări crescătoare ale documentelor sau informaţiilor, de la cel mai de jos nivel, unde se situează informaţiile deschise (*open*) sau neclasificate (*unclassified*), la cele confidenţiale, urcând spre informaţii secrete şi strict secrete (*top secret*).

Iniţial, s-a pornit de la ideea că informaţiile care prin compromitere pot *costa vieţi umane* sunt marcate „secrete", în timp ce informaţiile a căror compromitere costă *pierderea multor vieţi umane* sunt definite „top secret" (strict secrete). Angajaţii în domeniul securităţii sistemelor sunt investiţi cu responsabilităţi diverse, dar şi cu dreptul de a lucra cu anumite categorii de informaţii. Se poate vorbi de o strânsă legătură între responsabilităţi şi categoriile de informaţii cu care se dă dreptul de a lucra. În SUA, dreptul de verificare a fişierelor cu amprente ale FBI este acordat doar pentru verificarea unor informaţii secrete, în timp ce o verificare de tip „top secret" dă dreptul de accesare a tuturor datelor despre locurile de muncă din ultimii 5 până la 15 ani.

Pe linia accesului la unele categorii de informaţii, pentru exercitarea controlului lucrurile sunt mai clare: un oficial poate citi documentele dintr-o anumită categorie numai dacă el are cel puţin împuternicirea de accesare a informaţiilor din categoria respectivă sau dintr-una superioară. De exemplu, un împuternicit să acceseze informaţii „strict secrete" poate citi informaţii confidenţiale, secrete şi strict secrete, iar unul cu drept de accesare a informaţiilor secrete nu le poate accesa pe cele „strict secrete". Regula este că informaţiile pot circula doar în sus, de la confidenţial la secret şi strict secret, în timp ce invers, de sus în jos, pot circula doar dacă o persoană autorizată ia în mod deliberat decizia de a le declasifica.

De asemenea, s-au stabilit reguli de păstrare a documentelor, după cum urmează: documentele confidenţiale sunt păstrate în dulapuri cu cheie, în orice birou guvernamental, în timp ce documentele din categoriile superioare necesită seifuri de un anumit tip, uşi păzite şi control asupra copiatoarelor şi al celorlalte echipamente electronice.

Sunt foarte puţine unităţi care au proceduri stricte pe linia asigurării securităţii informaţiilor. Pe de altă parte, la nivel naţional există proceduri foarte riguroase privind secretul de stat. De regulă, există o ierarhie a ceea ce este cunoscut sub numele de clasificare, prin care orice document şi alte elemente importante sunt încadrate într-o anumită categorie.

Se practică *două strategii de bază* pe linia securităţii naţionale:

*1. Tot ceea ce nu este interzis este permis.*

*2. Tot ceea ce nu este permis este interzis.*

În Statele Unite ale Americii, prima strategie este cea care guvernează accesul la informaţiile guvernamentale. În multe ţări de pe glob, accesul la informaţiile naţionale este controlat prin legi privind secretul de stat, folosindu-se cea de-a doua strategie. Un angajat loial şi devotat firmei nu discută afacerile acesteia până când nu are convingerea că problema respectivă poate să fie făcută publică.

Se apelează la *două tactici de implementare a strategiei* fundamentale privind protejarea informaţiilor deosebite:

- *controlul discreţionar al accesului ;*
- *controlul legal al accesului.*

Prima tactică de control al accesului implementează *principiul celui mai mic privilegiu*: nici o persoană, în virtutea rangului sau a poziţiei ce o deţine, nu are drepturi nelimitate de a vedea informaţiile deosebite, iar persoanele care au o astfel de facilitate trebuie să le vadă numai pe cele care intră în sfera lor de activitate. Controlul discreţionar al accesului este aplicat printr-o matrice de control, conform modelului redat în fig 2.1. Pentru fiecare persoană (subiect) aflată pe listă şi pentru fiecare informaţie (obiect), matricea arată ceea ce poate face fiecare subiect cu obiectele din listă: citire, scriere, execuţie, aprobare ş.a.

| SUBIECT/OBIECT | OBIECT 1 | OBIECT 2 | OBIECT 3 |
|---|---|---|---|
| SUBIECT 1 | Execută | Citeşte | Citeşte/ Scrie |
| SUBIECT 2 | Aprobă | Execută | Citeşte |
| SUBIECT 3 | Citeşte/Scrie | Aprobă | Execută |
| SUBIECT 4 | Citeşte | Citeşte/Scrie | Aprobă |
| SUBIECT 5 | Execută | Citeşte | Citeşte/Scrie |

**Fig. 2.1 Matrice de control al accesului**

Controlul legal al accesului îşi exercită forţa pe baza legilor existente (legea securităţii naţionale, legea energiei atomice ş.a.). În SUA, prin lege, sunt stabilite două tipuri de structuri de control: ierarhizate şi neierarhizate.

*Structura ierarhizată* încadrează informaţiile senzitive în patru categorii: strict secrete, secrete, confidenţiale şi neclasificate.

Primele trei categorii sunt referite printr-o denumire generică: *informaţii clasificate*.

În alte ţări NATO, inclusiv Canada, a patra categorie este cunoscută sub numele de *informaţii restrictive*.

În structura neierarhizată sunt două categorii: *compartimentate* şi *cu obiecţii* sau *ascunse vederii unor categorii de persoane*. Compartimentările pot avea nume scurte, suficient de sugestive, care să scoată în relief aspecte cum sunt: *SECOM* (securitatea comunicaţiei), *CRIPTA* (criptare), *COMSEC* (comunicaţii secrete), *HUMINT* (*Human INTeligence*), *SIGINT* (*SIGnal INTeligence*), *IMINT* (*IMage INTeligence*) ş.a. Categoria „cu obiecţii" priveşte îndeosebi naţionalitatea potenţialilor cititori şi autori ai obiectelor. În SUA, contestaţiile (obiecţiile) sunt: *NOFOR* (*no foreign* = neaccesibile străinilor), *US/UK EYES ONLY* (de văzut numai de către englezi sau americani) ş.a.

Informaţiile strict secrete, care sunt într-o anumită compartimentare, se numesc *informaţii senzitive compartimentate* şi presupun o atenţie deosebită la întrebuinţare. Doar o categorie este superioară acesteia din urmă. Este vorba despre *informaţiile din planul operativ integrat unic* sau *răspunsul naţional în caz de război*.

Clasificarea şi legislaţia din România sunt prezentate în capitolul 9.

Informaţi-vă despre cazul *Wikileaks*. Argumentaţi pro sau contra oportunităţii existenţei acestui proiect.

# 2.3 Clasificarea informaţiilor

Atunci când informaţiile au fost împărţite în două mari categorii, clasificate şi neclasificate, s-a ţinut cont de anumite principii. Pentru a le cunoaşte, însă, este nevoie de o abordare preliminară a unor concepte[1].

Guvernele pornesc de la o clasificare mai largă, împărţind informaţiile în două mari tipuri: *informaţii subiective* şi *informaţii obiective*. Anterior a operat o altă clasificare: *informaţii „operaţionale”* şi *informaţii „ştiinţifice”*. Unii chiar au menţionat un al treilea tip de informaţii clasificate de guverne – *informaţii „tehnice”*, însă în multe materiale, informaţiile tehnice şi cele ştiinţifice sunt submulţimi ale informaţiilor obiective.

## 2.3.1 Informaţii subiective

*Informaţiile subiective* au mai fost caracterizate şi ca *„secrete adevărate”*, iar alţi autori le-au numit *informaţii „operaţionale”* sau *secrete operaţionale*. Cel mai potrivit nume este, însă, informaţii subiective sau *secrete subiective*. Aceste informaţii sunt unice pentru guvern, în sensul că el decide asupra modului în care se vor derula principalele activităţi ce-i revin. Cât timp guvernul controlează şi protejează informaţiile pe baza cărora ia decizii, acele informaţii nu pot fi dezvăluite independent de către adversar. De exemplu, în domeniul militar, o informaţie subiectivă este cea referitoare la planul de invadare a altei ţări (momentul şi locul invaziei). Adversarul nu are cum să producă o astfel de informaţie, dar o poate obţine numai prin spionaj sau dezvăluire neautorizată.

Aceste informaţii au următoarele caracteristici:

- *dimensiune redusă* – secretul poate fi exprimat prin doar câteva cuvinte; din această cauză poate să fie furat cu uşurinţă şi dat altora;
- *perceptibilitate universală* – nu este nevoie de pregătire specială pentru a înţelege secretul; oricine poate să-l fure;
- *supuse arbitrarului* – pentru a intra în posesia lor un adversar le poate fura; secretul nu poate fi descoperit independent;
- *conţinutul poate fi schimbat* – secretul poate fi modificat şi în ultima clipă; dacă o ţară a aflat că adversarul cunoaşte momentul şi locul invaziei, acestea pot fi schimbate;
- *sunt perisabile după scurt timp* – secretele au o viaţă scurtă; după declanşarea invaziei, adversarul a aflat secretul, el devenind public; în concluzie, secretul poate fi ţinut doar pentru o perioadă scurtă de timp.

Daţi exemple de informaţii subiective întâlnite în cadrul organizaţiilor economice. Justificaţi importanţa lor pentru respectivele organizaţii.

## 2.3.2 Informaţii obiective

*Informaţiile obiective* sunt acelea care chiar dacă sunt descoperite, dezvoltate sau controlate de către guvern, pot fi deja cunoscute sau pot fi descoperite independent de o altă ţară. În această categorie intră *informaţiile ştiinţifice* sau *secretele ştiinţifice*. Asupra acestui fel de informaţii nu se poate avea un control absolut. Ele ţin de natura lucrurilor, nu de un secret. Oamenii de ştiinţă din alte ţări, independenţi unii de alţii, pot face descoperiri identice. Informaţiile de acest tip sunt referite şi ca *informaţii obiective* sau *secrete „obiective”*.

Informaţiile obiective sunt marcate de următoarele caracteristici:

[1] U.S. Department of Energy – „Identification of Classified Information”, *Office of Classification*, December 1991, Chapter IV, Part B, § 3.

- *sunt confuze* – de regulă, nu se bazează pe o formulă magică; pentru descrierea informaţiilor ştiinţifice sunt necesare rapoarte lungi; din această cauză ele nu se pot transmite cu uşurinţă;
- *pot fi înţelese numai de către oamenii de ştiinţă*;
- *nu sunt supuse arbitrarului* – şi alţii pot să afle răspunsul la o anumită întrebare ştiinţifică, dacă formulează întrebarea cuvenită;
- *nu sunt supuse schimbării* – au caracter etern; un fenomen natural are o singură valoare;
- *pot avea o viaţă lungă ca secret* – alţii pot descoperi informaţiile în mod independent, dar o astfel de descoperire necesită mult timp, ceea ce va conduce la păstrarea secretului pentru o lungă perioadă.

Daţi exemple de trei informaţii obiective întâlnite în cadrul organizaţiilor economice. Justificaţi importanţa lor pentru respectivele organizaţii.

### 2.3.3 Informaţii tehnice, văzute ca secrete obiective

Al treilea tip de informaţii nu se încadrează perfect în categoriile cunoscute – subiective sau obiective, ele fiind informaţii tehnice, de genul proiectelor şi execuţiilor tehnice ale unor noi arme, diferite de caracterul ştiinţific al proiectării, fiind cunoscute sub denumirea de *informaţii tehnice, văzute ca secrete obiective*.

Caracteristicile informaţiilor tehnice sunt similare cu cele ale informaţiilor ştiinţifice, dar există unele diferenţe între aceste două tipuri. Spre deosebire de informaţiile ştiinţifice, informaţiile tehnice nu sunt fenomene naturale, ci înseamnă o metodă, un proces, o tehnică sau un echipament angajate în crearea unui produs. Se poate spune că informaţiile tehnice sunt utilizate pentru exploatarea informaţiilor ştiinţifice. Cu toate acestea, în domeniul clasificării informaţiilor, cele ştiinţifice şi tehnice sunt considerate că formează un singur tip de informaţii.

Daţi exemple de trei informaţii tehnice, văzute ca secrete obiective, întâlnite în cadrul organizaţiilor economice. Justificaţi importanţa lor pentru respectivele organizaţii.

### 2.3.5 Secrete subiective, secrete obiective şi secrete comerciale

Cu toate că există două tipuri principale de informaţii clasificate (secrete subiective şi obiective), legea secretului comercial recunoaşte numai un tip al secretelor comerciale – secretele obiective. Secretele comerciale includ informaţiile despre procesele de fabricaţie, „reţetele" unor produse (cum este cazul formulei de fabricaţie pentru Coca-Cola®), precum şi alte informaţii obiective care pot fi descoperite independent de către alte afaceri. Multe secrete comerciale sunt asemănătoare informaţiilor ştiinţifice şi tehnice.

Secretele subiective nu sunt protejate prin legile secretului comercial. Dacă un guvern poate clasifica şi proteja datele privind invazia unei alte ţări (informaţii subiective), o firmă nu poate primi protecţia secretului comercial pentru data la care îşi planifică să introducă în fabricaţie un nou produs.

Daţi exemple de alte secrete comerciale cunoscute de dvs.

## 2.3.6 Determinarea necesităţii clasificării informaţiilor

În vederea clasificării informaţiilor se parcurg trei etape distincte:
1. stabilirea nevoii de clasificare;
2. determinarea nivelurilor clasificării;
3. determinarea duratei clasificării.

**Stabilirea nevoii de clasificare**

Etapa se realizează în cinci paşi principali:
a. definirea cu exactitate a informaţiilor de clasificat (opţional, dar recomandat);
b. stabilirea dacă informaţiile se încadrează într-unul din domeniile supuse clasificării;
c. verificarea dacă informaţiile se află sub control guvernamental;
d. concluzionarea dacă dezvăluirea informaţiilor poate să conducă la cauzarea daunelor pentru securitatea naţională;
e. specificarea precisă a nevoii de clasificare a informaţiilor (opţional, dar recomandat).

**Determinarea nivelurilor clasificării**

Atunci când o informaţie trebuie să fie clasificată ei i se va atribui un nivel de clasificare, ceea ce va evidenţia importanţa relativă a informaţiei clasificate în sistemul naţional de securitate, specificându-se cerinţele minime pe care trebuie să le îndeplinească acea informaţie.

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

În *sistemul american de clasificare a informaţiilor* există trei niveluri de clasificare: top secret (strict secret), secret şi confidenţial. Informaţiile neclasificate constituie o altă categorie. În Legea 182/2002 privind protecţia informaţiilor clasificate, din România, informaţiile clasificate din clasa secretelor de stat sunt încadrate în trei niveluri, astfel: strict secrete de importanţă deosebită, strict secrete şi secrete.

*Informaţiile strict secrete* (SUA), cărora le corespund *informaţiile strict secrete de importanţă deosebită* (România), sunt informaţiile a căror divulgare neautorizată este de natură să producă daune de o gravitate excepţională securităţii naţionale.

*Informaţiile secrete* (SUA), ceea ce echivalează cu *informaţiile strict secrete* (România), sunt informaţiile a căror divulgare neautorizată este de natură să producă daune grave securităţii naţionale.

*Informaţiile confidenţiale* (SUA), corespunzătoare *informaţiilor secrete* (România), sunt informaţiile a căror divulgare neautorizată este de natură să producă daune securităţii naţionale.

Apreciem că o nesincronizare a nivelurilor de clasificare din sistemul românesc cu cel american este o probă de neinspiraţie, cu atât mai mult cu cât intrarea în NATO generează, probabil, multe disfuncţionalităţi circulaţiei informaţiilor clasificate. Considerăm că, în timp, nivelurile securizării din România vor fi schimbate tocmai pentru eliminarea neajunsurilor menţionate anterior.

**Determinarea duratei clasificării**

Guvernele clasifică informaţiile şi aplică proceduri de securitate specială documentelor şi materialelor ce le conţin sau sunt purtătoare ale acelor informaţii pentru a preîntâmpina obţinerea lor de către adversari, cu intenţia de a le folosi împotriva deţinătorului autorizat. Din păcate, informaţiile clasificate nu stopează, în mod automat, accesul adversarilor la ele. Se

spune[2] că pentru păstrarea în mare taină a informaţiilor trebuie fie să nu spui nimănui acele informaţii, fie să foloseşti metoda căpitanului Kidd. Totuşi, cum informaţiile trebuie să fie utilizate de mai mulţi guvernanţi, ele nu pot fi ţinute în taină de o singură persoană. Pe de altă parte, metoda căpitanului Kidd, de păstrare a secretului, este de neacceptat. În consecinţă, *guvernele folosesc metoda clasificării informaţiilor pentru a asigura păstrarea secretului*. Metoda căpitanului Kidd, din păcate, a operat mult timp în istoria omenirii. El era un căpitan pirat despre care se spune că îşi îngropa comorile cu scopul de a le recupera ulterior. Toţi cei care participau la astfel de operaţiuni erau ucişi, încât nimeni altul decât Kidd nu mai ştia locul ascuns al comorilor. Discipolii lui Kidd au lansat chiar sloganul sadic „Trei persoane pot păstra un secret dacă două dintre ele sunt omorâte".

În general, informaţiile, oricât ar fi de preţioase, nu pot fi păstrate o perioadă nelimitată de timp fără să fie aflate de adversari. Uneori ei le obţin prin spionaj. Alteori, ele sunt aflate datorită proastei gestionări de către posesorul autorizat. Sunt şi cazuri în care, îndeosebi pentru informaţiile ştiinţifice şi tehnice, adversarii le obţin cu eforturi proprii, prin invenţii şi inovaţii.

Chiar dacă informaţiile pot fi păstrate ani mulţi fără a fi aflate de adversari, nu este, de regulă, recomandat să se păstreze perioade îndelungate. Clasificatorii informaţiilor sunt cei ce vor hotărî dacă este cazul să se specifice timpul de păstrare a informaţiei clasificate sau să se indice momentul în care va interveni declasificarea automată. Durata informaţiilor clasificate trebuie să fie atât de scurtă cât să nu genereze costuri fără rost cu păstrarea lor. Nici duratele prea scurte nu sunt recomandate, deoarece adversarii ar intra prea devreme în posesia lor şi ar putea acţiona pentru şubrezirea întregului sistem de securitate naţională. În concluzie, doar clasificatorul trebuie să aibă grija stabilirii duratei de clasificare.

Când se încearcă a se discuta despre durata de păstrare a informaţiilor clasificate, părerile sunt destul de diferite. În SUA, în 1970, într-un raport al unui organism specializat, s-a făcut următoarea declaraţie: „Este puţin probabil ca informaţiile clasificate să poată fi protejate o perioadă mai mare de cinci ani şi este mult mai rezonabil să presupunem că ele devin cunoscute de către alţii în perioade de cel mult un an, prin descoperire independentă, dezvăluire clandestină sau alte mijloace." Alţi specialişti au declarat că experienţa istoriei demonstrează că nici un secret militar nu poate fi păstrat prea mult; în unele cazuri există aproape întotdeauna o limită definită de timp, în funcţie de importanţă. Un director al Departamentului Apărării din SUA declara că durata păstrării informaţiilor clasificate poate fi influenţată de o serie de factori, după cum urmează: nivelul la care se află tehnologia, succesele raportate de serviciile secrete proprii sau ale adversarilor, precum şi realizările din domeniile politic, militar şi tehnic. De reţinut este faptul că nu există o formulă magică sau un anumit standard pentru stabilirea numărului de ani de păstrare a informaţiilor clasificate sau a echipamentelor sau materialelor ce prelucrează sau conţin astfel de informaţii.

În final, se poate spune că perioada de păstrare a informaţiilor clasificate depinde de tipul informaţiei ce urmează a fi protejată (subiectivă sau obiectivă; operaţională sau ştiinţifică), de numărul persoanelor care cunosc informaţia clasificată, de procedurile de securitate folosite pentru protejarea acestor informaţii, precum şi de calităţile celor puşi să le păstreze şi protejeze.

Durata clasificării informaţiilor se determină prin una dintre următoarele metode:

a. ca o perioadă de timp măsurată de la data emiterii documentului;
b. în funcţie de un eveniment viitor ce poate să apară înaintea operaţiunii de declasificare;
c. dacă data, respectiv evenimentul nu pot fi specificate, atunci documentul conţinând informaţii clasificate va fi marcat, pentru a se indica instituţia aflată la originea lui, ce va avea sarcina declasificării.

[2] Katz, A.H. – „Classification: System or Security Blanket", *J. Natl. Class. Mgmt. Soc.*, 8, 76-82 (1972), p. 81

Daţi exemple de trei informaţii dintr-o organizaţie care este necesar să fie clasificate. Precizaţi nivelul de clasificare pe care le aşezaţi şi propuneţi durate de clasificare, în funcţie de natura informaţiilor şi obiectul de activitate al organizaţiei. Argumentaţi.

## 2.4 Clasificarea asocierilor de informaţii

Informaţiile ce nu sunt clasificate, uneori, sunt supuse clasificării ca urmare a asocierii lor cu alte informaţii care, implicit sau explicit, conduc la dezvăluirea altor informaţii care sunt clasificate. Clasificarea asocierilor este referită ca o *clasificare prin context*[3], ce nu trebuie să fie confundată cu clasificarea prin compilare, descrisă ulterior.

De regulă, clasificarea informaţiilor prin asociere este rezultatul cuplării informaţiilor despre părţile echipamentelor sau despre materiale folosite pentru fabricarea echipamentelor clasificate. Astfel, un echipament comercial nu poate fi el însuşi clasificat, dar asocierea lui cu un proiect clasificat poate conduce la clasificare numai în contextul asocierii cu acel proiect. La fel se întâmplă şi cu materialele, îndeosebi chimice. Alteori, simpla prezenţă a numelui unei persoane pe o listă de distribuţie a materialelor, care este un document neclasificat, poate să conducă la clasificarea acestuia dacă persoana este managerul unui proiect clasificat. Dacă un expert tehnic vizitează un loc al cărui obiect de activitate este clasificat, atunci şi vizita expertului trebuie să fie clasificată. Dacă se cere o astfel de clasificare, persoana vizitatoare va figura cu un nume fictiv.

În ultimul timp, localităţile în care se află amplasamente clasificate sunt subiectul unor supravegheri sporite, îndeosebi pe linia scurgerii de substanţe chimice care poluează mediul. Operaţiunea este efectuată de agenţii specializate, organizaţii neguvernamentale, echipe de investigare diverse. Toate acestea solicită datele primare pentru identificarea chimicalelor folosite, inclusiv concentraţiile lor, pe baza unor probe preluate din atmosferă, din scurgeri de ape reziduale, din pânza de apă freatică, din sol ş.a. În cele mai multe cazuri, materialele întrebuinţate sunt neclasificate, dar asocierea lor cu un loc cu destinaţie specială conduce la clasificare prin asociere cu locul respectiv. Iată de ce publicarea listei materialelor neclasificate, în acest caz, poate să conducă la elemente de legătură cu utilizare clasificată.

Daţi exemple de informaţii (necesar a fi) clasificate prin asociere, din activitatea organiţaiilor cunoscute de dvs.

## 2.5 Clasificarea compilărilor de informaţii

Aşa cum am menţionat anterior, informaţiilor li se dă o clasificare pe linia securităţii atunci când dezvăluirea lor neautorizată poate să cauzeze daune de dimensiuni variate securităţii naţionale. Clasificarea informaţiilor conduce la înregistrarea unor costuri specifice inevitabile, motiv pentru care este necesară o atenţie deosebită asupra informaţiilor care trebuie neapărat să fie clasificate pentru a li se asigura protecţia şi pentru a fi ascunse potenţialilor adversari. Şi totuşi, aşa cum sunt informaţii ce devin clasificate în urma asocierii, există şi informaţii neclasificate care, prin compilare, trebuie să fie tratate ca informaţii clasificate. Aceasta nu trebuie să fie o regulă, ci o excepţie. Se pot da ca exemple compilările titlurilor neclasificate sau ale rezumatelor neclasificate ale proiectelor clasificate din cadrul departamentelor de apărare, care determină nevoia clasificării ca urmare a posibilităţii de a fi dezvăluite tendinţele cercetării şi dezvoltării din departamentele de apărare. La rândul lor, aceste tendinţe sunt clasificate, dar,

[3] U.S. Department of Energy – „Identification of Classified Information", *Office of Classification*, December 1991, Chapter IV, Part B, § 3.

prin compilarea titlurilor, a rezumatelor sau a cuprinsurilor proiectelor clasificate, se poate ajunge la aflarea trendurilor respective.

Sunt două motive importante pentru care informaţiile neclasificate nu trebuie să fie clasificate prin compilare. Primul motiv este acela al evitării costurilor suplimentare generate de clasificare. Al doilea motiv este cel al menţinerii credibilităţii programului de clasificare, ca aspect important al succesului politicii de clasificare.

Multitudinea punctelor de vedere referitoare la clasificarea compilării informaţiilor neclasificate provine probabil din ambiguitatea cuvântului compilare. Unele dintre dispute ar putea să dispară dacă ar fi definită corect compilarea. Federaţia Oamenilor de Ştiinţă Americani defineşte compilarea ca pe o ordonare a materialelor preexistente (fapte, statistici ş.a.) colectate din mai multe surse într-un singur document. În acest sens, se consideră că sunt două tipuri principale de compilări:

1. compilări care nu adaugă o valoare substanţială (informaţie) compilatorului;
2. compilări care adaugă o valoare substanţială compilatorului.

În legătură cu această clasificare, este de făcut menţiunea că nu se aplică aceleaşi reguli tipurilor descrise anterior.

Daţi exemple de informaţii (necesar a fi) clasificate prin compilare, din activitatea organizaţiilor cunoscute de dvs.

## 2.6 Declasificarea şi degradarea informaţiilor clasificate

Atunci când se efectuează clasificarea unor informaţii se iau în calcul anumite cerinţe de îndeplinit. Când, din diferite cauze, se schimbă circumstanţele, firesc, şi cerinţele îndeplinite iniţial se modifică, situaţie în care informaţiile clasificate se declasifică sau trec pe un nivel inferior de clasificare.

*Declasificarea informaţiilor* se efectuează de către reprezentanţi ai guvernului, cărora le revine misiunea de declasificare. Trebuie remarcat faptul că este o diferenţă între declasificarea informaţiilor şi declasificarea documentelor sau materialelor. Ultima categorie poate fi efectuată şi de către contractorii guvernamentali.

*A degrada informaţiile clasificate* înseamnă reducerea nivelului clasificării. În acest mod informaţiile strict secrete pot fi degradate la nivelul secret sau confidenţial. Informaţiile secrete pot fi degradate în informaţii confidenţiale, iar cele confidenţiale nu pot fi degradate, ci pot fi doar declasificate sau, dacă este cazul, ridicate pe un nivel superior.

Termenul de degradare provine din sistemul britanic de clasificare a sistemelor informaţionale. Britanicii vorbesc despre gradarea informaţiilor şi nu despre clasificarea lor, atunci când se referă la ceea ce americanii numesc clasificarea informaţiilor. Ulterior, după primul război mondial, şi americanii au preluat termenul de degradare (*down-grading*), preluând sistemele folosite foarte mult de către britanici şi francezi.

De regulă, degradarea se efectuează de către persoanele care au clasificat iniţial informaţiile, de către succesorii acestora, şefii lor sau de către alţi oficiali delegaţi cu o astfel de autorizare, în scris, de către şefii agenţiei sau de către responsabilii pe această linie.

- Daţi exemple de declasificări de informaţii.
- Daţi exemple de informaţii supuse procesului de degradare (downgrading).

## 2.7 Principiile clasificării informaţiilor şi legea secretului comercial

Se spune că, în lumea afacerilor, organizaţiile îşi protejează informaţiile care le oferă avantaje în faţa concurenţilor, aşa cum guvernele îşi protejează informaţiile care le conferă avantaje în confruntarea cu adversarii lor. Unul dintre cele mai bine păstrate secrete ale zilelor noastre este secretul comercial, aşa cum este reţeta de fabricaţie pentru Coca-Cola Classic®. „Secretele de stat" probabil că au însoţit formarea primelor „state", în timp ce „secretele comerciale" au fost cele mai importante averi ale primelor afaceri. Ocazional, secretele de stat şi secretele comerciale erau identice. De exemplu, în China, pentru aproximativ 3000 de ani, familia regală a garantat îndeaproape, ca pe un secret de stat, metodele de producere a mătăsii, un produs foarte important al comerţului exterior al Chinei cu alte ţări. Abia în secolul VI d.C., cu ajutorul a doi călugări persani, ouăle viermilor de mătase şi seminţele dudului au părăsit China. Disperată, China a încercat să producă derută în rândul celor ce intenţionau să dezvolte industria mătăsii, afirmând că mătasea se obţine prin expunerea lânii la soare, stropirea ei cu apă şi apoi se efectuau unele combinaţii pentru a rezulta produsul finit, mătasea.

Există o mulţime de asemănări între clasificarea şi protejarea informaţiilor de apărare naţională şi de relaţii internaţionale de către guverne, pe de o parte, şi protecţia secretelor comerciale de către companii, pe de altă parte. În ambele ipostaze, informaţia protejată este atât de importantă încât ajungerea ei în posesia adversarilor (duşman/concurent) poate să aibă efecte negative asupra intereselor majore (securitatea naţională/profitul) ale protectorului. Atât secretele comerciale, cât şi informaţiile clasificate necesită o vigilenţă continuă pentru asigurarea protecţiei împotriva dezvăluirilor neautorizate. De asemenea, ambele pot să-şi piardă statutul de secrete odată cu trecerea timpului. Regula secretului comercial, care spune că „ceea ce a devenit proprietate publică nu poate fi redenumit ca fiind secret", are echivalentul ei în domeniul clasificării, prin faptul că informaţiile declasificate sau făcute publice pe cale oficială nu mai pot fi reclasificate.

Unele secrete comerciale, cum sunt formulele chimice sau cunoştinţele despre anumite procese de fabricaţie, sunt comparabile cu informaţiile ştiinţifice şi tehnice clasificate. Alte secrete comerciale, cum este cazul listei clienţilor, sunt asemănătoare informaţiilor subiective clasificate.

Informaţiile despre un nou produs comercial sunt păstrate ca secrete ale unei firme pentru a avea prioritatea lansării pe piaţă şi a păstrării unor avantaje în faţa concurenţilor. Identic, informaţiile despre conceperea şi realizarea unei noi arme sunt considerate secrete naţionale pentru a-i oferi ţării deţinătoare avantaje majore în faţa adversarilor săi.

Spionajul, mult timp fiind doar o practică a guvernelor, are corespondentul său în lumea afacerilor, prin spionajul industrial.

Protecţia legală, permisă atât de secretele comerciale, cât şi de secretele de stat, are rădăcinile în dreptul comun.

De regulă, guvernele consemnează trei niveluri ale clasificării (confidenţial, secret şi strict secret). S-a sugerat ca şi în lumea afacerilor, unde se apelează la secretele comerciale, să fie stabilite două sau trei grade (niveluri) de importanţă pentru acele secrete. Au existat diferite propuneri, dintre care una sugera ca informaţiile, ce trebuie să fie protejate de către companii, să fie grupate astfel: *secrete comerciale* şi *know-how* – acesta fiind o informaţie valoroasă dar probabil nu va asigura protecţia secretului comercial.

Legea secretului comercial nu protejează pe deţinătorul secretului împotriva unor descoperiri normale, prin invenţii sau inovaţii, ale secretului comercial respectiv. Din acest punct de vedere, legea secretului comercial se aseamănă cu politicile de clasificare, pentru că obiectivele clasificării nu sunt de a împiedica adversarul să obţină aceleaşi informaţii prin eforturi independente sau prin ingineria inversă, ci de a evita sprijinirea adversarilor să

achiziţioneze acele informaţii. Prin inginerie inversă se porneşte de la un produs şi se încearcă a se afla cum a fost realizat.

În general, se poate spune că există o puternică asemănare între caracteristicile informaţiilor protejate sub forma secretului comercial şi caracteristicile informaţiilor protejate ca informaţii clasificate. Literatura de specialitate[4] enumeră şase elemente sau factori care au fost propuşi să fie utilizaţi atunci când se încearcă a se stabili dacă informaţiile reprezintă sau nu un secret comercial, astfel:

1. gradul în care informaţia este cunoscută în afara organizaţiei;
2. gradul în care este cunoscută de angajaţi şi alte persoane implicate în afacere;
3. dimensiunea măsurilor luate pentru a se garanta secretul informaţiilor;
4. valoarea informaţiilor pentru proprietar şi pentru competitorii lui;
5. mărimea efortului sau banii cheltuiţi pentru obţinerea acelor informaţii;
6. uşurinţa sau dificultatea cu care informaţia poate fi achiziţionată sau multiplicată de către alţii.

Justificaţi, cu exemple, importanţa secretelor comerciale în activitatea firmelor.

## 2.8 Principiile protejării informaţiilor speciale

Date fiind clasificările anterioare, pe linia protejării informaţiilor speciale pot fi enunţate 10 principii:

**Principiul delimitării autorizării**

Repartizarea informaţiilor pe tipuri va consta într-o grupare ierarhică plus suma compartimentărilor în care se regăseşte informaţia (de exemplu, o informaţie poate fi clasată pe principiul ierarhic în categoria *strict secretă* şi, în acelaşi timp, să figureze în compartimentările *criptare* şi *comunicare secretă*). Autorizarea unei persoane sau prelucrări (când executant va fi calculatorul) presupune stabilirea sferei de exercitare a funcţiei şi ea constă din autorizarea pe criteriul ierarhic al persoanei plus suma autorizărilor compartimentărilor persoanelor din subordinea sa.

**Principiul securităţii simple**

Nici o persoană sau proces, dintr-o anumită subordonare, nu trebuie să vadă informaţiile unei categorii care depăşeşete autorizarea sa. Într-o formă scurtă, principiul poate fi formulat: Tu, categoric, nu trebuie să le ştii!

**Principiul stea**

Nici o persoană sau proces nu va scrie ceva pe obiectele dintr-o categorie inferioară celei la care persoana sau procesul are acces.

**Primul principiu al integrităţii**

Nici un program pentru calculator nu va accepta informaţii de la un program inferior lui, pe linia privilegiilor.



---

[4] Gros, A.Y. – *What is "Trade Secret" So As to Render Actionable Under State Law Its Use or Disclosure by Former Employee*, 59 ALR 4th, 641, 652 (1988), p. 652.

Gross combină elementele 1 şi 6, 2 şi 3, 4 şi 5, reieşind cei 6 factori din *Restatment of the Law of* Torts

**Al doilea principiu al integrităţii**

Nici un program pentru calculator nu va scrie ceva într-un program superior lui, prin prisma privilegiilor.

**Principiul etichetării**

Fiecare purtător de informaţii va fi etichetat clar cu categoria informaţiilor conţinute, în format accesibil omului şi în format sesizabil de către echipamentele periferice.

**Principiul clarificării**

Nici o persoană sau procedură nu va schimba categoriile existente ale informaţiilor şi nici autorizările existente, conform unor proceduri în vigoare.

**Principiul inaccesibilităţii**

Nici o informaţie nu va fi lăsată la dispoziţia altor persoane sau procese, cu excepţia celor consemnate prin norme interne.

**Principiul verificabilităţii**

Pentru toate activităţile semnificative pe linia securităţii (deschiderea fişierelor, ştergerea obiectelor, transmiterea în altă parte) se vor crea înregistrări imposibil de şters, cu rolul facilitării verificării sistemului.

**Principiul încrederii în software**

Cât timp nici un calculator nu poate controla perfect respectarea principiilor anterioare, dar, totuşi, efectuează activităţi utile, încrederea în software va permite apariţia unor excepţii de la regulă, dacă este cazul.

Exemplificaţi modul în care principiile enunţate mai sus se aplică într-o organizaţie cunoscută de dvs.

## 2.9 Protejarea suporturilor informaţionale

Întrucât calculatoarele generează ieşiri care, potenţial, sunt mult mai valoroase decât intrările din fişierele ce le-au generat, obligaţia pe linia încadrării informaţiilor în diverse categorii revine persoanelor care autorizează prelucrarea şi directorului centrului de prelucrare automată a datelor (p.a.d.) sau delegatului acestuia.

Toate suporturile care conţin informaţii obţinute din prelucrarea automată a datelor trebuie să fie catalogate ca documente ale prelucrării automate a datelor. Ele sunt discuri de orice tip, benzi magnetice, tamburi magnetici, pachete de discuri, dischete, registre, circuite electronice ş.a. Tratamentul lor trebuie să fie similar documentelor ce conţineau aceleaşi date în condiţiile prelucrării tradiţionale.

Toate materialele intermediare şi informaţiile obţinute în cursul prelucrării automate a datelor trebuie să fie considerate ca materiale auxiliare pentru prelucrarea automată a datelor. Ele includ materialele anulate, de genul benzilor şi discurilor magnetice, hârtiei de imprimantă, benzilor tuşate ş.a. Aceste materiale auxiliare trebuie să fie supuse clasificărilor în funcţie de informaţiile ce le conţin.

Ştergerea informaţiilor clasificate este o operaţiune căreia trebuie să i se acorde o importanţă deosebită. Suporturile de prelucrare automată a datelor care posedă caracteristici de remanenţă după ştergere, cum sunt suporturile magnetice, trebuie să fie tratate cu mare atenţie din faza aprobării ştergerii lor. După ştergere ele pot fi folosite pentru păstrarea unor informaţii cel puţin la fel de importante ca şi precedentele.

Fiecare persoană care autorizează operaţiuni de prelucrare automată a datelor trebuie să verifice dacă există o fişă de securitate, care să conţină categoria persoanei executante, categoria informaţiilor prelucrate şi instrucţiuni privind statutul informaţiilor rezultate. De asemenea, vor fi consemnate date privind durata prelucrării, timpul de utilizare a componentelor bazei de date, generaţiile reţinute (fiu, tată, bunic), astfel încât să poată fi reconstituită baza de date în caz de avarii, precum şi alte cerinţe pe linia păstrării copiilor de siguranţă.

Documentele aflate sub regimul controlului special trebuie să fie numerotate şi înregistrate pentru a se putea şti ce s-a folosit sau ce s-a văzut din ele.

Toate documentele obţinute prin prelucrarea automată a datelor, cum este hârtia de imprimantă, trebuie să fie marcate, astfel încât să fie vizibilă categoria din care fac parte, prin plasarea marcajului în colţul din dreapta sus, precum şi în partea inferioară a fiecărei pagini. În plus, se va consemna numărul de exemplare al fiecărui document.

## 2.9.1 Marcarea materialelor cu regim special

Sub accepţiunea prelucrării automate a datelor, un ecran cu informaţii este tratat ca o pagină de document, şi încadrarea într-o categorie sau alta se va face pe o linie distinctă a acestuia.

*Marcarea în cod maşină* trebuie să se efectueze prin coduri sesizabile de echipamente, astfel încât să rezulte foarte clar din ce categorie fac parte informaţiile prelucrate şi la ce operaţiuni pot fi supuse. Codul trebuie să fie una dintre primele informaţii ce vor fi date sistemului, astfel încât să nu fie posibilă accesarea altor date înainte de a se şti statutul lor. Codul poate fi ultimul caracter al numelui fişierului, iar caracterul utilizat să aibă valorile:

**S** = special, **C** = confidenţial, **P** = privat, **R** = cu restricţii, **N** = neclasificate.

Exemplu de nume de fişier: SALARII**C** – ultimul caracter, C, arată că sunt informaţii confidenţiale.

*Marcarea fizică* se referă la toate suporturile supuse prelucrării automate a datelor. Marcajul trebuie să reziste în timp şi să nu fie afectat sau să afecteze prelucrarea automată a datelor. Marcarea se poate face chiar pe suport sau pe caseta, rola sau plicul ce-l conţine. Suporturile reutilizabile trebuie să fie marcate cu etichete adezive sau creioane ce pot fi şterse ulterior.

*Marcarea suporturilor de hârtie*, cum au fost cartelele şi benzile perforate, au marcajul prin culori distincte: portocaliu = informaţii care necesită control special, roz = confidenţiale, verde = private, galben = cu restricţii, albe = comune. Dacă numai o parte a benzii sau pachetului conţine informaţii protejate, tot volumul va căpăta acelaşi statut.

*Marcarea cutiilor şi a carcaselor* este necesară atunci când suporturile de memorare sunt păstrate în astfel de condiţii, caz în care se impune etichetarea neambiguă a acestora, precum şi scrierea fişierelor conţinute de suporturile din interior. Se recomandă etichetele color adezive.

*Marcarea benzilor magnetice* se efectuează cu etichete lipite chiar pe bandă, fără să afecteze prelucrarea datelor.

*Marcarea pachetelor de discuri* se realizează cu carioca în centrul acestora.

*Marcarea microfilmelor* se face pe prima imagine cadru sau pe cutie, cu carioca. La fel se procedează cu microfişele.

## 2.9.2 Păstrarea şi distrugerea materialelor speciale

Materialele care păstrează date supuse prelucrării automate a datelor şi cele auxiliare se păstrează în camere speciale.

Documentele ce conţin informaţii aflate sub un control special se păstrează în seifuri sau în locuri protejate prin sisteme speciale.

Operaţiunea de distrugere trebuie să urmeze proceduri speciale. Cea mai bună cale de distrugere este *arderea*, folosită, de regulă, pentru gunoaiele informatice adunate în pungi speciale. Înaintea arderii ele trebuie păstrate în locuri cu o astfel de destinaţie. La operaţiune vor participa două persoane, care sunt obligate să ţină un registru special pentru consemnarea a ceea ce se supune arderii. Cenuşa trebuie să fie împrăştiată pentru distrugerea oricărei posibilităţi de reconstituire a datelor conţinute. La fel pot fi distruse şi alte materiale, cum sunt pachetele de discuri magnetice, după ce se recuperează anumite piese.

*Transformarea în pastă* este posibilă numai pentru reziduurile de hârtie, nu şi pentru banda magnetică, microfilm sau benzi tuşate.

*Fărâmiţarea* se aplică resturilor de hârtie, indigo, bandă magnetică, microfilm, dar o astfel de operaţiune trebuie să fie a treia şi ca utilizare. Înaintea acestei operaţiuni, în cazul benzii magnetice, în primul rând, trebuie tăiată întreaga rolă. Standardele internaţionale prevăd ca particulele rezultate din această operaţiune să nu fie mai mari de 1/32 inch. De regulă, fărâmiţarea este recomandată înaintea arderii.

O atenţie specială se va acorda suporturilor magnetice întrucât ele se pot refolosi. Dacă aceasta se întâmplă în aceeaşi unitate, noul posesor trebuie să aibă cel puţin aceeaşi autorizare pe linia accesului la informaţii ca şi precedentul. Pentru un plus de siguranţă se recomandă completarea cu zerouri a vechiului suport, sau cu cifre aleatoare. Dacă se utilizează în afara unităţii, vor fi luate măsuri suplimentare, dar oricum nu se va declara utilizarea avută anterior.

Pentru ştergerea benzilor magnetice există aparatură specială de demagnetizare, realizată de Ampex, Hewlett-Packard sau Consolidated Engineering Corp.

Discurile magnetice sunt şterse prin curent alternativ sau continuu, dacă sistemul de prelucrare automată a datelor permite o astfel de operaţiune, după care se efectuează scrierea de trei ori cu cifre 1 şi 0, şi încă o dată cu un singur caracter alfabetic.

## 2.10 Clasificarea informaţiilor organizaţiilor

La nivelul unei organizaţii, pe un plan corespunzător, ar trebui văzute la fel lucrurile ca şi la nivel naţional, încadrându-se informaţiile în mai multe categorii, cu protecţii diferite, după cum urmează:

*Informaţiile care necesită un control special* sunt cele cunoscute la nivel naţional ca fiind *strict secrete*. La nivelul firmei ele se numesc *speciale*, notate cu **S**. Aici pot fi incluse informaţiile şi materialele a căror compromitere ar duce la pierderea a 10 procente din profitul brut anual.

*Informaţiile confidenţiale la nivel de unitate*, notate cu **C**, corespund celor *secrete* la nivel naţional, şi se atribuie acest calificativ informaţiilor şi materialelor a căror compromitere ar duce la pierderea unui procent din profitul net anual.

*Informaţiile private*, asemănătoare celor *confidenţiale* de la nivel naţional, notate cu **P**, cuprind informaţiile şi materialele a căror compromitere poate prejudicia statutul unei persoane din unitate sau al corporaţiei.

*Informaţiile de uz intern* sunt acelea ce nu fac parte din categoriile anterioare şi, pentru că au restricţii în utilizare, se vor nota cu litera **R**.

*Informaţiile publice* au un regim mult diferit de cele asemănătoare de la nivel guvernamental, fiind totuşi recunoscute prin statutul de neclasificate, notate cu **N**.

La nivel guvernamental, orice informaţie neîncadrată într-una din categoriile speciale, sub incidenţa legii accesului liber la informaţiile publice, poate fi publicată de orice organ de presă scrisă, video sau vorbită, sub motivaţia că *tot ceea ce nu este interzis este permis*.

La nivel privat, se înregistrează o reţinere mai mare pe linia informaţiilor publice şi numai documentele cu menţiunea „pentru public” pot fi accesibile tuturor. De fapt, deviza în acest caz este *tot ceea ce nu este permis este interzis*. Totuşi, un tratament special îl au informaţiile solicitate de organismele guvernamentale de la unităţile private.

La nivelul firmelor, deseori şefii compartimentelor uzează de sistemul consemnării exprese, sub forma unor subcategorii de genul: „Numai pentru domnul/doamna ...”, „Numai pentru compartimentul ...”.

Şi în acest caz, detaliile din legislaţia românească se află în capitolul 10.

### 2.10.1 Criterii de clasificare a informaţiilor

După amplele discuţii din ţara noastră privind legile care reglementează informaţiile publice şi pe cele clasificate, iată câteva criterii generale de clasificare a acestora la nivelul organizaţiilor.

*Valoarea*. Îndeosebi în sectorul privat, valoarea constituie criteriul principal de clasificare. Dacă o informaţie este valoroasă pentru o organizaţie sau pentru concurenţii ei, atunci ea trebuie să fie clasificată.

În domeniul militar s-a pornit de la valoarea inestimabilă a vieţilor omeneşti pierdute prin dezvăluirea informaţiilor.

La nivel naţional, valoarea informaţiilor este dată de nivelul prejudiciilor aduse unei ţări prin dezvăluirea lor.

*Vârsta*. În clasificarea informaţiilor, în funcţie de natura lor, vârsta conduce la stabilirea unei valori diferenţiate. Cu cât vechimea e mai mare, cu atât informaţiile pierd din valoare, deci pierd din interesul pentru ele. De regulă, în domeniul apărării, informaţiile clasificate se declasifică după un anumit număr de ani.

*Uzura morală*. Ca şi mijloacele fixe, atunci când informaţiile sunt înlocuite de altele noi sau când în organizaţie s-au produs schimbări radicale, vechea clasificare devine perimată şi va fi înlocuită cu alta.

*Asocierea cu persoanele* are influenţă în procesul de clasificare în funcţie de importanţa persoanelor care reglementează regimul datelor personale.

### 2.10.2 Procedurile de clasificare a informaţiilor

Atunci când se vorbeşte despre un sistem de clasificare, trebuie urmăriţi paşii de parcurs, după o anumită ordine de prioritate, astfel:

1. identificarea administratorului/custodelui;
2. specificarea criteriilor după care vor fi clasificate şi etichetate informaţiile;
3. clasificarea datelor după proprietar, care devine subiect supus auditării efectuate de un superior;
4. precizarea şi documentarea oricăror excepţii de la politicile de securitate;
5. precizarea controalelor aplicate fiecărui nivel de clasificare;
6. specificarea procedurilor de declasificare a informaţiilor sau pentru transferarea custodiei unei alte entităţi;
7. crearea unui program de conştientizare la nivel de organizaţie despre controalele pe linia clasificării informaţiilor.

### 2.10.3 Roluri şi responsabilităţi în procesul de clasificare a informaţiilor

Principalele roluri în procesul de clasificare le au proprietarul, utilizatorul sau custodele datelor clasificate.

*Proprietarul informaţiilor* poate fi administratorul sau directorul unei organizaţii. O astfel de persoană răspunde de averile informaţionale încredinţate. Spre deosebire de custode, proprietarul are responsabilitatea finală a protecţiei datelor şi răspunde în faţa legii în cazul neachitării de această obligaţie. Cu toate acestea, tendinţa din zilele noastre pe planul protecţiei datelor este de deplasare în afara unităţii, de externalizare, prin semnarea actelor de custodie.

Printre responsabilităţile unui proprietar se află:

- întreprinde demersuri pentru stabilirea nivelului de clasificare a informaţiilor, care înseamnă, de fapt, cerinţele organizaţiei de protejare a acestora;
- efectuează verificări periodice ale clasificărilor existente, în vederea adaptării la cerinţele organizaţiei;
- deleagă responsabilitatea protejării datelor către un custode specializat şi autorizat.

*Custodele informaţiilor* este cel ce prestează un serviciu externalizat organizaţiei, delegându-i-se responsabilităţile pe linia protejării informaţiilor. Acest rol este îndeplinit de specialişti în tehnologii informaţionale. Dintre obligaţiile sale, amintim:

- efectuează copii de siguranţă periodice şi teste de rutină a validităţii datelor;
- efectuează restaurări de date din copiile de siguranţă, când este cazul;
- întreţine datele înregistrate, în concordanţă cu politicile de clasificare a informaţiilor.

Deseori, custodele are şi obligaţia alcătuirii schemei de clasificare a informaţiilor, preluând aceste prerogative de la proprietarul lor.

*Utilizatorul*. În schema clasificării informaţiilor, un utilizator final este considerat orice persoană – operator, angajat, persoană din afară – care, prin prisma locului de muncă, foloseşte informaţii. El este considerat consumator de date care are nevoie, zilnic, să acceseze informaţii pentru a-şi duce la îndeplinire obligaţiile de serviciu ce îi revin.

În ceea ce-i priveşte pe utilizatori, aceştia au obligaţiile:

- de a urma întocmai procedurile de funcţionare, definite prin politicile de securitate ale organizaţiei, şi să respecte normele publicate privind utilizarea informaţiilor;
- să acorde toată atenţia menţinerii securităţii informaţiilor în timpul activităţii prestate, după cum se stipulează în politicile de utilizare a informaţiilor emise de organizaţia proprietară. Ei trebuie să asigure protejarea împotriva accesului neautorizat la informaţiile clasificate;
- să folosească resursele informaţionale ale firmei numai în scopul urmărit de aceasta, nu şi în scop personal.



Completaţi următorul tabel:

| Suport informaţional | Nivel de clasificare | Mod de marcare | Mod de păstrare | Mod de distrugere | Responsabil cu suportul |
|---|---|---|---|---|---|
| Raport listat cu contul de profit şi pierdere al firmei X pe 2010 | | | | | |
| Dosarele medicale ale personalului firmei X | | | | | |
| DVD cu copia de siguranţă a bazei de date la sf. lui februarie 2011 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| CD cu procesul tehnologic de obţinere a principalului produs al firmei | | | | | |

## Rezumat

*Clasificarea* înseamnă etichetări crescătoare ale documentelor sau informaţiilor, de la cel mai de jos nivel, unde se situează informaţiile deschise (*open*) sau neclasificate (*unclassified*), la cele confidenţiale, urcând spre informaţii secrete şi strict secrete (*top secret*). În domeniul militar, informaţiile care prin compromitere pot *costa vieţi umane* sunt marcate „secrete", în timp ce informaţiile a căror compromitere costă *pierderea multor vieţi umane* sunt definite „top secret" (strict secrete).

Se practică *două strategii de bază* pe linia securităţii naţionale:

1. Tot ceea ce nu este interzis este permis;

2. Tot ceea ce nu este permis este interzis.

Se apelează la *două tactici de implementare a strategiei* fundamentale privind protejarea informaţiilor deosebite: *controlul discreţionar al accesului* şi *controlul legal al accesului.*

Guvernele împart informaţiile în două mari tipuri: *informaţii subiective* şi *informaţii obiective*. Anterior a operat o altă clasificare: *informaţii „operaţionale"* şi *informaţii „ştiinţifice"*. Unii autori au menţionat şi un al treilea tip de informaţii clasificate de guverne – *informaţii „tehnice"*.

În vederea clasificării informaţiilor se parcurg *trei etape* distincte: stabilirea nevoii de clasificare; determinarea nivelurilor clasificării; determinarea duratei clasificării.

În *sistemul american de clasificare a informaţiilor* există trei niveluri de clasificare: top secret (strict secret), secret şi confidenţial. Informaţiile neclasificate constituie o altă categorie. În România, informaţiile clasificate din clasa secretelor de stat sunt încadrate tot în trei niveluri, astfel: strict secrete de importanţă deosebită, strict secrete şi secrete.

Informaţiile ce nu sunt clasificate, uneori, sunt supuse clasificării ca urmare a asocierii lor cu alte informaţii care, implicit sau explicit, conduc la dezvăluirea altor informaţii care sunt clasificate. Clasificarea asocierilor este referită ca o *clasificare prin context*, ce nu trebuie să fie confundată cu clasificarea prin compilare.

Există şi informaţii neclasificate care, prin compilare, trebuie să fie tratate ca informaţii clasificate. Aceasta nu trebuie să fie o regulă, ci o excepţie. se consideră că sunt două tipuri principale de compilări: compilări care nu adaugă o valoare substanţială (informaţie) compilatorului; compilări care adaugă o valoare substanţială compilatorului.

Atunci când se efectuează clasificarea unor informaţii se iau în calcul anumite cerinţe de îndeplinit. Când, din diferite cauze, se schimbă circumstanţele, firesc, şi cerinţele îndeplinite iniţial se modifică, situaţie în care informaţiile clasificate se *declasifică* sau trec pe un nivel inferior de clasificare (*degradarea informaţiilor*).

S-a sugerat ca şi în lumea afacerilor, unde se apelează la secretele comerciale, să fie stabilite două sau trei grade (niveluri) de importanţă pentru acele secrete. Au existat diferite propuneri, dintre care una sugera ca informaţiile, ce trebuie să fie protejate de către companii, să fie grupate astfel: *secrete comerciale* şi *know-how* – acesta fiind o informaţie valoroasă dar probabil nu va asigura protecţia secretului comercial. Au fost specificaţi şase factori care au fost propuşi să fie utilizaţi atunci când se încearcă a se stabili dacă informaţiile reprezintă sau nu un secret comercial.

Pe linia protejării informaţiilor speciale pot fi enunţate *10 principii*: delimitării autorizării, securităţii simple, stea, al integrităţii I, al integrităţii II, etichetării, clarificării, inaccesibilităţii, verificabilităţii, încrederii în software.

Toate suporturile care conţin informaţii obţinute din prelucrarea automată a datelor trebuie să fie catalogate ca documente ale prelucrării automate a datelor. Tratamentul lor trebuie să fie similar

documentelor ce conţineau aceleaşi date în condiţiile prelucrării tradiţionale. Măsurile de protecţie sunt: marcarea materialelor cu regim special, păstrarea şi distrugerea materialelor speciale.

La nivelul unei organizaţii ar trebui văzute la fel lucrurile ca şi la nivel naţional, încadrându-se informaţiile în mai multe categorii, cu protecţii diferite: i*nformaţiile care necesită un control special*, *informaţiile confidenţiale la nivel de unitate*, *informaţiile private*, *informaţiile de uz intern*, *informaţiile publice*. Criteriile generale de clasificare a informaţiilor la nivelul organizaţiilor sunt: valoarea, vârsta, uzura morală. Rolul şi responsabilităţile procesului de clasificare revin proprietarului, utilizatorului sau custodelui.

CAPITOLUL III

# Controlul accesului în sistemele informaţionale

După fatidica zi de 11 septembrie 2001, sensul controlului accesului în sistem s-a schimbat radical, atât prin prisma *mijloacelor de exercitare*, cât şi a *domeniilor de aplicare*. În privinţa mijloacelor, dominantă a fost discuţia de la sfârşitul anilor '90, dacă trebuie să se introducă sau nu sistemele de identificare biometrică a persoanelor, făcându-se asocierea cu luarea amprentelor digitale doar pentru elucidarea unor cazuri criminale. Opoziţia cea mai puternică venea din partea sistemului bancar, dar nu numai. Alte instrumente păreau incomode sau periculoase şi, ca atare, erau refuzate în serie. După data susmenţionată lucrurile s-au schimbat radical, în privinţa identificării biometrice – tendinţă ce va fi demonstrată într-un paragraf distinct al prezentului capitol. Domeniile de aplicare s-au extins, totul venind din convingerea intimă a proprietarilor şi administratorilor de sisteme, văzându-se astfel alte modalităţi de verificare a persoanelor ce doresc accesul în mai toate instituţiile prezidenţiale, guvernamentale şi altele de tip public sau privat, iar aeroporturile şi-au extins zonele supuse unei atenţii speciale.

Nici sistemele informaţionale nu au rămas aceleaşi. Doar simpla trimitere la ceea ce a făcut Microsoft pe linia securizării este destul de elocventă, căci aproape orice mişcare a personalului este sub control, apelându-se la dependenţa totală a acestuia de carduri speciale.

În acest spirit, dorim ca, la finalul parcurgerii capitolului de faţă, cititorii să:

- dobândească suficiente cunoştinţe pentru stabilirea tipurilor de control al accesului adecvate pentru o anumită organizaţie şi pentru implementarea acestora;
- cunoască modele de control şi a modalităţile de combinare a lor;
- deţină suficiente informaţii pentru stabilirea modalităţilor de identificare şi autentificare a persoanelor necesare unei anumite organizaţii.

## 3.1 Tipuri de control al accesului în sistem

De regulă, controalele sunt introduse pentru diminuarea riscurilor la care sunt expuse sistemele şi pentru reducerea potenţialelor pierderi. Controalele pot fi *preventive, detective* sau *corective*[1].

Controalele *preventive*, după cum sugerează şi numele lor, au ca scop preîntâmpinarea apariţiei unor incidente în sistem; cele *detective* vizează descoperirea unor apariţii ciudate în sistem, iar controalele *corective* sunt folosite pentru readucerea la normalitate a sistemului după anumite incidente la care a fost expus.

Ca să poată fi atinse obiectivele enumerate, controalele pot fi *administrative, logice sau tehnice* şi *fizice*.

*Controalele administrative* sunt exercitate prin politici şi proceduri, instruire cu scop de conştientizare, verificări generale, verificări la locurile de muncă, verificarea pe timpul concediilor şi o supraveghere exigentă.

*Controalele logice sau tehnice* cuprind restricţiile de accesare a sistemului şi măsurile prin care se asigură protecţia informaţiilor. Din această categorie fac parte sistemele de criptare, cardurile inteligente, listele de control al accesului şi protocoalele de transmisie.

*Controalele fizice* încorporează, în general, gărzile de protecţie şi pază, securitatea clădirilor, cum sunt: sistemele de încuiere a uşilor, securizarea camerelor cu servere şi laptop-uri,

[1] Krutz, R.L., Vines, R.D. – *The CISSP Prep Guide – Mastering the Ten Domains of Computer Security*, Wiley Computer Publishing, John Wiley & Sons, Inc., New York, 2001, pp. 31-50.

protecţia cablurilor, separarea atribuţiilor de serviciu, precum şi realizarea copiilor de siguranţă a fişierelor.

Controalele vizează responsabilizarea persoanelor care accesează informaţii sensibile. Responsabilizarea este înfăptuită prin mecanisme de control al accesului care necesită, la rândul lor, exercitarea funcţiilor de *identificare, autentificare* şi *auditare*. Controalele trebuie să fie în deplină concordanţă cu politica de securitate a organizaţiei, iar *procedurile de asigurare* au scopul de a demonstra că prin mecanismele de control se implementează corect politicile de securitate pentru întregul ciclu de viaţă al sistemului informaţional.

Prin combinarea controlului preventiv şi detectiv cu mijloacele celorlalte tipuri de control – administrativ, tehnic (logic) şi fizic – se obţin următoarele perechi:

- preventiv/administrativ;
- preventiv/tehnic;
- preventiv/fizic;
- detectiv/administrativ;
- detectiv/tehnic;
- detectiv/fizic.

Schematic, aceste perechi sunt redate în figura 3.1.

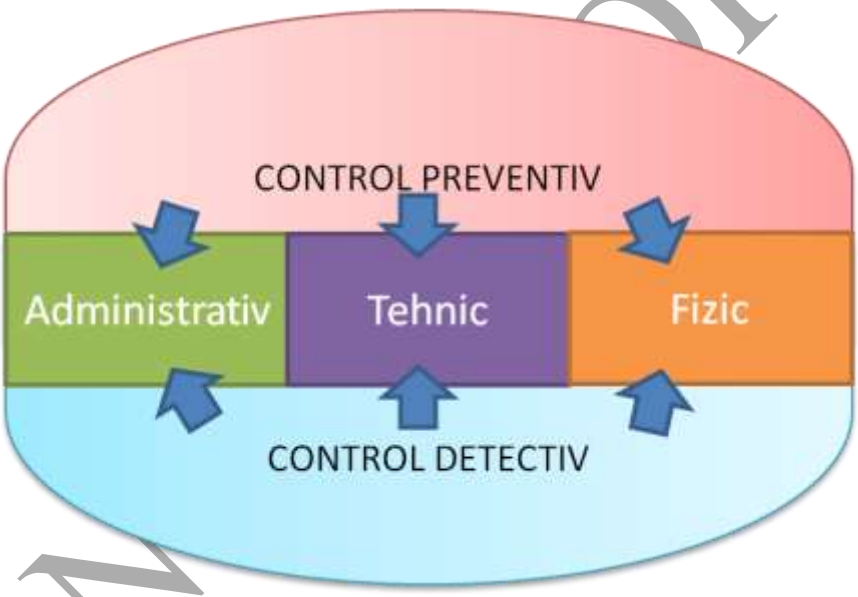


**Fig. 3.1 Perechile formelor de control**

**Controlul preventiv/administrativ**

În această variantă, accentul se pune pe resposabilităţile administrative care contribuie la atingerea obiectivelor controlului accesului. Aceste mecanisme cuprind politicile şi procedurile organizaţionale, verificările de fond înainte de angajare, practicile de încetare a contractului de muncă în condiţii normale şi anormale, planificarea plecărilor în concediu, etichetarea sau marcarea materialelor speciale, supravegherea mai exigentă, cursuri de instruire în scopul conştientizării importanţei securităţii, conştientizarea modului de comportare, precum şi procedurile de semnare a contractului în vederea obţinerii accesului la sistemul informaţional şi la reţea.

**Controlul preventiv/tehnic**

Împerecherea preventiv-tehnic vizează utilizarea tehnologiilor pentru consolidarea politicilor de control al accesului. Controlul tehnic se mai numeşte şi control logic şi poate fi realizat prin sistemele de operare, prin aplicaţii sau printr-o componentă suplimentară hard/soft. Dintre controalele preventive/tehnice fac parte protocoalele, criptarea, cardurile inteligente, biometria

(cu scopul de autentificare), pachetele software pentru realizarea controlului accesului local sau de la distanţă, parolele, meniurile, softul de scanare a viruşilor ş.a.

**Controlul preventiv/fizic**

În cea mai mare parte, măsurile de control preventiv/fizic sunt de tip intuitiv. Ele vizează restricţionarea accesului fizic în zonele ce conţin informaţii sensibile ale sistemului. Zonele respective sunt definite printr-un aşa-zis *perimetru de securitate*, aflat sub controlul accesului.

În această categorie intră împrejmuirile cu gard, ecusoanele, uşile multiple (după trecerea printr-o uşă, aceasta se blochează automat, iar la următoarea trebuie cunoscut sistemul de deschidere, persoana fiind captivă între două uşi, motiv pentru care se numesc şi *uşi-capcană*), sistemele de intrare pe bază de cartelă magnetică, aparatura biometrică (pentru identificare), servicii de pază, câini de pază, sisteme de controlare a mediului (temperatură, umiditate ş.a.), schiţa clădirii şi a căilor de acces, locurile special amenajate pentru depozitarea suporturilor de informaţii.

**Controlul detectiv/administrativ**

Câteva dintre controalele detective/administrative se suprapun controalelor preventive/administrative pentru că ele pot fi exercitate cu scopul prevenirii posibilelor violări ale politicilor de securitate sau pentru detectarea celor în curs. Din această categorie fac parte procedurile şi politicile de securitate, verificările de fond, planificarea plecărilor în concediu, marcarea sau etichetarea materialelor speciale, o supraveghere mai exigentă, instruiri cu scopul conştientizării importanţei securităţii. În plus, cu scop detectiv/administrativ sunt controalele ce vizează rotirea personalului la locurile de muncă, exercitarea în comun a unor responsabilităţi, precum şi revizuirea înregistrărilor cu scop de auditare.

**Controlul detectiv/tehnic**

Măsurile controlului detectiv/tehnic vizează scoaterea în evidenţă a violării politicii de securitate folosindu-se mijloace tehnice. Aceste măsuri se referă la sistemele de detectare a intruşilor şi la rapoartele privind violările securităţii, generate automat, pe baza informaţiilor colectate cu scopul de a fi probă în auditare. Rapoartele pot evidenţia abaterile de la funcţionarea „normală" sau pot detecta semnături cunoscute ale unor episoade de acces neautorizat.

Datorită importanţei lor, informaţiile folosite în auditare trebuie să fie protejate la cel mai înalt nivel posibil din sistem.

**Controlul detectiv/fizic**

De regulă, aceste controale necesită *intervenţia omului* pentru evaluarea a ceea ce oferă *senzorii* sau *camerele* pentru a stabili dacă există un pericol real pentru sistem. În acest caz, controlul se exercită prin camere video, detectoare termice, de fum, de mişcare.

Analizaţi modalităţile de control al accesului implementate într-o organizaţie cunoscută de dvs., încadrându-le în formele combinate prezentate în subcapitolul anterior. Apreciaţi, în câteva fraze, eficienţa controalelor folosite de organizaţia respectivă.

## 3.2 Identificarea şi autentificarea

În orice sistem de bariere fizice, sistemul de securitate trebuie să discearnă care sunt persoanele autorizate şi care sunt vizitatorii şi alte categorii neautorizate. Autentificarea poate să o facă corpul de pază, alte persoane care se ocupă de controlarea accesului sau sistemele automate investite cu această funcţie.

De regulă, *identificarea şi autentificarea persoanelor* se efectuează prin analiza a patru elemente:

1. *Ceva aflat în posesia persoanei*. De regulă, se posedă lucruri cum sunt: chei, cartele magnetice, cartele speciale, echipamente de identificare personală şi jetoane. Ele permit un prim pas de accesare a sistemului. Există marele pericol al pierderii lor sau de dare spre folosinţă altor persoane.
2. *Ceva care individualizează persoana*. Identificările biometrice sunt o altă variantă de condiţionare a accesului. Ele pot fi: amprentele degetelor, buzelor, semnătura, vocea, forma mâinii, imaginea retinei, venele de pe faţa externă a mâinii, liniile din palmă, imaginea feţei ş.a. Toate aceste tehnici sunt foarte scumpe, în comparaţie cu cele clasice, şi deseori sunt incomode sau neplăcute la utilizare. Există suficiente tehnici eficiente care să fie folosite până când cele enumerate vor fi mai ieftine.
3. *Ceva ce persoana ştie*. O parolă, de exemplu, numai că ea se află la discreţia oamenilor şi, de modul de păstrare a secretului ei sau de uşurinţa cu care poate fi aflată, depinde soarta întregului sistem.
4. *Locul geografic* unde este înregistrat calculatorul.

Metodele de controlare a accesului trebuie să se bazeze pe cel puţin două dintre cele patru căi enumerate; deseori se apelează la combinaţiile cartelă-parolă, cheie-parolă, jeton-parolă. În ultimul timp se recomandă ca în sistemele de protecţie să se folosească tot mai mult un al treilea element, cel biometric.

- Daţi exemple de **2 situaţii** în care **identificarea şi/sau autentificarea** unei persoane se fac folosind **locul geografic în care este înregistrat calculatorul său.** Precizaţi dacă în exemplul dvs. este vorba de identificare, autentificare sau ambele.
- Daţi exemple de **2 situaţii** în care **identificarea şi/sau autentificarea** unei persoane se fac folosind **ceva ce ştie o persoană.** Precizaţi dacă în exemplul dvs. este vorba de identificare, autentificare sau ambele.
- Daţi exemple de **2 situaţii** în care **identificarea şi/sau autentificarea** unei persoane se fac folosind **ceva care individualizează persoana (o trăsătură biometrică).** Precizaţi dacă în exemplul dvs. este vorba de identificare, autentificare sau ambele.
- Daţi exemple de **2 situaţii** în care **identificarea şi/sau autentificarea** unei persoane se fac folosind **ceva aflat în posesia persoanei.** Precizaţi dacă în exemplul dvs. este vorba de identificare, autentificare sau ambele.

## 3.2.1 Principii de bază ale controlului accesului

Ca principiu general, *simpla posesie a unui element de control al accesului nu trebuie să constituie şi proba accesului privilegiat* la informaţiile importante ale firmei, întrucât el poate fi dobândit şi pe căi ilegale sau poate fi contrafăcut.

Un al doilea principiu arată că *atunci când valorile patrimoniale sunt deosebit de importante şi mecanismul de protecţie trebuie să fie pe măsură,* iar persoanele cu drept de acces să fie cât mai puţine, deci de principiul „trebuie să ştie" să beneficieze cât mai puţine persoane.

Al treilea principiu, de regulă aplicat informaţiilor secrete, este acela că *nici unei persoane nu trebuie să i se garanteze accesul permanent, gestiunea sau cunoaşterea informaţiilor secrete numai pe motivul poziţiei ierarhice pe care o deţine*. Este o replică la principiul „trebuie să ştie".

Fiecare centru de prelucrare automată a datelor cu mai mult de 25 angajaţi trebuie să apeleze la sistemul ecusoanelor şi la biometrie, ca măsuri suplimentare faţă de protecţiile realizate prin alte metode privind accesul în clădire. Ecusoanele trebuie să fie purtate prinse pe rever sau la gât. La modă sunt ecusoanele inteligente, care, de la distanţă, oferă informaţii despre posesor.

Locurile care nu dispun de uşi ce pot fi încuiate trebuie să aibă intrările supravegheate, iar o persoană, ofiţer de serviciu, să răspundă de această operaţiune, punându-i-se la dispoziţie şi un sistem de comunicaţie cu forţele de ordine. Cu acelaşi scop, poate fi folosită şi televiziunea cu

circuit închis, utilizată de forţele de ordine, cu condiţia ca o persoană să nu supravegheze mai mult de trei monitoare. Similar pot fi folosite camerele de luat vederi cu supraveghere continuă a principalelor încăperi ale clădirii, îndeosebi unde pătrund vizitatori.

Pentru vizitatori vor fi camere special amenajate, fără ca aceştia să aibă acces în zona prelucrării automate a datelor.

Imaginaţi câte un exemplu de aplicare pentru principiile de control al accesului enunţate mai sus.

### 3.2.2 Controlul accesului prin obiecte

Pentru a pătrunde într-o clădire sau o sală a ei, deseori se apelează la mai multe metode de autentificare, folosite alături de o *cartelă de plastic* sau un *jeton*. Cu acestea se oferă informaţii suplimentare despre purtător, cum ar fi numele, adresa, contul bancar, contul cardului de debit sau credit, informaţii medicale, drepturi de acces ş.a. Toate informaţiile menţionate pot fi codificate prin coduri bară, peliculă magnetică, microprocesoare. Unele dintre carduri conţin şi o fotografie a proprietarului, realizată, prin noile tehnologii, direct pe card.

Există şi *carduri inteligente* care se utilizează pentru criptarea şi decriptarea datelor, semnarea mesajelor şi introducerea sistemelor de plăţi electronice. Se pot folosi carduri care să aibă fotografia deţinătorului şi două microprocesoare folosite în scopuri diferite. Primul, pentru sisteme de plată, prin implementarea Master sau Euro sau Visa Cash, şi pentru aplicaţii de protejare a datelor cu care lucrează angajatul respectiv. Al doilea microprocesor este folosit pentru înlesnirea accesului în clădire şi la locurile de parcare. În ultimul timp, prin carduri inteligente se controlează accesul în organizaţie, în sălile ei, la calculator, la datele personale din clasicele buletine de identitate, din paşapoarte, din carnetul de şofer şi la datele medicale.

Practica oferă şi *ecusoane-active*, care apelează la identificarea prin frecvenţe radio (RFID - Radio-frequency identification), fără să fie nevoie de trecerea cartelei prin faţa unui cititor special. De asemenea, prin tehnologiile infraroşu se poate realiza citirea conţinutului unei cartele de la câţiva metri.

Cele mai multe *carduri* sunt *auto-expirante*; prin tehnologii termice speciale se realizează carduri cărora li se anulează scrisul după o anumită perioadă de expunere la lumină. Altele folosesc cerneluri ce-şi schimbă culoarea după un timp bine controlat, astfel încât să nu mai poată fi reutilizate. Ambele metode se folosesc, îndeosebi, pentru vizitatorii organizaţiilor.

Viitorul este al cardurilor inteligente, însă mulţi potenţiali beneficiari spun „Cardurile inteligente par a fi cea mai bună soluţie pentru problema noastră. În schimb, le vrem mai performante pentru a răspunde la toate cerinţele noastre”[2].

De asemenea, accesarea spaţiului cibernetic cu ajutorul laptop-urilor şi al PDA-urilor (Personal Digital Assistant) necesită noi tipuri de cartele pentru securizarea reţelelor fără fir (Wireless LAN – WLAN). Găsirea rapidă de soluţii a condus la cuplarea forţelor unor foşti competitori. *Visa International* şi-a unit forţele cu realizatorul de chip-uri *Sony Corp.* şi cu *Infineon* pentru realizarea unui nou chip, care poate fi folosit prin contactul direct al cardului cu un cititor, dar şi fără contact. *Fujitsu* şi *STMicroelectronics* au intrat în parteneriat pentru realizarea memoriei feroelectrice, ca o posibilă viitoare generaţie a cardurilor fără contact.

Lumea cardurilor este într-un moment crucial. Şansele sunt reale, dar parteneriatele aproape că sunt obligatorii. Don Davis (op. cit.) opina „Este mai bine să împarţi o felie de plăcintă cu un partener, decât să rămâi cu un platou gol.”

[2] Davis, D. – „The Problems Catch Up With The Solution”, in *Card Technology*, April 2003, Volume 8, Number 4, p. 4.

Folosind Internetul, prezentaţi comparativ, în termeni de avantaje şi dezavantaje, două soluţii de control acces şi pontaj al angajaţilor cu ajutorul ecusoanelor active RFID.

### 3.2.3 Controlul accesului prin biometrie

Dumnezeu l-a făcut pe om după chipul şi asemănarea lui, dar, cum oamenii s-au înmulţit, s-a simţit nevoia identificării fiecărui individ în parte. Primele forme de identificare s-au bazat pe *descrieri din memorie*, făcute de alte persoane, enumerându-se anumite trăsături sau semne particulare ale celui identificat, de cele mai multe ori reperarea făcându-se prin descrierea feţei persoanei sau a vocii. După mii de ani s-au menţinut aceste forme de identificare, întrucât şi astăzi *portretele-robot* sunt realizate tot pe această cale, dar cu ajutorul calculatoarelor.

Un moment important l-a constituit *inventarea fotografiei*. Ea încă se foloseşte la identificarea şi autentificarea persoanei prin plasarea pe buletinele de identitate, paşapoarte, legitimaţii ş.a. Sistemul este util poliţiei, lucrătorilor de la frontieră, organizaţiilor comerciale, bancare, diverselor instituţii ş.a.

Invenţia *amprentelor digitale* a condus la apariţia altui mod de identificare şi autentificare, prin culegerea probelor de pe obiectele constatate la locul înfăptuirii unui delict.

Până la 11 septembrie 2001 metodele de identificare biometrică erau respinse cu duritate de potenţialii beneficiari direcţi supuşi unor metode de identificare ce le-ar fi afectat sănătatea sau intimitatea. Cum invenţiile şi inovaţiile din domeniu nu au ţinut cont de părerile lor, au apărut o mulţime de tehnologii biometrice în sistemele de securitate a organizaţiilor. Unele dintre realizări sunt de-a dreptul stranii, deşi nu au nimic în comun cu biometria. Ne referim la viitoarele camere de luat vederi presărate peste tot: pe străzi, pe holurile instituţiilor, acasă, în mijloacele de transport. În Anglia, există deja 1.500.000 de camere de luat vederi pe străzi, Londra având introdus sistemul cu mulţi ani în urmă. Mai mult, noile camere de luat vederi pot dezbrăca, la propriu, trecând peste veşmintele protectoare ale persoanei, sau pot trece prin pereţii camerelor. Unde mai este protejată intimitatea!?!

Revenind la biometrie, am putea face referire şi la angajaţii Microsoft, care depind de o *cartelă inteligentă, cu elemente biometrice incluse*, de la intrarea în campusul unde se află locul de muncă, până la pătrunderea în birou, în restaurantul companiei, în orice loc unde îi este permis accesul persoanei, dar cu ea se poate realiza şi identificarea celui ce doreşte să lucreze la un calculator. Sistemul a cam bulversat angajaţii lui Bill Gates, dar se pare că s-au obişnuit cu el.

Mai şocantă ni se pare propunerea venită din partea Statelor Unite, ca efect al actului terorist de la 11 septembrie 2001, transformată în lege, adoptată de Congresul American, prin care se stipulează că orice străin care intră pe teritoriul Americii deţină un *document purtător al datelor biometrice*. Totul se bazează pe ideea ca posesorul unui paşaport furat sau al unei vize false să fie identificat prin amprenta digitală, a irisului, retinei sau feţei – în funcţie de tehnica biometrică adoptată. Oricum, se conturează obligativitatea includerii componentelor biometrice în toate actele de călătorie în doar câţiva ani, ceea ce conduce la dezvoltarea unei puternice industrii biometrice şi a alteia, a cardurilor inteligente.

Se preconizează că vor avea un demaraj foarte puternic *tehnologiile bazate pe recunoaşterea feţei şi a amprentelor digitale*, cărora li se va alătura, într-o mai mică măsură, *recunoaşterea irisului*. Oricum acestea sunt şi cele trei elemente biometrice recomandate de Organizaţia Internaţională de Aviaţie Civilă, cu sediul la Montreal, din care fac parte peste 188 de ţări. Prin progresele înregistrate în domeniul realizării noilor *chipuri*, ele pot fi plasate pe filele tuturor documentelor personale.

În tabelul 3.1 se face o scurtă descriere a celor mai noi patru tehnologii biometrice.

*Tabel nr. 3.1 – Prezentare comparativă a patru tehnologii biometrice*

| **Caracteristici** | **Recunoaşterea feţei** | **Amprenta digitală** | **Recunoaşterea irisului** | **Forma mâinii** |
|---|---|---|---|---|
| Rata respingerilor eronate | 3,3%-70% | 0,2%-36% | 1,9%-6% | 0-5% |
| Rata acceptărilor eronate | 0,3%-5% | 0%-8% | Sub 1% | 0%-2,1% |
| Timpul pentru o verificare | 10 secunde | 9-19 secunde | 12 secunde | 6-10 secunde |
| Mărimea probei culese | 84-1300 octeţi | 250-1000 octeţi | 512 octeţi | 9 octeţi |
| Numărul furnizorilor principali | 2 | Peste 25 | 1 | 1 |
| Preţul echipamentelor | Moderat | Mic | Mare | Moderat |
| Factorii ce afectează probele luate | Lumina, orientarea feţei, ochelarii de soare | Murdăria, degetele deshidratate sau accidentele | Vederea slabă, încruntarea sau reflexia | Răni, artrită, umflături |

*Sursa*: U.S. General Accounting Office
După *Card Technology*, April 2003, Volume 8, nr. 4, p. 23.

Informaţii suplimentare despre biometrie se pot obţine de pe următoarele adrese web:

- www.ibia.org – Asociaţia Internaţională a Industriei Biometrice
- www.visionics.com – Recunoaşterea feţei
- www.identix.com – Amprenta digitală
- www.recogsys – Amprenta digitală
- www.iriscan.com – Recunoaşterea irisului
- www.eyeticket.com – Recunoaşterea irisului

Consiliul de Conducere al Asociaţiei Internaţionale a Industriei Biometrice, după 11 septembrie 2001, făcea următoarele remarci:

- biometria şi intimitatea nu se exclud reciproc; de fapt, tehnologiile, în mod inerent, protejează identitatea împotriva dezvăluirilor neautorizate;
- nici o tehnologie nu este mai bună decât celelalte în cazul tuturor domeniilor de aplicaţii în care este folosită. În funcţie de aplicaţie, există mai multe opţiuni pentru soluţia biometrică optimă, astfel încât să fie diminuate ameninţările la care este supus sistemul;
- în ceea ce priveşte problema complexă a securităţii informaţionale, cercetările în dezvoltare vor oferi soluţii ce vor fi supuse testelor, ele constituind variante biometrice integrate pentru asigurarea protecţiei şi securităţii noilor sisteme;
- tot pe linia preocupărilor internaţionale, se vor realiza standarde şi produse biometrice care să acopere o cât mai largă paletă a cerinţelor beneficiarilor şi ale aplicaţiilor.

Toate cele de mai sus sunt puse la dispoziţia statelor sau organizaţiilor publice şi private pentru a diminua cât mai mult posibil efectul distructiv al actelor de vandalism şi terorism.

- Care este, în opinia dvs., cea mai spectaculoasă/utilă/eficientă/nouă tehnologie biometrică? Justificaţi
- Identificaţi alte tehnologii biometrice decât cele descrise mai sus şi prezentaţi-le pe scurt.
- Prezentaţi şi analizaţi controversa iscată la introducerea paşapoartelor biometrice în România. Care este părerea dvs. în raport cu acest subiect?

### 3.2.4 Controlul accesului prin parole

Principiul parolelor, cunoscut din lumea basmelor, într-o oarecare măsură este asemănător întrebuinţat şi în lumea calculatoarelor. Uneori, dintr-o dragoste excesivă faţă de trecut, utilizatorii greşesc, rămânând în aceeaşi lume, şi, ca atare, apelează şi în acest caz la arhicunoscutele cuvinte magice ale copilăriei. Un astfel de comportament este intuit şi de spărgătorii de sisteme, care, nu de puţine ori, reuşesc să le acceseze pe această cale. Multe „uşi informatice" s-au deschis la aflarea parolei „SESAM", dar, oricât de drag ne-ar fi cuvântul, utilizarea lui este total neinspirată.

Aşadar, parolele sunt utilizate pentru a ni se permite accesul la un calculator, fie ca utilizatori, fie sub forma grupurilor de utilizatori, fie ca personal al sistemului de prelucrare automată a datelor. După identificarea sau „legitimarea" persoanei, prin metodele amintite anterior, şi, eventual, oferirea unui jeton de acces, cei interesaţi prezintă sistemului propria lor parolă, fie prin tastarea de la un terminal, fie prin introducerea într-un echipament special al unui document care să conţină parola. Calculatorul compară parola cu o listă aprobată a acestora, aflată în softul sistemului, permiţându-i-se accesul şi garantându-i-se respectarea privilegiilor predefinite la anumite resurse ale sistemului, astfel:

- *Execuţie.* Poate lansa în execuţie un program, dar nu i se permite să umble la structura acestuia, prin adăugarea sau modificarea unor linii.
- *Citire.* Se poate citi un fişier, dar nici o altă operaţiune nu mai este permisă.
- *Scriere.* Se oferă posibilitatea de scriere a datelor în fişierul deschis, dar se interzic alte operaţiuni.
- *Citire-Scriere.* Se poate citi fişierul şi, de asemenea, se oferă dreptul de scriere în el.
- *Adăugare.* Dreptul este mai limitat, constând numai în posibilitatea de adăugare a noi date la cele existente, dar nu se pot citi sau schimba datele fişierului deschis.
- *Ştergere.* Utilizatorul poate efectua ştergerea unor date din fişier.

Menţionăm că sistemul parolelor, cât de complex ar fi el, nu realizează şi o securitate totală, ea depinzând în mod substanţial de modul de păstrare a secretului parolei. Să nu uităm că şi cele mai solide uşi, cu cele mai inteligente lacăte, sunt vulnerabile în faţa celor care au intrat în posesia cheilor.

Problema parolelor nu este încă suficient de bine înţeleasă de utilizatorii lor, apelându-se la forme foarte scurte, la nume ale eroilor din filme, din basme, la numele soţiei sau soţului, al copiilor, la numărul autoturismului ş.a. – toate vulnerabile în faţa unor spărgători calificaţi. O altă greşeală, amintită şi într-un paragraf anterior, constă în scrierea parolelor de teamă de a nu fi uitate, dar suportul lor este lăsat la vederea oricăror persoane ce ajung în cameră.

Parolele trebuie să fie eliberate doar persoanelor autorizate să exercite anumite funcţii în sistem şi nu trebuie să fie un proces generalizat, dându-se tuturor celor ce deţin poziţii importante în conducerea firmei. În cazul sistemelor ce conţin informaţii speciale, parolele se atribuie de ofiţerul cu securitatea sistemului. A da astfel de parole în folosinţa unor persoane echivalează cu permisiunea acestora de a accesa cele mai importante averi ale firmei.

Parolele pot fi create şi de utilizatori pentru datele mai puţin importante, dar există unele probleme care se repetă în numeroase cazuri, şi anume:

1. utilizatorii nu-şi schimbă la timp parolele, iar dacă o fac nu aduc modificări de substanţă în structura lor;

2. utilizatorii îşi păstrează parolele, din precauţia de a nu le uita, pe bucăţi de hârtie lăsate în văzul tuturor;
3. pentru o memorare uşoară se apelează la formele, amintite anterior, de atribuire a cuvintelor-parolă, ceea ce le face deosebit de vulnerabile. Printr-un recent studiu efectuat în Anglia, s-a constatat că, totuşi, cele mai uzuale parole date după celebrul mesaj al sistemului PASSWORD, ceea ce înseamnă parola sau cuvântul de trecere, sunt ... PASSWORD (ceea ce în româneşte ar însemna folosirea cuvântului PAROLA) şi SECRET.

În rândul specialiştilor români, deseori am constatat că parolele reprezintă numele copiilor, ale soţiilor, numele lor citite de la sfârşit la început, nume istorice, cuvinte bombastice din limba engleză (SMART, CLEVER, DUMMY, CRAZY ş.a.) sau banalul cuvânt GHICI.

Din cele relatate, rezultă că o parolă este şi o cheie şi trebuie să i se poarte de grijă ca şi obiectelor sau valorilor protejate prin ea. Din această cauză se impun câteva reguli de controlare a parolelor:

1. parolele trebuie să fie schimbate cam la şase luni, dar pentru datele deosebit de importante se impun termene şi mai scurte;
2. parolele comune trebuie schimbate imediat ce o persoană părăseşte grupul sau nu mai are dreptul utilizării lor;
3. parolele trebuie să fie schimbate imediat ce se constată unele bănuieli privind cunoaşterea lor de persoane neautorizate sau atunci când, din motive de forţă majoră, secretul lor a trebuit să fie dezvăluit pentru redresarea unei stări anormale temporare;
4. parolele trebuie să fie ţinute minte şi nu scrise pe oriunde, cu excepţia următoarelor cazuri:
   a) trebuie să fie scrise pentru intervenţii de urgenţă;
   b) fiecare parolă scrisă va fi introdusă într-un plic sigilat şi marcat în exterior cu scurte detalii privind calculatorul la care poate fi folosită şi numele celor autorizaţi a le folosi;
   c) plicul respectiv are tratamentul asemănător averilor protejate sau al categoriei de informaţii accesate prin parolă. După ruperea sigiliului, pe plic vor fi scrise data şi numele celor ce au aflat-o;
   d) plicurile cu parole se păstrează de către responsabilul cu securitatea sistemului;
5. dacă parolele-duplicat se păstrează prin intermediul calculatorului, astfel de fişiere trebuie să fie protejate împotriva accesului neautorizat şi create copii de siguranţă. Accesul la acest fişier trebuie să fie înlesnit doar persoanelor autorizate, respectându-se principiul „niciodată singur”. Listele cu parole vor fi memorate în formă criptată;
6. parolele nu vor fi afişate niciodată pe echipamentele din configuraţia sistemului, iar la introducerea lor de la tastatură nu trebuie să se afle persoane străine în preajmă;
7. parolele, în cele mai multe cazuri, au cel puţin opt caractere. Ele sunt caractere alfanumerice - litere (mari şi mici), cifre şi spaţii, folosite în ordine aleatoare, ceea ce ar însemna câteva mii de cuvinte de opt sau mai puţine caractere, care pot fi testate cu ajutorul calculatorului, în doar câteva minute, deci sunt suficient de vulnerabile pentru „profesioniştii” în spargeri de sisteme;
8. pentru blocarea operaţiunilor de încercare repetată, de ordinul miilor, calculatoarele trebuie să permită un număr limitat de încercări de introducere a acestora, uzual trei. Dacă limita a fost depăşită de către utilizator, intenţia trebuie să fie raportată conducătorului sistemului sau responsabilului cu securitatea, însoţită de un semnal sonor specific de avertizare. În acest timp trebuie să se blocheze terminalul de la care s-au efectuat prea multe încercări eşuate. Repunerea lui în funcţiune stă la îndemâna conducătorului sistemului. În cazul sistemelor speciale, se recomandă şi blocarea sălii sau a locului de unde s-a încercat accesarea prin parole eronate repetate, pentru identificarea persoanei respective;
9. odată ce au pătruns în sistem, utilizatorilor nu trebuie să li se permită să-şi schimbe identitatea cu care au efectuat deschiderea sesiunii şi nici să nu poată pătrunde în partiţiile alocate altor utilizatori;

10. dacă un terminal funcţionează o perioadă lungă de timp, procesul de autentificare trebuie să aibă loc la intervale regulate de timp pentru a se asigura că nu foloseşte altcineva sistemul. Dacă terminalul rămâne neutilizat, dar deschis, el trebuie să se închidă automat după un anumit interval de timp, de exemplu, 10 minute;
11. la deschiderea unei noi sesiuni de lucru, utilizatorului trebuie să i se aducă la cunoştinţă ultimul timp de accesare a sistemului cu parola respectivă, pentru a se verifica dacă altcineva a folosit-o între timp.

În cazul accesării bazelor de date deosebit de importante, cum sunt sistemele de operare, listele cu parole, se impune controlul dual al parolei, pe principiul „niciodată singur". Dar, cele două persoane nu trebuie să fie tot timpul aceleaşi şi ambele să fie la fel de bune cunoscătoare ale consecinţelor declanşării unor operaţiuni de la calculator.

Pentru preîntâmpinarea unor aspecte vulnerabile din sistemul de protecţie prin parole, se recomandă apelarea la un semn special sau la o dovadă de recunoaştere a utilizatorului. Ele pot fi: o cheie de descuiere a consolei, o cartelă magnetică bazată pe microprocesor, astfel încât să poată stabili cine, cum, când şi de unde să o folosească. Doar costul foarte mare nu duce la generalizarea acestui sistem.

De ultimă oră sunt produsele care apelează la echipamente ce acţionează pe principiul calculatoarelor portabile. Ele sunt sisteme speciale de criptare, care generează valori (parole) de autentificare personală a utilizatorilor şi care se preiau de la tastatura terminalelor, ca la sistemul clasic, pentru a se compara cu ceea ce generează un echipament similar aflat în calculator. Pe o astfel de cale nu mai sunt necesare cartele speciale de acces, totul fiind controlat prin calculator, îmbunătăţindu-se substanţial principiul simplu al parolelor.

Faceţi un inventar al parolelor pe care le folosiţi în prezent. Enumeraţi greşelile pe care le faceţi în legătură cu parolele şi, dacă sunt necesare, propuneţi câteva îmbunătăţiri ale modului de utilizare a parolelor dvs.

## 3.2.5 Controlul geografic al accesului în sistem

Într-o declaraţie a unui cunoscut om de afaceri din Rusia, Kasperski, se punea problema legitimării persoanelor utilizatoare de servicii informatice şi comunicaţii din spaţiul global, tocmai pentru a se asigura responsabilizarea şi conştientizarea participanţilor la noul tip de trafic. El făcea asemănarea cu sistemul de conducere a automobilelor de la începutul secolului XX, când, fiind atât de puţine, în caz de accident, era foarte uşor de identificat proprietarul – de cele mai multe ori el fiind şi conducătorul. Odată cu explozia de automobile de pe piaţă s-a simţit nevoia identificării proprietarului maşinii, prin *cartea de identitate a maşinii* şi prin *certificatul de înmatriculare*, dar şi a conducătorului auto, prin *permisul de conducere*.

La fel trebuie să se întâmple şi cu deţinătorii şi utilizatorii de calculatoare, deoarece, în prezent, multe acţiuni maliţioase se înfăptuiesc de persoane necunoscute, aflate în locuri învăluite în mister.

Autentificarea bazată pe localizarea geodezică (*location-based authentification*) este o metodă de autentificare a entităţilor din spaţiul cibernetic bazată pe localizarea geodezică (latitudinea, longitudinea şi altitudinea unui loc geografic bine definit). Aceasta va avea ca efect delimitarea porţiunii din spaţiul cibernetic de unde se declanşează un anumit eveniment. Se face astfel breşă într-un sistem destul de întrebuinţat de atacatorii sistemelor aflaţi într-un colţ al planetei, săvârşind fărădelegi în al colţ al acesteia, susţinând că se află în cu totul altul.

În literatură sunt prezentate realizările corporaţiei *International Series Research, Inc.* din Boulder, Colorado, care a realizat tehnologia autentificării locaţiei. Ea se numeşte *CyberLocator*, iar sistemul foloseşte semnalele bazate pe microunde transmise printr-o

constelaţie de 24 de sateliţi ai GPS (*Global Positioning System*) pentru calcularea şi validarea unei *semnături a locaţiei*, care este unică pentru fiecare loc de pe pământ în fiecare moment solicitat. Fiecare utilizator al unui sistem protejat are un senzor al semnăturii locaţiei (SSL), care este un tip special al receptorului GPS. SSL interceptează semnalele GPS şi transmite semnătura sa către o gazdă ce va face autentificarea. Gazda foloseşte semnalele GPS colectate de propriul SSL, plus informaţiile despre fiecare utilizator memorate într-o bază de date pentru a determina dacă acesta este conectat la un site aprobat anterior. Tehnologiile au ajuns la performanţe de acurateţe până la nivelul câtorva metri sau chiar şi mai bune (zeci de centimetri). Pentru că observaţiile GPS ale unui site anume sunt impredictibile prin simulări anticipate, la un nivel cerut de acurateţe, schimbate constant, unice oriunde ar fi, este practic imposibil de contrafăcut semnătura.

Autentificarea prin localizarea geodezică are câteva caracteristici esenţiale. Ea asigură o protecţie continuă împotriva celor rău intenţionaţi aflaţi la distanţă. Semnătura locaţiei poate fi folosită ca un mijloc comun de autentificare. Ştiindu-se reperele unui utilizator, se poate identifica uşor un intrus, dar se pot oferi şi probe că o persoană nu a fost în locaţia respectivă în momentul săvârşirii unei fapte condamnabile. O astfel de protecţie este recomandată pentru site-urile fixe, în care se poate plasa un senzor pe acoperiş sau la fereastră, cu condiţia orientării spre cer. Facem menţiunea că semnalele GPS nu trec prin ziduri şi acoperişuri. Deocamdată sunt unele limite tehnologice ale utilizării senzorilor în cazul utilizatorilor mobili.

Un dezavantaj al autentificării geodezice a locaţiei este acela al refuzului serviciului, în cazul bruierii semnalului sau al furtului senzorului. Alt dezavantaj se referă la uşurinţa localizării unei persoane în cazul unui război informaţional ofensiv, motiv pentru care accesul la datele geodezice trebuie să fie strict limitat.

În ce sisteme/situaţii consideraţi oportună folosirea controlului geografic al accesului?

## Rezumat

Sensul controlului accesului în sistem s-a schimbat radical, după 11 septembrie 2001, atât prin prisma mijloacelor de exercitare, cât şi a domeniilor de aplicare. Controalele sunt introduse pentru diminuarea riscurilor la care sunt expuse sistemele şi pentru reducerea potenţialelor pierderi. Controalele pot fi *preventive*, *detective* sau *corective*. Pentru atingerea obiectivelor, controalele pot fi *administrative*, *logice sau tehnice* şi *fizice*. Există şi forme combinate de control: preventiv/administrativ, preventiv/tehnic, preventiv/fizic, detectiv/administrativ, detectiv/tehnic, detectiv/fizic.

*Identificarea şi autentificarea persoanelor* se efectuează în patru moduri: prin ceva aflat în posesia persoanei, ceva care individualizează persoana, ceva ce ştie persoana, locul geografic în care se află aceasta la un moment dat.

Principiile de bază ale controlului accesului sunt: *simpla posesie a unui element de control al accesului nu trebuie să constituie şi proba accesului privilegiat*; *atunci când valorile patrimoniale sunt deosebit de importante şi mecanismul de protecţie trebuie să fie pe măsură*; *nici unei persoane nu trebuie să i se garanteze accesul permanent, gestiunea sau cunoaşterea informaţiilor secrete numai pe motivul poziţiei ierarhice pe care o deţine*.

CAPITOLUL IV

# Politici, standarde, norme şi proceduri de securitate

Orice organizaţie care doreşte să-şi apere valorile informaţionale trebuie să conceapă o modalitate logică şi coerentă de protejare a acestora, ţinând seama de recomandările legale în domeniu şi de realităţile specifice activităţii sale. Ea va analiza pe de o parte pericolele interne şi externe, iar pe de altă parte metodele disponibile de contracarare a lor. Demersurile sale se vor concretiza, printre altele, în politici, standarde, norme şi proceduri de securitate.

Obiectivele capitolului curent sunt:

- cunoaşterea principalelor modele ale politicilor de securitate;
- identificarea elementelor care trebuie să stea la baza dezvoltării programelor de securitate;
- dobândirea cunoştinţelor necesare pentru a realiza politici de securitate pentru diverse zone ale unei organizaţii.

## 4.1 Modele de politici de securitate

Situaţia definirii politicilor de securitate a devenit complicată atunci când sistemul militar de clasificare a informaţiilor a fost preluat ca model de domenii civile, cum sunt cel economic, politic, medical ş.a., informaţiile fiind grupate în două mari categorii: clasificate (confidenţiale, secrete, strict secrete) şi neclasificate (sau publice). Lucrurile s-au complicat şi mai tare după ce britanicii au mai introdus un nivel, RESTRICŢIONATE, între informaţiile NECLASIFICATE şi cele CONFIDENŢIALE. Şi în SUA a existat acest nivel dar, odată cu promulgarea legii accesului liber la informaţii (*Freedom of Information Act, FOIA*), el a dispărut. Ca atare, America are două marcaje suplimentare: *numai pentru utilizare oficială* (*For Official Use Only, FOUO*), care se referă la date neclasificate dar care nu pot fi făcute publice prin efectul legii accesului liber la informaţii, în timp ce informaţiile neclasificate, dar sensibile (*Unclassified but sensitive*) includ FOUO plus datele ce pot fi făcute publice, ca efect al FOIA.

În Marea Britanie, informaţiile restricţionate, în practică, sunt făcute publice, dar marcajul aplicat, RESTRICŢIONATE, face ca jurnaliştii şi alte categorii interesate de scurgeri de informaţii să fie sancţionaţi dacă le fac publice, ca efect al legii secretului oficial. Este o ciudăţenie care se adaugă alteia: documentele neclasificate din SUA care traversează oceanul în Marea Britanie devin automat RESTRICŢIONATE, iar dacă se transmit înapoi în SUA devin CONFIDENŢIALE – motiv serios pentru realizatorii sistemelor militare clasificate americane să acuze politica din Marea Britanie că ar fi una ce sparge schema clasificării SUA.

În plus, există sistemul bazat pe cuvinte-cod, prin care informaţiile de orice tip pot fi supuse altor restricţii, numite *clasificare compartimentală* (în varianta americană) sau *securitate multilaterală* (în varianta europeană). Se utilizează în acest scop *descriptori*, *cuvinte-de-avertizare* şi *marcaje internaţionale de apărare* (*International Default Organization, IDO*).

Toate aceste aspecte sunt tratate ştiinţific prin *modelele de politici de securitate*, grupate în *modele de securitate multinivel* şi în *modele de securitate multilaterală*.

### 4.1.1 Modele de securitate multinivel

Când privim un sistem, din punct de vedere al securităţii lui, întregul este separat în părţi, prin linii orizontale, realizându-se aşa-zisa securitate pe niveluri multiple (multinivel) prin care se face o delimitare netă între categoriile de informaţii din sistem (publice, confidenţiale, secrete,

strict secrete). O astfel de delimitare asigură certitudinea citirii informaţiilor dintr-o anumită clasificare numai de persoanele care au autorizarea cel puţin egală cu clasificarea informaţiilor citite. Într-o formă schematică, sistemul este structurat ca în figura 4.1.


**Fig. 4.1 Model de securitate multinivel**

Politicile de controlare a accesului sunt foarte clare: o persoană poate citi un document numai dacă autorizarea sa este cel puţin egală cu clasificarea informaţiei citite. Ca efect, *informaţiile vor circula doar de jos în sus*, de la nivelul CONFIDENŢIAL, la SECRET, STRICT SECRET ş.a., iar de sus în jos nu au voie să circule decât dacă o persoană autorizată le declasifică.

**Modelul Bell-LaPadula**

Cel mai cunoscut model al politicilor de securitate este cel propus de David Bell şi Len LaPadula, în 1973, ca răspuns la preocupările Forţelor Aeriene ale Statelor Unite de securizare a sistemelor de partajare a timpului, bazate pe mainframe-uri. Modelul este cunoscut sub numele *Bell-LaPadula* sau *modelul de securitate multinivel*. Sistemele ce le adoptă sunt numite şi „sigure multinivel" sau MLS (*MultiLevel Secure*). Proprietatea de bază a acestor sisteme este aceea că *informaţiile pot circula în jos*.

Formal, modelul Bell-LaPadula a introdus trei principii:

- *principiul* (sau proprietatea) *securităţii simple*, prin care nu-i este permis nici unui proces să citească date aflate pe un nivel superior lui. Este cunoscut şi ca *Nu citi deasupra* (*No Read Up*, *NRU*);
- *principiul* * (se citeşte stea): nici un proces nu poate să scrie date pe un nivel aflat sub el. Este cunoscut şi ca *Nu scrie dedesubt* (*No Write Down*, *NWD*);
- *principiul securităţii discreţionare* introduce o matrice de acces pentru a specifica controlul accesului discreţionar. Este cunoscut şi ca *Trusted Subject* (subiect de încredere). Prin acest principiu, subiectul de încredere violează principiul *, dar nu se abate de la scopul său.

Cele trei principii sunt redate în figura 4.2.


**Fig. 4.2 Modelul Bell-LaPadula, cu cele trei principii**

**Modelul matricei de control al accesului**

Printr-o matrice de acces se oferă drepturi de acces pentru *subiecte de încredere* la obiectele sistemului. Drepturile de acces sunt de tipul *citeşte, scrie, execută* ş.a. Un *subiect de încredere* este o entitate activă care îşi caută drepturile de acces la resurse sau obiecte. Subiectul poate fi o persoană, un program sau un proces. Un *obiect* este o entitate pasivă, cum sunt fişierele sau o resursă de stocare. Sunt cazuri în care un element poate fi, într-un anumit context, subiect şi, în alt context, poate fi obiect. O matrice de acces este redată în figura 4.3.

Coloanele se numesc *Liste de control al accesului*, iar liniile, *Liste de competenţe*. Modelul matricei de control al accesului acceptă controlul discreţionar al accesului pentru că intrările în matrice sunt la discreţia persoanelor care au autorizaţia de a completa tabelul.

În matricea de control al accesului, competenţele unui subiect sunt definite prin tripleta (*obiect, drepturi, număr aleator*).

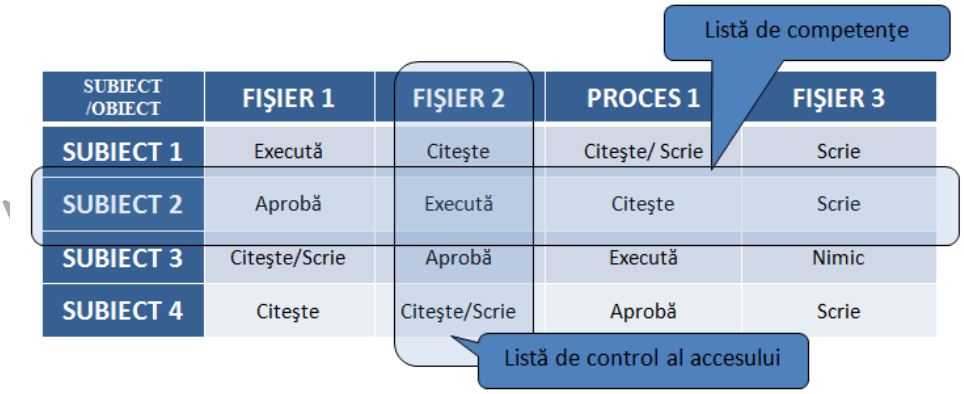


**Fig. 4.3 Matrice de control al accesului**

**Modelul Biba**

În multe cărţi este amintit şi modelul Biba, al lui Ken Biba, ocupându-se doar de integritatea sistemelor, nu şi de confidenţialitate. El se bazează pe observaţia că în multe cazuri confidenţialitatea şi integritatea sunt concepte duale: în timp ce prin confidenţialitate se impun restricţii celor ce pot citi un mesaj, prin integritate sunt controlaţi cei ce pot să scrie sau să modifice un mesaj.

În unele organizaţii guvernamentale sau comerciale există aplicaţii în care integritatea datelor este mult mai importantă decât confidenţialitatea, ceea ce a făcut să apară modele formale ale integrităţii.

Integritatea vizează trei scopuri principale:

- protejarea datelor împotriva modificărilor efectuate de utilizatorii neautorizaţi;
- protejarea datelor împotriva modificărilor neautorizate efectuate de utilizatori autorizaţi;
- asigurarea consistenţei interne şi externe a datelor.

Modelul a fost realizat în 1977 ca unul al integrităţii datelor, aşa cum modelul Bell-LaPadula este cunoscut ca modelul confidenţialităţii datelor. Modelul Biba este unul de tip reţea şi foloseşte *relaţia mai mic sau egal*. O structură a reţelei este definită ca un ansamblu parţial ordonat cu cea mai mică limită superioară, LUB (*Least Upper Bound*), şi cea mai mare limită inferioară, GLB (*Greatest Lower Bound*).

O reţea reprezintă un ansamblu de clase de integritate (CI) şi de relaţii ordonate între aceste clase. Ea poate fi definită astfel:

*(CI, <=, LUB, GLB)*.

Aşa cum Bell-LaPadula operează cu niveluri diferite de sensibilitate, modelul Biba clasifică obiectele în diferite niveluri de integritate. Modelul enunţă trei axiome ale integrităţii:

1. *axioma integrităţii simple*. Ea stabileşte că unui subiect aflat pe un anumit nivel de integritate nu-i este permis să observe (citească) un obiect de o integritate mai joasă (*No Read Down, Nu citi dedesubt*).
2. *axioma integrităţii* * (se citeşte stea) stabileşte că unui obiect situat pe un anumit nivel de integritate nu-i este permis să modifice (scrie) alt obiect situat pe un nivel mai înalt de integritate (*No Write Up, Nu scrie deasupra)*;
3. *un subiect de pe un anumit nivel de integritate nu poate solicita un subiect situat pe un nivel de integritate superior*.

Axiomele şi modelul Biba sunt redate în figura 4.4.

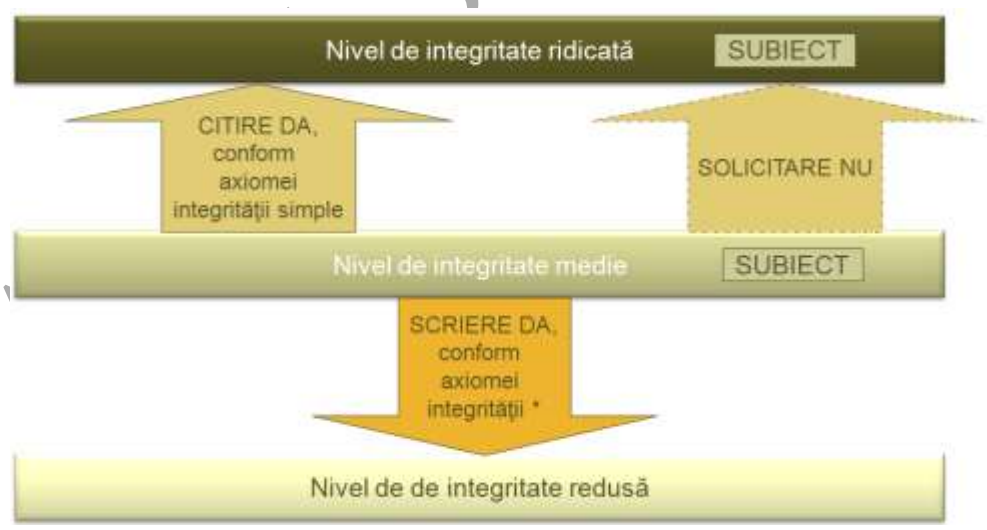


**Fig. 4.4 Modelul Biba, cu axiomele lui**

În practică au fost implementate mai multe tipuri de sisteme de securitate multinivel, cum sunt SCOMP, Blocker, MLS Unixe, CMWs, NRL Pump, MLS Logistics, Purple Penelope ş.a.

### 4.1.2 Modele ale securităţii multilaterale

Deseori, în realitate, preocupările noastre s-au concentrat nu către prevenirea curgerii *în jos* a informaţiilor, ci către stoparea fluxurilor *între* diferite compartimente. În astfel de sisteme, în locul frontierelor orizontale, aşa cum recomandă modelul Bell-LaPadula, s-au creat altele verticale, conform figurii 4.5.

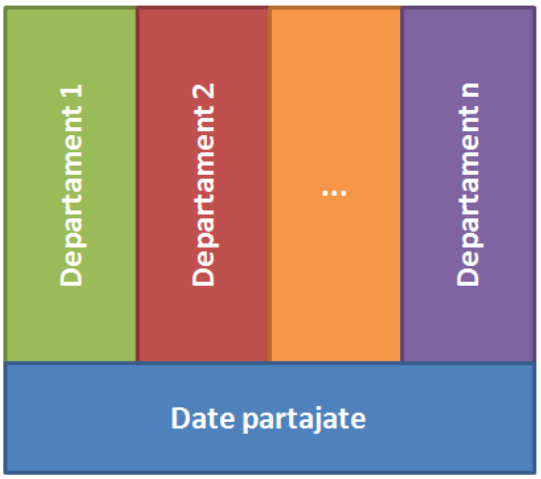


**Fig. 4.5 Modelul securităţii multilaterale**

Acest control al fluxurilor informaţionale laterale este unul organizaţional, aşa cum este cel al organizaţiilor secrete, pentru păstrarea în taină a numelor agenţilor care lucrează în alte ţări, fără să fie cunoscuţi de alte departamente speciale. La fel se întâmplă şi în companii, unde separarea verticală a compartimentelor, după funcţiile îndeplinite (producţie, comercială, personal-salarizare ş.a.), conduce la o situaţie identică.

Există cel puţin trei modele diferite de implementare a controlului accesului şi de control al fluxurilor informaţionale prin *modelul securităţii multilaterale*. Ele sunt:

- *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 informaţionale din domeniul sănătăţii, conform cu etica medicală.

**Compartimentarea şi modelul reţea**

Ani mulţi acest model a servit ca practică standard, în SUA şi guvernele aliate, pentru restricţionarea accesului la informaţii, prin folosirea cuvintelor-cod şi a clasificărilor. Este arhicunoscut cuvântul-cod *Ultra*, folosit în cel de-al doilea război mondial, de către englezi şi americani, pentru decriptarea mesajelor criptate de germani cu maşina Enigma. Cercul persoanelor cu acces la mesajele decriptate fiind foarte redus, numărul autorizărilor pentru informaţii 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 şi deasupra ei.

Cuvintele-cod sunt folosite pentru crearea grupurilor de control al accesului printr-o variantă a modelului Bell-LaPadula, numită *modelul reţea*. Clasificările, împreună cu cuvintele-cod, formează o reţea, conform figurii 4.6. Potrivit modelului, o persoană autorizată să aibă acces la informaţii SECRETE nu poate accesa informaţii SECRETE CRIPTO, dacă nu are şi autorizaţie pentru CRIPTO.

Ca un sistem să răspundă acestor cerinţe, va trebui ca problemele clasificării informaţiilor, ale autorizării persoanelor şi ale etichetelor ce însoţesc informaţiile să se transfere în politica de securitate pentru a defini ţintele securităţii, modul de implementare şi evaluare.

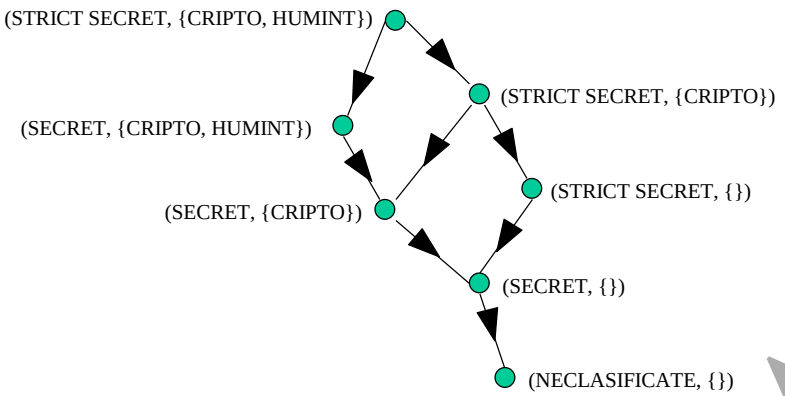


**Fig. 4.6 Model reţea cu etichete de securitate**

**Modelul zidului chinezesc**

Modelul a fost realizat de Brewer şi Nash. Numele provine de la faptul că firmele care prestează servicii financiare, cum sunt băncile de investiţii, 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 firmele prestatoare de servicii au clienţii lor şi pentru a-i păstra se află într-o veritabilă competiţie. 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 puţin pentru o perioadă controlată de timp. Prin aceasta, caracteristica modelului zidului chinezesc constă într-un *mix de libertate de opţiune şi de control obligatoriu al accesului*: *oricine este liber să lucreze la orice companie, dar îndată ce a optat pentru una, se supune restricţiilor ce operează în domeniul respectiv de activitate*.

Modelul zidului chinezesc introduce *principiul separării obligaţiilor de serviciu*: un utilizator anume poate să prelucreze tranzacţiile A sau B, nu amândouă. Aşadar, 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 pacienţilor. În efortul multor ţări de a introduce carduri inteligente cu datele medicale personale, se înregistrează o puternică opoziţie din partea publicului. Acesta invocă vulnerabilitatea individului prin trecerea informaţiilor despre anumite boli foarte grave, purtate până acum pe brăţara de la mână, pe cartela inteligentă, ceea ce va face ca atunci când se va afla în avion, în ţări străine, să fie foarte greu sau chiar imposibil să i se citească informaţiile respective. O altă problemă se referă la păstrarea secretului datelor personale sau a unei părţi dintre acestea.

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

Scopul modelului politicii de securitate BMA este acela de consolidare a *principiului consimţământului pacientului* şi de a preveni accesul prea multor persoane la datele personale din bazele de date ce le conţin. 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, controlul modificărilor din liste, consimţământul şi notificarea clientului, persistenţa, marcarea accesului pentru a servi ca probă în justiţie, urmărirea fluxului informaţiilor, controlul agregării informaţiilor, încrederea în sistemele informatice.

În metodele top-down de proiectare a securităţii trebuie, mai întâi, să se determine modelul ameninţării, apoi să se scrie politica, după care aceasta se supune testului pentru a vedea cum îşi face efectul.

Realizaţi o matrice de control al accesului pentru un (sub)sistem informaţional cunoscut.

## 4.2 Programul de securitate

Organizaţiile au nevoie să-şi protejeze valorile patrimoniale vitale, începând cu resursele umane, continuând cu clădiri, terenuri, utilaje, echipamente speciale şi încheind cu una dintre cele mai importante averi ale noului mileniu, informaţia. Tocmai din această cauză se concep programe de securitate informaţională. Înainte ca acest program să fie abordat, se cuvine efectuată structurarea iniţiativei încă din faza intenţională, realizându-se sau definindu-se politicile, standardele, normele şi procedurile. În acest context, programul de securitate trebuie să se supună elementelor enunţate anterior.

Fără politici riguroase, programele de securitate vor fi aproape fără suport, ineficiente şi nu se vor alinia strategiei şi obiectivelor organizaţiei. Politicile, standardele, normele şi procedurile constituie fundaţia programului de securitate al organizaţiei. Politicile eficiente, clar formulate, vor servi proceselor de auditare şi eventualelor litigii. Combinând elementele specificate, o entitate poate implementa controale specifice, procese, programe de conştientizare şi multe altele, tocmai pentru a-i aduce un plus de linişte. Spune românul: paza bună trece primejdia rea.

### 4.2.1 Politicile

O politică, deseori, înseamnă mai multe lucruri, atunci când ne referim la securitatea informaţională a unei organizaţii. Cineva poate să se rezume doar la firewall-urile folosite pentru controlarea accesului şi a traseelor pe care circulă informaţiile, altcineva se gândeşte la lacătele, cardurile de acces, camerele de luat vederi ce înregistrează totul din perimetrele controlate. Dar, câte alte accepţiuni nu i se pot da!

Atunci când discutăm despre politici de securitate, trebuie pornit de la vârful piramidei manageriale, unde se află *top managerii*. Ei au misiunea de a formula *Declaraţia politicii organizaţiei* (*Statement of Policy*). Aceasta este o formulare generală, o declaraţie din care să reiasă:

- importanţa resurselor informaţionale pentru atingerea obiectivelor strategice ale organizaţiei;
- formularea clară a sprijinului acordat tehnologiilor informaţionale în unitate;
- angajamentul top managerilor de a autoriza sau coordona activităţile de definire a standardelor, procedurilor şi normelor de securitate de pe nivelurile inferioare.

În afara declaraţiei politicii de securitate la nivelul top managerilor, există şi politici obligatorii, politici recomandate şi politici informative.

*Politicile obligatorii* sunt politici de securitate pe care organizaţiile sunt obligate să le implementeze ca efect al acordurilor, regulamentelor sau al altor prevederi legale. De regulă, aici se încadrează instituţiile financiare, serviciile publice sau orice alt tip de organizaţie care serveşte interesului public. Aceste politici sunt foarte detaliate şi au elemente specifice, în funcţie de domeniul de aplicare.

De regulă, politicile obligatorii au două scopuri de bază:

- asigurarea că o organizaţie urmează procedurile standard sau politicile de bază din domeniul ei de activitate;
- de a oferi încredere organizaţiilor că ele urmează standardele şi politicile de securitate din domeniul de activitate.

*Politicile recomandate*, prin definiţie, nu sunt obligatorii, dar sunt puternic susţinute, cu prezentarea consecinţelor foarte dure în cazul înregistrării eşecurilor. O organizaţie este direct interesată ca toţi angajaţii 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 mulţi angajaţi vor fi riguros controlaţi prin astfel de politici, definindu-le rolurile şi responsabilităţile în organizaţie.

*Politicile informative* au scopul de a informa cititorii. Nu poate fi vorba de cerinţe specifice, iar interesaţii de aceste politici pot să se afle în interiorul organizaţiei sau printre partenerii ei.

După aceste descrieri, putem să facem o scurtă prezentare a elementelor comune tuturor politicilor de securitate, astfel:

- *domeniul de aplicare*: declararea domeniului de aplicare înseamnă prezentarea intenţiei vizate de politică şi ea va scoate în relief şi legăturile existente cu întreaga documentaţie a organizaţiei. Formularea trebuie să fie scurtă şi se plasează la începutul documentului;
- *declararea politicii top managerilor* se include la începutul documentului şi are dimensiunea unui singur paragraf, specificând scopul global al politicii;
- *responsabilităţile* constituie conţinutul unei secţiuni distincte şi cuprind persoanele implicate în asigurarea bunei funcţionări a politicii;
- *consecinţele*: printr-o astfel de formulare se prezintă pierderile posibile dacă politica nu va fi respectată;
- *monitorizarea*: se specifică modul în care se monitorizează respectarea şi actualizarea continuă a politicii;
- *excepţiile*: se menţionează cazurile în care apar excepţii şi modalităţile de tratare a lor; de regulă, au o durată limitată de aplicare, de la un caz la altul.

### 4.2.2 Standardele, normele şi procedurile de securitate

Pe nivelul inferior politicilor se află trei elemente de implementare a politicii: standardele, normele şi procedurile. Ele conţin detaliile politicii, cum ar fi posibilităţile de implementare, ce standarde şi proceduri să fie întrebuinţate. Ele sunt făcute publice la nivel de organizaţie, prin manuale, Intranet, cărţi, cursuri ş.a.

De cele mai multe ori, standardele, normele şi procedurile sunt tratate laolaltă, dar nu este cea mai inspirată idee, fiindcă tratarea separată a lor este justificată de următoarele argumente:

- fiecare dintre ele serveşte unei funcţii diferite şi are propria audienţă; chiar şi distribuţia lor fizică este mai lejeră;
- controalele securităţii pe linia confidenţialităţii sunt diferite pentru fiecare tip de politică;
- actualizarea şi întreţinerea politicii ar deveni mai anevoioase, prin prisma volumului documentaţiei, dacă s-ar trata nediferenţiat.

**Standardele**

Standardele specifică utilizarea anumitor tehnologii, într-o viziune uniformă. De regulă, standardele sunt obligatorii şi sunt implementate la nivel de unitate, tocmai pentru asigurarea uniformităţii. Elementele principale ale unui standard de securitate informaţională sunt:

- *scopul şi aria de aplicare*, prin care se oferă o descriere a intenţiei standardului (realizarea unui tip de server pe o anumită platformă);
- *roluri şi responsabilităţi* la nivel de corporaţie pe linia definirii, execuţiei şi promovării standardului;
- *standardele cadrului de bază*, prin care sunt prezentate declaraţiile de pe cel mai înalt nivel, aplicabile platformelor şi aplicaţiilor;

- *standardele tehnologiei* conţin declaraţiile şi descrierile aferente (configuraţia sistemului sau serviciile nesolicitate de sistem);
- *standardele administrării* reglementează administrarea iniţială şi în timpul exploatării platformei şi aplicaţiilor.

**Normele**

Normele sunt oarecum asemănătoare standardelor, referindu-se la metodologiile sistemelor securizate, numai că ele sunt acţiuni recomandate, nu obligatorii. Sunt mult mai flexibile decât standardele şi iau în considerare naturile diverse ale sistemelor informaţionale. Ele specifică modalităţile de dezvoltare a standardelor sau garantează aderenţa la principiile generale ale securităţii.

Elementele principale ale unei norme de securitate informaţională sunt:

- *scopul şi aria de aplicare*, descriindu-se intenţia urmărită prin regula respectivă;
- *roluri şi responsabilităţi* pe linia definirii, execuţiei şi promovării normei;
- *declaraţii de orientare*: este un proces pas-cu-pas de promovare a tehnologiilor respective;
- *declaraţii de exploatare*: se definesc obligaţiile zilnice, săptămânale sau lunare pentru o corectă exploatare a tehnologiei respective.

**Procedurile**

Procedurile prezintă paşii detaliaţi ce trebuie să fie parcurşi pentru execuţia unei activităţi. Se descriu acţiunile concrete pe care trebuie să le efectueze personalul. Prin ele se oferă cele mai mici detalii pentru implementarea politicilor, standardelor şi normelor. Uneori se foloseşte în locul acestui concept cel de *practici*.

### 4.2.3 Aspecte practice ale politicii de securitate informaţională[1]

Pentru realizarea propriei politici de securitate există mai multe puncte de pornire. În primul rând, literatura de specialitate este destul de bogată şi poate fi consultată cu multă uşurinţă. Pentru cei mai comozi, dar care dispun de resursele financiare necesare, recomandăm vizitarea site-ului: *www.information-security-policies-and-standards.com/*. Aici există posibilitatea procurării *pre-written policies*, a politicilor pre-definite, ce pot fi adaptate apoi intereselor organizaţiei. Şi, fiindcă am amintit site-ul de mai sus, tot aici veţi putea vedea structura standardului internaţional de definire a politicii de securitate, ISO 17799, bazat pe standardul britanic BS7799. El este organizat pe 10 secţiuni, fiecare acoperind domenii sau teme diferite, după cum urmează:

1. *Planificarea funcţionării neîntrerupte a unităţii*, cu obiectivul contracarării întreruperilor de activitate ale unităţii şi ale proceselor principale ca efect al unor accidente majore sau dezastre.
2. *Controlul accesului în sistem*, cu obiectivele:
   2.1) controlarea accesului la informaţii;
   2.2) prevenirea accesului neautorizat în sistemul informaţional;
   2.3) asigurarea protecţiei serviciilor prestate în reţea;
   2.4) prevenirea accesului neautorizat la calculatoare;
   2.5) detectarea activităţilor neautorizate;
   2.6) asigurarea securităţii informaţiilor când se folosesc comunicaţiile mobile şi tele-activităţile.
3. *Dezvoltarea şi întreţinerea sistemului*, cu obiectivele:
   3.1) asigurarea securităţii prin sistemul operaţional;

[1] Paragraf realizat de conf. univ. dr. Adrian Bogdănel Munteanu.

3.2) prevenirea pierderilor, modificărilor sau folosirii inadecvate a datelor din aplicaţiile sistemului;
3.3) protejarea confidenţialităţii, integrităţii şi autenticităţii informaţiilor;
3.4) asigurarea că proiectele informatice şi activităţile colaterale se derulează după proceduri sigure;
3.5) menţinerea securităţii softului şi datelor din aplicaţiile sistemului.

4. *Securitatea fizică şi a mediului*, cu obiectivele:
4.1) prevenirea accesului neautorizat, a distrugerilor şi interferenţelor cu informaţiile şi celelalte componente ale sistemului;
4.2) prevenirea pierderilor, distrugerilor sau compromiterilor valorilor patrimoniale, precum şi stoparea întreruperilor de activitate;
4.3) prevenirea compromiterii sau furtului de informaţii şi al altor resurse informaţionale.

5. *Maleabilitatea*, cu obiectivele:
5.1) preîntâmpinarea încălcării cadrului juridic, a celui statutar, regulamentar sau a oricărei obligaţii contractuale, precum şi a cerinţelor pe linia securităţii;
5.2) asigurarea maleabilităţii sistemului la politicile şi standardele organizaţionale pe linia securităţii;
5.3) maximizarea eficienţei procesului de auditare a sistemului şi minimizarea interferenţelor cu acesta.

6. *Securitatea personalului*, cu obiectivele:
6.1) diminuarea riscurilor provocate de factorul uman, fraudă sau folosirea ilegală a componentelor sistemului;
6.2) asigurarea că utilizatorii sunt conştienţi şi preocupaţi de preîntâmpinarea sau diminuarea ameninţărilor asupra securităţii informaţiilor, susţinând politica de securitate a organizaţiei prin tot ceea ce fac zi de zi;
6.3) minimizarea pagubelor provocate de incidentele apărute în sistem sau de proasta funcţionare a acestuia, precum şi reţinerea incidentelor ca lecţii pentru viitor.

7. *Organizarea securităţii*, cu obiectivele:
7.1) asigurarea managementului securităţii informaţionale în cadrul organizaţiei;
7.2) asigurarea securităţii componentelor folosite în prelucrarea informaţiilor organizaţiei accesate de către terţi;
7.3) asigurarea securităţii informaţiilor când responsabilitatea prelucrării acestora revine unei alte organizaţii, ca serviciu externalizat.

8. *Managementul resurselor informatice şi al exploatării lor*, cu obiectivele:
8.1) asigurarea funcţionării corecte şi sigure a componentelor sistemului informatic;
8.2) minimizarea riscului căderii sistemului;
8.3) protejarea integrităţii softului şi a informaţiilor;
8.4) asigurarea integrităţii şi disponibilităţii informaţiilor prelucrate şi comunicate;
8.5) asigurarea încrederii în informaţiile din reţele şi protejarea infrastructurii corespunzătoare;
8.6) prevenirea pierderilor de valori patrimoniale şi a întreruperilor de activitate;
8.7) prevenirea pierderilor, modificărilor sau utilizărilor ilegale în schimburile de informaţii cu alte organizaţii.

9. *Clasificarea şi controlarea valorilor patrimoniale*, cu obiectivele:
9.1) menţinerea unei protecţii corespunzătoare a valorilor patrimoniale ale organizaţiei;
9.2) oferirea încrederii că valorile patrimoniale informaţionale au asigurat un nivel de protecţie corespunzător .

10. *Politica de securitate*, cu obiectivele:
10.1) oferirea de direcţii manageriale;
10.2) sprijinirea acţiunilor întreprinse pe planul securităţii informaţionale.

Fiecare dintre cele zece secţiuni are în structură descrieri detaliate prin care se defineşte standardul ISO 17799.

Fiecare dintre cele zece secţiuni are în structură descrieri detaliate prin care se defineşte standardul ISO 17799 - cunoscut din 2005 ca ISO 27002.

În prezent, ISO/IEC 27001 este standardul formal în baza cărora organizaţiile îşi pot certifica sistemele de management al securităţii informaţiilor (SMSI). Standardul acoperă toate domeniile de activitate şi specifică cerinţele pentru stabilirea, implementarea, operarea, monitorizarea, revizia, întreţinerea şi îmbunătăţirea unui SMSI documentat.

La începutul anilor '90, British Standard Institution (BSI)[2] a dezvoltat o serie de standarde ca răspuns la cererile industriei, guvernului şi mediului de afaceri de a crea o structură comună pentru securitatea informaţiilor. În 1995, autoritatea de reglementare din Marea Britanie a adoptat în mod oficial BS7799.

În decembrie 2000, ISO a preluat primele 4 părţi ale BS şi le-a publicat sub numele „ISO 17799 - Code of Practice". La sfârşitul anului 2002, partea a doua a BS7799 a fost revizuită pentru a reflecta şi prevederile ISO 9001: 2000, ISO 14001: 1996 şi principiile OECD. Standardul este adoptat în 2005 sub denumirea ISO 27001; totodată, ISO 17799 devine ISO 27002.

Cu toate acestea, de atunci şi până astăzi, standardul nu a fost şi nu este obligatoriu nici măcar pentru companiile din ţara mamă.

Pe piaţa autohtonă s-a lansat ideea că, dacă o companie este certificată/evaluată în baza ISO 27001 şi are un sistem informaţional în conformitate cu acest standard, în mod automat sistemul informaţional este *sigur!* În primul rând, nu poate afirma nimeni, despre nici un sistem, că ar fi 100% sigur. Standardul oferă, de fapt, sprijin organizaţiilor în adoptarea unor controale interne mai eficiente. Sunt destule voci care critică acest standard pentru că nu are cum să acopere toate speţele legate de securitatea informaţională, evoluţia tehnologică fiind mult mai rapidă.

ISO 27001 este organizat în 10 secţiuni care acoperă următoarele domenii:

- *Politica de Securitate:* orice organizaţie *trebuie* să aibă un document care să definească şi să explice securitatea informaţională;
- *organizarea securităţii:* defineşte principiile care stau la baza managementului securităţii în orice organizaţie;
- *securitatea personalului:* descrie cerinţele legate de recrutarea şi instruirea angajaţilor şi managementul incidentelor din sistem;
- *securitatea fizică şi a mediului de lucru:* sunt avute în vedere controalele generale implementate în cadrul organizaţiei;
- *managementul operaţional şi al comunicaţiilor:* acoperă procedurile documentate cu privire la operarea la calculator şi comunicarea informaţiilor;
- *controlul accesului:* principiile care guvernează accesul securizat la informaţii;
- *dezvoltarea şi întreţinerea sistemelor:* cerinţele legate de securitate trebuie avute în vedere în fiecare etapă a ciclului de viaţă al unui sistem;
- *planificarea continuităţii afacerii:* analiza de impact, proceduri de refacere, testare;
- *conformitatea:* securitatea informaţională trebuie să fie conformă cu orice prevedere legală aplicabilă.

Filosofia standardului o reprezintă considerarea securităţii informaţiilor ca proces de sine stătător format din patru etape: PLAN-DO-CHECK-ACT (Planificare-Implementare-Verificare-Corectare), aşa cum se observă în figura nr. 4.7.

[2] La adresa http://www.bsi-global.com/

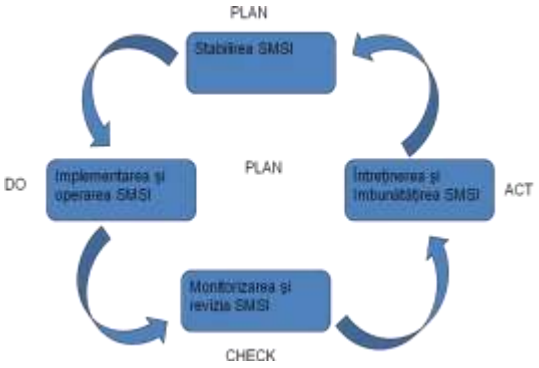


**Fig. 4.7 Etapele procesului de securitate a informaţiilor în standardul ISO 27001**

Sistemul de management al securităţii (SMSI) trebuie să faciliteze relaţia dintre procesele IT şi resursele implicate şi se concentrează asupra:

- nevoilor de securitate ale organizaţiei;
- strategiei adoptate de management pentru a satisface nevoile identificate;
- cuantificării rezultatelor;
- îmbunătăţirii strategiei în timp.

Implementarea unui SMSI nu se concentrează doar asupra aspectelor tehnice. Abordarea organizaţiei trebuie să fie holistică şi să aibă în vedere resursele umane, tehnologia şi procesele implicate.

Pe scurt, cele patru faze presupun:

*Plan (stabilirea SMSI)*

- Definirea scopului SMSI
- Definirea politicii de securitate
- Identificarea şi evaluarea riscurilor
- Stabilirea obiectivelor de control
- Documentarea proceselor

*Do (Implementarea şi operarea SMSI)*

- Formularea şi implementarea planului de management al riscurilor
- Implementarea controalelor identificate ca fiind necesare

*Check (Monitorizarea şi revizia SMSI)*

- Executarea procedurilor de monitorizare
- Reevaluarea periodică a eficacităţii SMSI
- Revizuirea nivelurilor acceptabile de risc şi a riscului rezidual
- Auditarea periodică a SMSI

*Act (Întreţinerea şi îmbunătăţirea SMSI)*

- Implementarea măsurilor de îmbunătăţire identificate
- Formularea acţiunilor corective şi preventive
- Validarea îmbunătăţirilor

Pentru *a fi în conformitate* cu ISO 27001, o organizaţie trebuie să aibă implementat şi documentat propriul sistem de management al securităţii informaţionale, în conformitate cu obiectivele de control.

*Certificarea* ISO este cea care oferă probe şi asigurări că o organizaţie a atins obiectivele controlului stipulate în standard. Aceasta presupune realizarea unui audit de către un evaluator independent care va verifica implementarea controalelor stipulate în Standard.

Procesul prin care se poate obţine conformitatea cu acest standard este similar cu obţinerea certificării ISO 9000. Etapele obţinerii acestei certificări pot fi sintetizate astfel:

- organizaţia decide să implementeze prevederile ISO 27001;

- odată luată această decizie, conducerea trebuie să desemneze o echipă care să elaboreze Politica de Securitate a organizaţiei;
- acest document trebuie revizuit, aprobat şi adus la cunoştinţa tuturor angajaţilor;
- organizaţia trebuie să stabilească apoi scopul certificării, care poate fi o componentă funcţională, un departament sau întreaga organizaţie;
- acest scop trebuie documentat, rezultând *ISMS Scope Document* (Scopul Sistemului de Management al Securităţii Informaţionale);
- în cadrul acestui Scop, trebuie identificate activele organizaţiei (şi valoarea asociată acestora) care trebuie protejate (Inventarul activelor);
- pentru acest inventar se va realiza Analiza de Risc: ameninţările, vulnerabilităţile şi impactul asupra activelor ce trebuiesc protejate;
- în baza rezultatului acestei analize se identifică riscul acceptabil;
- se documentează controalele care vor fi implementate pentru a menţine riscurile în limite acceptabile. Acestea vor fi preluate din Anexa standardului sau din *alte documente* recunoscute ca fiind „cele mai bune practici" ale domeniului;
- fiecare control considerat relevant trebuie să se adreseze unui risc;
- după completarea acestor etape se trece la implementarea controalelor;
- după implementarea controalelor se realizează Analiza breşelor pentru a identifica controalele care nu au fost implementate în totalitate sau pentru care utilizatorii necesită instruire;
- se implementează acţiunile corective prin care se remediază situaţiile identificate anterior;
- toată documentaţia se pune la dispoziţia unei firme sau a unui evaluator acreditate să ofere certificare în baza ISO 27001;
- auditorii firmei vor efectua o verificare formală prin care certifică existenţa fizică a controalelor documentate;
- dacă situaţia faptică este conformă cu documentaţia se eliberează certificatul de conformitate.

Implementarea unui SMSI se poate face cu resursele interne sau prin apelarea la o firmă ce oferă astfel de servicii. În primul caz activităţile implicate trebuie gestionate ca un proiect de sine stătător, după cum urmează:

1. Definirea proiectului
    a. Obiective
    b. Buget
    c. Active avute în vedere
    d. Controale/măsuri de securitate
2. Pregătirea proiectului
    a. Echipă
    b. Sisteme critice pentru afacere
    c. Identificarea ameninţărilor
    d. Identificarea unor controale posibile/aplicabile
3. Managementul proiectului
    a. Management propriu-zis
    b. Aspecte tehnice şi logice
4. Analiza riscurilor
    a. Selectarea unei metode
    b. Atribuirea de valori financiare activelor (punctul de vedere al unui contabil este binevenit pentru a nu fi contestate cifrele)
    c. Ameninţări-vulnerabilităţi
    d. Estimarea riscurilor

5. Reducerea/eliminarea/externalizarea riscurilor
    a. Selectarea măsurilor de protecţie
    b. Costuri asociate
    c. Eficienţă
    d. Soluţii alternative
6. Recomandări/livrabilele proiectului
    a. Riscuri acceptate
    b. Reducerea efectelor
    c. Documentarea procesului
    d. Aprobarea managementului

### 4.2.4 Exemple de politici de securitate

Încă de la început, trebuie să spunem că nu există două organizaţii care să aibă politici de securitate identice. Din multitudinea lor, vom prezenta, în continuare, o sinteză a formelor existente, reunind ceea ce se regăseşte în mai multe locuri.

De regulă, se începe cu un program de securizare a sistemelor informaţionale, situaţie în care se foloseşte conceptul de *politica programului de securitate informaţională*. Ea este acoperişul sub care se vor realiza politici tehnice de securitate, standarde şi norme de aplicare. Într-o unitate sunt necesare politici speciale pentru utilizarea Internetului şi a e-mail-ului, pentru accesarea de la distanţă a sistemului, pentru modurile de utilizare a unui sistem informatic, pentru protecţia informaţiilor ş.a. Aşadar, se poate spune că printr-o politică a programului de securitate informaţională se defineşte politica de ansamblu a organizaţiei în acest domeniu, precum şi responsabilităţile din sistem. În aceste condiţii, politicile ce se vor emite sunt componente esenţiale ale programului şi ele trebuie să răspundă la cinci obiective majore:

- *prevenire*: abilitatea de prevenire a accesului neautorizat la valorile patrimoniale ale organizaţiei;
- *asigurare*: asigurarea că politicile, standardele şi normele sunt în concordanţă cu intenţiile organizaţiei pe linia protejării valorilor patrimoniale informaţionale;
- *detectare*: abilitatea de a detecta intruşii din sistem şi de a lansa arsenalul de contramăsuri corespunzătoare;
- *investigare*: capacitatea de a folosi tehnici adecvate pentru obţinerea informaţiilor despre posibilii intruşi din sistem;
- *continuitate*: posibilitatea de a garanta funcţionarea neîntreruptă prin existenţa unui plan de acţiune în cazul dezastrelor, dezvoltat şi testat în organizaţie.

În continuare, vom face o descriere succintă a câtorva politici[3].

*Politica utilizării adecvate*

O astfel de politică trebuie să analizeze şi să definească utilizarea corespunzătoare a resurselor informatice din organizaţie. Utilizatorii trebuie să o citească şi semneze atunci când îşi exprimă intenţia de deschidere a unui cont de utilizator. Responsabilităţile utilizatorului pentru protejarea informaţiilor, memorate în conturile lor, trebuie să fie formulate explicit, ca şi nivelurile de utilizare a Internetului şi e-mail-ului. Politica, de asemenea, trebuie să răspundă următoarelor întrebări:

- Trebuie ca utilizatorii să citească şi copieze fişiere care nu sunt ale lor, dar la care au acces?

[3] Andress, M. – *Surviving Security: How to Integrate People, Process and Technology*, SAMS, Indianapolis, 2002, pp. 59-63.

King, C.M., Dalton, C.E., Osmanaglu, T.E. – *Security Arhitecture: Design, Deployment& Operations*,Osborne/McGraw-Hill, New York, 2001, pp. 18-26

- Trebuie ca utilizatorii să modifice fişierele la care au drept de scriere, dar nu sunt ale lor?
- Trebuie ca utilizatorii să facă copii ale fişierelor de configurare a sistemului, în scopul folosirii personale sau să le dea altora?
- Trebuie ca utilizatorii să folosească în comun conturile deschise?
- Trebuie ca utilizatorii să aibă dreptul de a face oricâte copii de pe softul care e procurat cu licenţă de utilizare?

*Politica privind conturile utilizatorilor*

Politica vizează normele după care se formulează cererile de deschidere a conturilor din sistem şi cum se efectuează întreţinerea lor. Este foarte utilă în organizaţiile mari, în care utilizatorii au conturi în mai multe sisteme. Este recomandată modalitatea de citire şi semnare a politicii de către utilizator. O astfel de politică trebuie să ofere răspunsuri la întrebări de genul:

- Cine are autoritatea aprobării cererilor de noi conturi-utilizator?
- Cui (angajaţilor, soţiilor/soţilor, rudelor, copiilor, vizitatorilor ş.a.) îi este permis să folosească resursele informatice ale organizaţiei?
- Poate un utilizator să aibă mai multe conturi în acelaşi sistem?
- Pot folosi utilizatorii în comun aceleaşi conturi?
- Care sunt drepturile şi obligaţiile utilizatorilor?
- Când va fi dezactivat şi arhivat un cont?

*Politica accesului de la distanţă*

Prin ea se definesc modalităţile de conectare de la distanţă la reţeaua internă a organizaţiei. Ea este necesară în organizaţiile care au utilizatori şi reţele dispersate geografic. Politica trebuie să răspundă următoarelor întrebări:

- Cine poate să aibă dreptul accesării de la distanţă?
- Ce metode sunt acceptate de organizaţie (dial-up, modem)?
- Este permis accesul din afară la reţeaua internă prin modem?
- Se impun anumite condiţii, cum ar fi soft antivirus şi de securitate, pentru accesarea de la distanţă?
- Pot alţi membri ai familiei să acceseze reţeaua?
- Sunt restricţii privind tipul datelor ce pot fi accesate de la distanţă?

*Politica protecţiei informaţiilor*

Printr-o astfel de politică se aduc la cunoştinţa utilizatorilor condiţiile prelucrării, stocării şi transmiterii informaţiilor sensibile. Scopul principal al acestei politici este asigurarea că informaţiile sunt protejate, în mod corespunzător, împotriva modificărilor sau dezvăluirii neautorizate. O astfel de politică trebuie semnată de toţi angajaţii. Ea trebuie să dea răspuns cel puţin la următoarele întrebări:

- Care sunt nivelurile de sensibilitate ale informaţiilor?
- Cine poate să aibă acces la informaţiile sensibile?
- Cum sunt stocate şi transmise informaţiile sensibile?
- Ce niveluri de informaţii sensibile pot fi listate pe imprimante publice?
- Cum trebuie să fie şterse informaţiile sensibile de pe suporturi (tocarea şi arderea hârtiilor, curăţirea discurilor ş.a.)?

*Politica gestionării firewall-urilor*

Politica gestionării firewall-urilor descrie modul în care sunt gestionate hardul şi softul şi cum sunt formulate şi aprobate cererile de schimbare din sistem. O astfel de politică trebuie să dea răspuns la următoarele întrebări:

- Cine are acces la sistemele firewall?
- Cine trebuie să primească solicitările de efectuare a schimbărilor în configuraţia firewall-urilor?

- Cine trebuie să aprobe efectuarea schimbărilor în configuraţia firewall-urilor?
- Cine poate să vadă normele şi listele de acces la configuraţia firewall-ului?
- Cât de des trebuie efectuată revizia firewall-urilor?

*Politica accesului special*

Prin ea se definesc condiţiile formulării cererilor de obţinere a dreptului de utilizare a unor conturi speciale din sistem (root, Administrator ş.a.). Ea trebuie să ofere răspunsurile la următoarele întrebări:

- Cine trebuie să primească cererile pentru acces special?
- Cine trebuie să aprobe cererile pentru acces special?
- Care sunt regulile parolelor pentru conturile cu acces special?
- Cât de des se schimbă parolele?
- Care sunt motivele sau situaţiile ce vor conduce la revocarea privilegiului de a avea acces special?

*Politica de conectare la o reţea locală*

Prin ea se definesc condiţiile adaugării de noi echipamente la reţea şi trebuie să răspundă la întrebările:

- Cine poate instala o resursă nouă în reţea?
- Cine trebuie să aprobe instalarea de noi echipamente?
- Cui trebuie să i se aducă la cunoştinţă faptul că au fost adăugate noi echipamente în reţea?
- Sunt unele restricţii pe linia securităţii în legătură cu echipamentele adăugate în reţea?

*Politica partenerului de afaceri*

O astfel de politică stabileşte ce măsuri de securitate trebuie să respecte fiecare companie parteneră. Ea este o politică cu atât mai necesară acum când organizaţiile oferă reţeaua lor internă partenerilor, clienţilor, furnizorilor. Deşi o astfel de politică este diferită de la o organizaţie la alta, ea, totuşi, trebuie să ofere răspunsuri la următoarele întrebări:

- I se cere fiecărei organizaţii să aibă scrisă o politică de securitate?
- Trebuie ca fiecare organizaţie să aibă un firewall sau alte echipamente de securitate a perimetrului?
- Cum se vor realiza comunicaţiile (linie închiriată, VPN prin Internet ş.a.)?
- Cum se vor formula cererile pentru accesarea resurselor partenerului?

*Politica managementului parolelor*

Deseori este inima politicilor de securitate dintr-o organizaţie. De regulă, ea reglementează problemele expirării parolelor, ale lungimii lor şi altor verificări necesare. Iată câteva recomandări de surprins printr-o astfel de politică:

- lungimea minimă a unei parole trebuie să fie de cel puţin opt caractere;
- parola nu trebuie să fie un cuvânt din dicţionar;
- ea trebuie să fie o combinaţie de litere şi simboluri speciale;
- parola trebuie să expire după o anumită perioadă de timp predeterminată;
- parolele administratorilor de reţele trebuie să expire mult mai repede şi trebuie să fie mai lungi;
- parolele din organizaţie trebuie să difere de cele folosite în alte sisteme;
- trebuie să fie păstrată o listă cu vechile parole pentru a preveni reutilizarea (ultimele şase parole nu trebuie să se repete);
- parolele utilizatorilor noi trebuie să fie unice şi greu de ghicit.

*Politica folosirii Internetului*

Politica utilizării Internetului, referită deseori prin acronimul I-AUP (*Internet Acceptable Use Policy*), este documentul prin care se detaliază modurile în care utilizatorii unei reţele a organizaţiei trebuie să folosească serviciul public Internet. Politica va descrie softul folosit

pentru filtrare şi blocare, cu scopul protejării organizaţiei, dar şi activităţile specifice permise, precum şi cine sunt beneficiarii acestor drepturi de acces şi cui i se interzic. Ea este bine să se refere şi la metodele de autentificare înaintea accesării Internetului în afara organizaţiei/ţării pentru a preveni personalul că foloseşte reţeaua organizaţiei în scopuri ilegale.

Protocoalele specifice acoperite printr-o politică de utilizare a Internetului sunt următoarele:

- *Poşta electronică*. Aceasta vizează toate formele de e-mail utilizate de o organizaţie, definindu-se ceea ce se acceptă a se folosi, declarându-se softul utilizat pentru filtrare şi scanare. Ea trebuie să sublinieze cerinţele specifice referitoare la datele ce nu pot fi transmise prin e-mail şi procedurile de urmat în cazul în care un utilizator primeşte mesaje cu date de acest gen. Prin această politică trebuie prevăzute şi măsurile luate în cazul nerespectării condiţiilor de utilizare a e-mail-ului;
- *Web*. Politica va prevedea condiţiile specifice de realizare a traficului Web. Cât timp WWW (World Wide Web) foloseşte HTTP-ul (HyperText Transport Protocol) pentru transferarea informaţiilor, prin politica de faţă vor fi definite clar tipurile de site-uri Web care sunt strict interzise, de genul celor porno, jocurilor de noroc ş.a.;
- *FTP*. Permiţând utilizatorilor accesul la FTP (File Transfer Protocol), se deschide calea descărcării cu uşurinţă în sistemul organizaţiei a viruşilor, dar şi transmiterea pe serverele din afara orgnizaţiei a unor informaţii confidenţiale. Pentru specialiştii organizaţiei trebuie să se asigure un nivel de acces FTP pentru efectuarea unor descărcări de fişiere în vederea actualizării softului existent, dar politica de faţă trebuie să stabilească autorizările de utilizare FTP;
- *Chat/IRC*. IRC-ul (Internet Relay Chat) este mai puţin folosit în mediul organizaţional faţă de alte programe de chat (dialoguri Internet), cum sunt Yahoo, ICQ şi AOL Instant Messenger (AIM). Astfel de programe sunt foarte riscante pentru organizaţie deoarece informaţiile sunt transmise unor servere externe fără o protecţie corespunzătoare. Politica de faţă trebuie să stabilească în ce măsură produsele de tip *chat* servesc intereselor organizaţiei.

În general, prin politica Internet se face referire la următoarele aspecte:

- acceptarea folosirii şi condiţiile de accept pentru:
  - descărcările de fişiere;
  - newsgroup-uri;
  - comunicarea datelor sensibile;
  - tipurile de fişiere ataşate;
  - dimensiunea mesajelor;
  - softul fără licenţă;
  - pachete de aplicaţii soft neaprobate;
  - exportul informaţiilor sensibile;
  - protecţia fişierelor;
  - protecţia împotriva viruşilor;
- managementul schimbărilor din sistem;
- practicile de stocare a datelor;
- siguranţă şi disponibilitate;
- protecţia informaţiilor prin clasificarea lor;
- controlul accesului;
- e-mail-ul şi datele ce pot fi reţinute/stocate în unitate;
- monitorizarea;
- excepţiile şi amendamentele politicii Internet.

După prezentarea exemplelor de mai sus, dar şi din studierea politicilor unor organizaţii pe linia securităţii informaţionale, se poate analiza cadrul general al unei politici de securitate pe site-ul:

www.windowsecurity.com/whitepapers/What_Do_I_Put_in_a_Security_Policy_.html

- Întocmiţi, pentru o organizaţie cunoscută de dvs., un set cât mai complet de recomandări ale politicilor de securitate aplicabile în cadrul acesteia.
- Comentaţi următorul citat:

Multe dintre organizaţiile pe care le cunosc sunt fortăreţe impresionante. Limbajul pe care-l folosesc e unul puternic defensiv şi apare oriunde e vorba de practicile CYA[1], de secrete păzite cu stricteţe şi de fişierele personale încuiate în seifuri, de activităţi referite drept „campanii", „războaie", "hărţuieli", ca şi în sintagmele împrumutate din sport, care descriu orice lucru în termeni de apărare sau atac. Multe organizaţii simt că trebuie să se apere chiar de proprii angajaţi cu reguli, ghiduri, cititoare de cartele pentru pontaj, politici şi proceduri în care apar specificate, exhaustiv, toate situaţiile comportamentale posibile. Una dintre organizaţiile în care am lucrat îşi întâmpină noii angajaţi cu o listă de 27 de abateri pentru care pot fi concediaţi imediat şi fără drept de apel – în plus, îi asigură şi că pot fi daţi afară la fel de uşor şi pentru alte delicte, nespecificate. Multe firme au ierarhii rigide, care împiedică oamenii să vorbească nestingheriţi între departamente, iar în marile companii există protocoale care definesc cine poate fi consultat, sfătuit sau criticat. Iar ca stare de spirit generală, ne temem de ce s-ar putea întâmpla dacă lăsăm aceste elemente organizaţionale să se recombine, reconfigureze, discute sincer unele cu altele. Suntem profund speriaţi de o destrămare a lucrurilor.

Wheatley, M. J., *Leadership and the New Science – Discovering Order in a Chaotic World,* Second Edition, Berrett-Koehler Publishers, San Francisco, 1999 – pp. 19-20

*[1] Cover Your Ass* – într-o traducere adaptată, "Acoperă-te cu hârtii!"

## Rezumat

Politicile de securitate sunt tratate ştiinţific prin *modelele de politici de securitate*, grupate în *modele de securitate multinivel* şi în *modele de securitate multilaterală*.

Cele mai cunoscute modele de politici de securitate sunt: modelul Bell-LaPadula (de securitate multinivel), modelul matricei de control al accesului, modelul Biba (modelul de integritate), compartimentarea şi modelul reţea, modelul zidului chinezesc, modelul BMA (British Medical Association).

Fără politici riguroase, *programele de securitate* vor fi aproape fără suport, ineficiente şi nu se vor alinia strategiei şi obiectivelor organizaţiei. *Politicile, standardele, normele şi procedurile* constituie fundaţia programului de securitate al organizaţiei. Politicile eficiente, clar formulate, vor servi proceselor de auditare şi eventualelor litigii. Combinând elementele specificate, o entitate poate implementa controale specifice, procese, programe de conştientizare şi multe altele, tocmai pentru a-i aduce un plus de linişte.

În afara declaraţiei *politicii* de securitate la nivelul top managerilor, există şi politici obligatorii, politici recomandate şi politici informative.

*Standardele* sunt obligatorii şi sunt implementate la nivel de unitate, pentru asigurarea uniformităţii. *Normele* sunt oarecum asemănătoare standardelor, referindu-se la metodologiile sistemelor securizate, numai că ele sunt acţiuni recomandate, nu obligatorii. *Procedurile* prezintă paşii detaliaţi ce trebuie să fie parcurşi pentru execuţia unei activităţi.

CAPITOLUL V

# Criptografia

Scopul criptografierii este de a proteja informaţiile transmise fără să poată fi citite şi înţelese decât de către persoanele cărora le sunt adresate. Obiectivele capitolului de faţă sunt:

- cunoaşterea principalelor tehnologii criptografice;
- dobândirea de cunoştinţe generale privind sistemele de criptare prin chei secrete (simetrice) şi prin chei publice (asimetrice).

## 5.1 Concepte de bază

*Algoritmul criptografic* este o procedură pas-cu-pas utilizată pentru cifrarea unui text clar şi descifrarea textelor cifrate.

*Cheia* sau *variabila de criptare* este o informaţie sau o secvenţă prin care se controlează cifrarea şi descifrarea mesajului.

*Cifrarea* este o transformare criptografică a unor caractere sau biţi.

*Criptograma* sau *textul cifrat* reprezintă un mesaj neinteligibil.

*Cifrul bloc* se obţine prin separarea textului iniţial în blocuri de câte *n* caractere sau biţi şi aplicarea unui algoritm şi a unei chei identice, *k*, pentru fiecare bloc. De exemplu, dacă textul unui mesaj iniţial, M, este împărţit în blocurile M1, M2, ... Mp, atunci:

$$C(M,k) = C(M1,k)\ C(M2,k) \ldots C(Mp,k)$$

în care blocurile din dreapta ecuaţiei sunt concatenate pentru a forma textul criptat.

*Codurile* sunt o transformare care operează la nivelul cuvintelor sau frazelor.

*Criptanaliza* este actul obţinerii textului clar sau a cheii din textul cifrat, care este folosit pentru obţinerea informaţiilor utile necesare acestui scop.

*Criptarea* înseamnă realizarea formei neinteligibile a unui mesaj pentru a nu fi utilizat de persoanele neautorizate să-l acceseze.

*Criptarea end-to-end* (de la un capăt la altul). Informaţiile criptate sunt transmise din punctul de origine la destinaţia finală. În varianta criptării prin chei simetrice, atât expeditorul, cât şi destinatarul folosesc aceeaşi cheie de criptare. Cheile asimetrice conduc la utilizarea unor valori diferite la cele două capete, expeditor şi destinatar sau emiţător şi receptor.

*Criptarea înlănţuită*. Fiecare entitate are chei comune cu cele două noduri vecine din lanţul de transmisie. Astfel, un nod primeşte mesajul criptat, de la predecesor, îl decriptează, după care îl recriptează cu o altă cheie, care este comună cu nodul succesor. După aceasta, mesajul este transmis nodului succesor, unde procesul se repetă până la destinaţia finală.

*Criptografia* este arta şi ştiinţa ascunderii semnificaţiei unei comunicări împotriva unor interceptări neautorizate. Cuvântul are rădăcini greceşti, însemnând scriere ascunsă – *kryptos graphein*.

*Criptologia* reuneşte criptografia şi criptanaliza.

*Decriptarea* este procesul prin care un text cifrat este transformat într-un mesaj inteligibil.

*Sistemul de criptare* este un set de transformări din spaţiul mesajului clar la cel al textului cifrat.

*Stenanografia* este o formă de comunicare secretă prin care se încearcă ascunderea mesajului secret. Prin ea, într-o imagine digitală, cel mai puţin semnificativ bit al fiecărui cuvânt poate fi folosit pentru a forma un mesaj fără să provoace o schimbare evidentă a imaginii. În general, ascunderea mesajului într-un anumit mediu, cum ar fi un document, o imagine, o înregistrare sonoră sau video se numeşte *steganografie*. Oricine ştie că mediul respectiv conţine un mesaj secret poate să-l identifice, presupunând că ştie metoda de codificare.

*Textul clar* este forma inteligibilă de prezentare a unui mesaj, astfel încât el să fie accesibil oricui.

## 5.2 Scurt istoric al criptografiei

Scrierea secretă s-a întâlnit sub diverse forme în urmă cu 5000 de ani, la egipteni, prin scrierea *hieroglifică*, în greacă având semnificaţia de gravare sacră. Hieroglifele s-au transformat în scrieri *hieratice*, formă stilizată de prezentare, mult mai simplu de utilizat.

Cam cu 400 de ani î.C., spartanii au folosit criptografia militară sub forma unei fâşii de papirus sau pergament înfăşurată în jurul unui băţ. Mesajul de codificat se scria de-a lungul băţului (de sus în jos sau invers) pe fâşia înfăşurată care, după desfăşurare, se transmitea la destinatar, ceea ce însemna o panglică plină de caractere aleatoare, firesc, fără noimă. Când ea ajungea la destinaţie şi se înfăşura pe un băţ de acelaşi diametru, se afla mesajul iniţial.

Cu 50 de ani î.C., Iulius Cezar, împăratul Romei, a folosit *cifrul substituţiei* pentru a transmite mesaje lui Marcus Tullius Cicero. Printr-o astfel de tehnică, literele alfabetului latin erau înlocuite cu altele ale aceluiaşi alfabet. Deoarece se folosea numai un singur alfabet, cifrul s-a numit *substituţie monoalfabetică*. Acest cifru particular presupunea schimbarea literelor alfabetului printr-o deplasare la dreapta cu trei poziţii, astfel A devenea D, B este E ş.a.m.d., conform secvenţei din figura 5.1.

Substituţia unei litere în alta, aflată la dreapta peste trei poziţii, a făcut ca metoda să mai fie numită şi metoda de substituţie *C3*. Fiind invenţia lui Cezar, metoda este alteori întâlnită şi sub numele *inelul lui Cezar*.

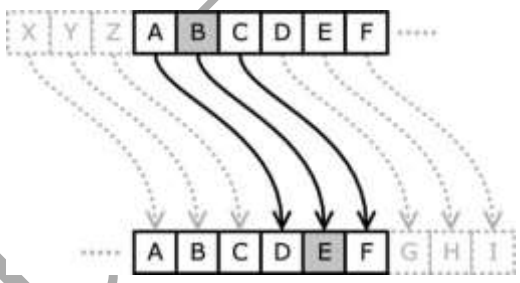


**Fig. 5.1 Cifrul substituţiei C3 al lui Cezar**

În general, sistemul lui Cezar de criptare poate fi scris sub forma:

$$T_i = S_n (C_i),$$

unde $T_i$ sunt caracterele textului criptat, $S_n$ este o transformare prin substituţie monoalfabetică, iar $C_i$ sunt caracterele textului clar. Iată un exemplu:

AM DAT UN EXEMPLU
↓ ... ↓
DP GDW XQ HAHPSOX

folosindu-se cifrul C3, conform substituţiilor din figura 5.1.

În ultimii 500 de ani discul a jucat un rol important în criptografie. De exemplu, în Italia, în jurul anilor 1460, Leon Battista Alberti a realizat discurile cifru pentru criptare, conform figurii 5.2. Se foloseau două discuri concentrice. Fiecare disc are alfabetul tipărit pe circumferinţa lui, iar prin rotirea unui disc faţă de celălalt, o literă a unui alfabet devenea altă literă în celălalt alfabet.

Leon Battista Alberti

Thomas Jefferson

**Fig. 5.2 Discuri cifru**

Ulterior, fiind buni matematicieni, statisticieni şi lingvişti, arabii au inventat criptanaliza. Scrierea lor criptată a fost o taină de-a lungul secolelor. De exemplu, filosoful arab Al-Kindi a scris un tratat, în secolul IX, care a fost descoperit în 1987, intitulat „Manuscrisul descifrării mesajelor criptate".

În 1790, Thomas Jefferson a realizat un echipament de criptare folosind un set de 26 discuri ce se puteau roti individual, prin tehnici speciale de utilizare, astfel încât descifrarea să fie aproape imposibilă.

Invenţiile s-au înmulţit teribil în ultimele secole, cel de-al doilea război mondial având în uz pe cele mai performante pentru acele vremuri. Dintre acestea au rămas în istorie „maşina japoneză de purpură" şi maşina germană „Enigma", ca fiind cele mai performante, dar şi ele au fost sparte, la figurat.

Informaţi-vă în detaliu asupra unui moment din istoria criptografiei care v-a reţinut atenţia.

## 5.3 Tehnologii criptografice

Cele două tipuri principale de tehnologii criptografice sunt *criptografia prin chei simetrice* (chei secrete sau chei private) şi *criptografia prin chei asimetrice* (chei publice).

În criptografia prin chei simetrice, atât emiţătorul, cât şi receptorul folosesc o cheie secretă comună. În cazul criptografiei prin chei asimetrice, transmiţătorul şi receptorul folosesc în partaj o cheie publică şi, individual, câte una privată.

Pentru înţelegerea metodelor de criptare şi a tehnicilor folosite în criptanaliză, o trecere în revistă a operaţiunilor fundamentale de criptare este strict necesară. Vom constata că, de-a lungul celor patru mii de ani, evoluţiile au fost spectaculoase şi înţelepciunea acelor vremuri ne încântă şi acum. Plăcerea este cu atât mai mare, cu cât concepte şi tehnici foarte vechi se regăsesc în sistemele moderne de criptare, firesc, beneficiind de acumulările de-a lungul timpului.

### 5.3.1 Substituţia

În urmă cu 2000 de ani, Iulius Cezar a folosit metoda substituţiei simple pentru a-şi crea propriul său sistem de criptare, cunoscut sub numele de *cifrul lui Cezar*. Se pare că el a fost

printre primii comandanţi ai imperiilor care şi-a iniţiat generalii în taina transmiterii mesajelor criptate. Cifrul lui Cezar este o submulţime a cifrului polialfabetic al lui Vigenère. În cifrul lui Cezar, caracterele mesajului şi numărul de repetiţii ale cheii sunt însumate laolaltă, modulo 26. În adunarea modulo 26, literelor alfabetului latin, de la A la Z, li se dau valori de la 0 la 25 (tabelul 5.1). Pentru cheie trebuie să se ofere doi parametri: *D*, numărul literelor ce se repetă, reprezentând chei; *K*, având rolul de cheie.

*Tabel nr. 5.1 – Corespondenţa litere-valori numerice*

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Pentru a înţelege modul de funcţionare, să presupunem că D = 3 şi K = DAC, iar mesajul este STRICT SECRET. Atribuind valori numerice mesajului, din tabelul valorii literelor (tabelul 5.1), rezultă:

| 18 | 19 | 17 | 8 | 2 | 19 | | 18 | 4 | 2 | 17 | 4 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | T | R | I | C | T | | S | E | C | R | E | T |

Valorile numerice ale cheii sunt:

| 3 | 0 | 2 |
|---|---|---|
| D | A | C |

După aceste corespondenţe, cheia repetată 302 se adaugă literelor mesajului, astfel:

| Cheia repetată: | 3 | 0 | 2 | 3 | 0 | 2 | 3 | 0 | 2 | 3 | 0 | 2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mesajul: | 18 | 19 | 17 | 8 | 2 | 19 | 18 | 4 | 2 | 17 | 4 | 19 |
| Echivalentul numeric al textului criptat: | 21 | 19 | 19 | 11 | 1 | 21 | 21 | 4 | 4 | 20 | 4 | 21 |
| Textul criptat: | V | T | T | L | C | V | V | E | E | U | E | V |

Convertirea numerelor în literele aferente alfabetului conduce la textul criptat, aşa cum reiese de mai sus: VTTLCV VEEUEV.

În cazul cifrului lui Cezar, D este 1 şi cheia este D(3). Luând exemplul anterior, cu mesajul STRICT SECRET, convertit în valorile numerice aferente poziţiilor literelor în alfabet, la care se adaugă valoarea cheii 3, rezultă:

| Cheia repetată: | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mesajul: | 18 | 19 | 17 | 8 | 2 | 19 | 18 | 4 | 2 | 17 | 4 | 19 |
| Echivalentul numeric al textului criptat: | 21 | 22 | 20 | 11 | 5 | 22 | 21 | 7 | 5 | 20 | 7 | 22 |
| Textul criptat: | V | W | U | L | F | W | V | H | F | U | H | W |

Convertind înapoi numerele în literele corespunzătoare alfabetului, se realizează textul criptat, care înseamnă, de fapt literele mesajului original deplasate spre dreapta cu trei poziţii. Atunci când sumele valorilor cheii şi ale numărului aferent literelor sunt mai mari sau egale cu 26, se determină modulo 26 din sumă, adică rezultatul final este obţinut prin scăderea din sumă a numărului 26.

*Exemplu*:

D = 3, K = DIO, iar mesajul este PAZA, rezultatele fiind:

– valorile numerice atribuite literelor mesajului sunt:

| 15 | 0 | 25 | 0 |
|---|---|---|---|
| P | A | Z | A |

– valorile numerice ale cheii K sunt:

| 3 | 8 | 14 |
|---|---|---|
| D | I | O |

Cheia repetată 3 8 14 se adaugă literelor mesajului, astfel:

| Cheia repetată: | 3 | 8 | 14 | 3 |
|---|---|---|---|---|
| Mesajul: | 15 | 0 | 25 | 0 |
| Echivalentul numeric al textului criptat: | 18 | 8 | 39 | 3 |

Valoarea 39 nu are echivalent în alfabetul latin, pentru că, aşa cum am menţionat, numerotarea celor 26 de litere se face de la 0 la 25. În acest caz, se calculează modulo 26 din 39,

rezultând valoarea 13, iar noul echivalent numeric al textului criptat este 18 8 13 3. Textul criptat aferent este SIND.

Cifrurile de mai sus pot fi descrise prin ecuaţia generală:

$$C = (M + b) \bmod N,$$

în care:

*b* este un număr întreg fix;

*N* este numărul literelor din alfabet;

*M* este mesajul textului clar în formă numerică;

*C* este textul criptat în formă numerică.

Revenind la monosubstituţia folosită de Cezar, în care orice literă este înlocuită prin alta situată mai în dreapta cu *n* poziţii (varianta Cezar, n = 3, A = D, B = E, C = F ş.a.m.d). O astfel de criptare este uşor atacabilă prin analiza frecvenţelor de apariţie a caracterelor. În fiecare limbă se ştie care sunt frecvenţele literelor din textele scrise. În limba engleză, frecvenţele apariţiei literelor sunt prezentate în tabelul 5.2. Cifrul lui Cezar, bazându-se pe substituţia simplă sau monoalfabetică, este uşor de „spart" pentru că un caracter este înlocuit de altul şi această schimbare este valabilă în tot textul, iar analiza frecvenţelor ne va conduce la caracterele adevărate ale textului clar.

*Tabel nr. 5.2 – Frecvenţa apariţiei literelor în limba engleză*

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 79 | 9 | 30 | 44 | 130 | 28 | 16 | 35 | 74 | 2 | 3 | 35 | 25 | 78 | 74 | 27 | 3 | 77 | 63 | 93 | 27 | 13 | 16 | 5 | 19 | 1 |

Cifrurile polimorfice sunt realizate prin apelarea la cifruri bazate pe substituţia multiplă. De exemplu, dacă se folosesc patru alfabete pentru substituţie, definite de cel ce intenţionează să cripteze, prima literă din textul clar este înlocuită cu prima literă din primul alfabet, a două literă a textului clar este înlocuită cu prima literă a celui de-al doilea alfabet, a treia literă a textului clar este înlocuită cu prima literă a celui de-al treilea alfabet, a patra literă a textului clar este înlocuită cu prima literă a celui de-al patrulea alfabet, a cincea literă a textului clar este înlocuită cu a doua literă a primului alfabet ş.a.m.d. Exploatând această metodă, Balise de Vigenère, diplomat francez născut în 1523, a dus mai departe realizările lui Alberti Trithemius şi Porta, elaborând un cifru polialfabetic foarte solid pentru acele vremuri. El folosea 26 de alfabete.

Un exemplu de cifru polialfabetic este redat în figura 5.3, în care se utilizează patru alfabete.

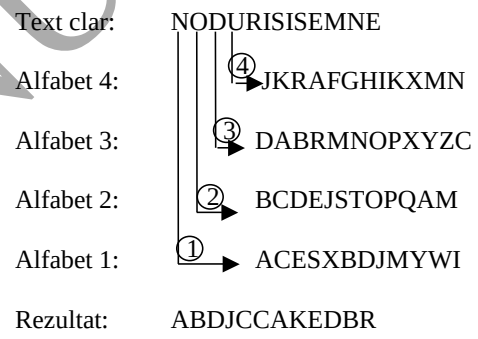


**Fig. 5.3 Exemplu de cifru polialfabetic**

## 5.3.2 Transpoziţia (permutarea)

Pentru a înţelege transpoziţia sunt necesare câteva informaţii acumulate anterior, cum ar fi: introducere în sistemele criptate, permutări şi matrice. Transpoziţia se bazează pe o idee foarte simplă. În loc să înlocuieşti un caracter cu altul, e mult mai simplu să înlocuieşti ordinea caracterelor. În plus, acest cifru nu va fi uşor descoperit prin analiza frecvenţei apariţiei unor caractere. De asemenea, cheia pentru un astfel de cifru nu este standard. În locul unei liste a

substituţiilor alfabetice, putem vorbi de o schemă a ordinii. De exemplu, dacă ordinea într-un text clar este 1, 2, 3, 4, 5, 6, într-un text cu transpoziţie poate fi 2, 5, 4, 3, 6, 1, ceea ce înseamnă că primul caracter al textului criptat este al doilea din textul clar, al doilea caracter este al cincilea ş.a.m.d. De exemplu, cuvântul SCOALA devine CLAOAS.

Permutările unui astfel de cifru acţionează într-o matrice bloc, ceea ce înseamnă că va fi o matrice de tip „patul lui Procust", în care tot ceea ce nu încape într-o linie se va alinia în cea următoare ş.a.m.d. De exemplu, mesajul PROTECTIE SI TEAMA, într-o matrice cu patru coloane devine:

PROT
ECTI
ESIT
EAMA

În această variantă, citindu-se în ordinea liniilor, mesajul criptat va fi:

PROT ECTI ESIT EAMA.

Dacă se va lucra la coloane, prin folosirea transpoziţiei controlate prin chei, rezultă altceva. De exemplu, dacă asupra coloanelor se aplică regula 1, 2, 3, 4 = 4, 2, 1, 3 – exemplul anterior devine:

EAMA
ECTI
PROT
ESIT,

ceea ce va însemna că textul criptat, citit pe linie, este:

EAMA ECTI PROT ESIT.

Aceleaşi reguli se pot aplica asupra coloanelor sau, şi mai interesant, asupra liniilor şi coloanelor.

Combinarea transpoziţiei cu substituţia poate să conducă la variante aproape imposibil de spart.

### 5.3.3 Cifrul lui Vernam

Cifrul lui Vernam constă într-o cheie constituită, pe criterii aleatoare, dintr-un set de caractere nerepetitive. Fiecare literă a cheii se adaugă modulo 26 la o literă a textului clar. În această variantă, fiecare literă a cheii se foloseşte o singură dată pentru un singur mesaj şi nu va mai putea fi folosită niciodată. Lungimea şirului de caractere a cheii este egală cu lungimea mesajului. Metoda este foarte utilă pentru criptarea mesajelor scurte. În cele ce urmează, vom prezenta un exemplu:

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Text clar: | CRIPTAREDATE | 2 | 17 | 8 | 15 | 19 | 0 | 17 | 4 | 3 | 0 | 19 | 4 |
| Cheie Vernam: | XYZABCPQRJDW | 23 | 24 | 25 | 0 | 1 | 2 | 15 | 16 | 17 | 9 | 3 | 22 |
| Suma aparentă: | | 25 | 41 | 33 | 15 | 20 | 2 | 32 | 20 | 20 | 9 | 22 | 26 |
| Modulo 26 din sumă: | | 25 | 15 | 7 | 15 | 20 | 2 | 6 | 20 | 20 | 9 | 22 | 0 |
| Textul criptat: | | Z | P | H | P | U | C | G | U | U | J | W | A |

Cifrul lui Vernam a fost preluat şi valorificat de compania americană AT&T.

### 5.3.4 Cifrul carte

Un astfel de cifru apelează la diverse surse, cum ar fi o carte, pentru a cripta un text clar. Cheia, cunoscută de transmiţător şi potenţialul receptor, poate fi formată din pagina cărţii şi numărul rândului de pe pagina în care se află textul.

### 5.3.5 Codurile

Codurile sunt utilizate pentru a putea transmite unele construcţii predefinite din domenii diverse, de regulă din afaceri, prin intermediul lor. De exemplu, codul 500 ar putea să însemne „De efectuat recepţia cantitativă şi calitativă a mărfurilor expediate". Odată cu generalizarea serviciilor telegrafice, pentru diminuarea preţului pe mesaj, s-a apelat la un astfel de sistem. De regulă, sunt două rânduri de cărţi: una conţine ordinea crescătoare a codurilor şi, în dreptul lor, semnificaţia în clar; alta conţine semnificaţia în clar, în ordine alfabetică şi codul corespunzător.

### 5.3.6 Ascunderea informaţiilor

Ascunderea informaţiei s-a practicat de mii de ani, rădăcinile ei numindu-se camuflare. Se pare că prima consemnare de acest gen îi aparţine lui Herodot, care a descris o astfel de tehnică din timpul războiului dintre greci şi persani, când, pentru transmiterea secretă de mesaje, unui sol i se rădea părul de pe cap, apoi pe piele se tatua mesajul secret. După ce îi creştea părul era trimis cu mesajul la un anumit receptor, unde, după tundere, se citea conţinutul mesajului.

În vechea Chină se folosea o altă tehnică a ascunderii informaţiilor. „Cheia" consta într-o matriţă de hârtie, în două exemplare – unul pentru emiţător, celălalt pentru receptor, cu perforaţii ce se urmăreau într-o anumită ordine, firesc ele fiind plasate într-o totală dezordine. Emiţătorul punea matriţa pe o coală de hârtie şi scria mesajul în ordinea ştiută a perforaţiilor, după care, renunţându-se la matriţă, se continua scrierea pe coala de hârtie pentru închiderea textului sau mesajului secret printre caracterele textului liber, numit text clar. Tehnica a fost preluată, în secolul XVI, de matematicianul italian Cardan şi din această cauză este cunoscută în criptografie sub numele *grila lui Cardan*.

Doar pentru frumuseţea textului scris de profesorul Dumitru Năstase[1], vă prezentăm constatarea sa:

„Modul „iniţiatic" de a comunica mesajele lor cele mai profunde, utilizat de scrierile şi actele noastre medievale, trebuie confruntat cu un alt cod, despre caracterul simbolic al căruia nu se îndoieşte nimeni, şi anume cel heraldic. Cu condiţia, însă, de a şti că şi simbolurile heraldice ale Ţărilor Române conţin elemente care se coroborează cu cele din textele scrise, dar care n-au putut fi utilizate ca mărturii, pentru bunul motiv că au fost, în cele mai multe cazuri, *atât de bine disimulate sub diferite camuflaje* (subl. ns.), încât au scăpat cu desăvârşire specialiştilor.

Exemplul cel mai însemnat şi mai frapant, de asemenea „necunoscută", e cel al *vulturului bicefal* (subl. ns.). Acest ilustru însemn a fost unanim socotit – şi din păcate mai este încă – drept străin heraldicii româneşti, în care n-ar fi făcut până târziu, decât apariţii sporadice. De aceea şi cazurile cunoscute au fost studiate fiecare în parte, atribuindu-li-se de fiecare dată o origine şi un specific străine istoriei româneşti.

În realitate, vulturul bicefal este neîncetat prezent – şi la loc de cinste – în heraldica noastră, unde are o evoluţie internă dintre cele mai interesante, *din veacul XIV şi până la 1821* (subl. ns.). Arborat mai întâi deschis de domnii noştri, formele lui „explicite" vor fi mai târziu dublate cu altele, cum am spus, *ascunse*, şi unele şi altele stabilind însă o lungă continuitate conştientă, grea de sensuri, a vulturului bicefal în heraldica românească."

Iată, aşadar, o sublimă tehnică de ascundere a informaţiei prezentă de secole în heraldica românească prin apariţii deosebit de interesante pe o mare varietate de obiecte sau în iconografia vremurilor. Aceasta este o probă vădită de steganografie, care înseamnă ascunderea informaţiei în faţa ochiului neavizat.

În vremurile noastre, ascunderea informaţiei a devenit interesantă pentru o paletă largă de utilizatori. Anii 1990 au consemnat interesul producătorilor de la Hollywood pentru găsirea unui

[1] Năstase, D. – *„Necunoscute" ale izvoarelor istoriei româneşti*, Extras din Anuarul Institutului „A. D. Xenopol", XXX, 1993, Ed. Academiei Române, Iaşi, p. 489.

mecanism de protejare a copyright-ului, interes regăsit şi în domeniul militar pentru comunicaţii care să nu dea nimic de bănuit interceptorilor neautorizaţi. Şi populaţia era îngrijorată de agresivitatea discuţiilor guvernamentale în legătură cu nevoia de a controla comunicaţiile criptate. Toate acestea au condus la o puternică dezvoltare a *ascunderii informaţiei*.

Ascunderea modernă a informaţiei viza ascunderea unor mesaje secrete într-un fişier audio MP3 sau seria unui program era încapsulată printre instrucţiunile executabile.

Interesele Hollywoodului vizau marca de înregistrare a copyright-ului, care să fie ascunsă percepţiei obişnuite din bucăţile audio digitale, video şi ale lucrărilor de artă. Ele sunt fie *filigrane* (*watermarks*), care reprezintă mesajul copyright-ului ascuns, fie *amprente* (*fingerprints*), care semnifică serii ascunse.

#### 5.3.6.1 Steganografia

Steganografia este arta ascunderii existenţei unui mesaj pe un anumit suport. În limba greacă *steganos* înseamnă acoperit şi *graphein* – a scrie. Aşadar, scriere camuflată/ascunsă.

Prin steganografie se exprimă interesul pentru confidenţialitate, întrucât scopul ei este de a include mesaje într-un anumit mediu astfel încât să rămână insesizabil. Un model conceptual cunoscut, propus de Simmons[2], este următorul. Alice şi Bob sunt în puşcărie şi doresc să pună la cale un plan de evadare; comunicarea dintre ei este posibilă doar prin intermediul gardianului Willie, dar dacă acesta va afla ce uneltesc pedeapsa lor va fi şi mai dură. Aşadar, ei trebuie să găsească o modalitate de a ascunde mesajele secrete într-un inocent text care să le acopere. Aşa cum se procedează în criptografie, presupunem că mecanismul folosit este cunoscut de gardian, aşa că din motive de securitate, ei trebuie să apeleze la o cheie secretă comună pe care doar ei să o ştie şi să o folosească.

David Kahn, autorul cărţii *The Codebreakers*, citează ca formă embrionară a steganografiei un caz din *Istoriile* lui Herodot, în care mesajul a fost scris pe scândurile unei mese, prin gravare, apoi s-a acoperit textul cu ceară, fără să dea nimic de bănuit. Doar primitorul mesei va şti taina.

O altă metodă constă în preluarea primei litere a fiecărui cuvânt dintr-un text, formând mesajul ascuns.

Alte metode de ascundere se realizează folosind cerneala invizibilă şi micropunctele. *Micropunctele* sunt fotografii de dimensiunea unui „**.**” (punct) care poate să reproducă perfect o pagină de text. În timpul celui de-al doilea război mondial, germanii au dezvoltat această tehnologie, plasând sute de micropuncte pe scrisori de dragoste, către ai casei, în comunicările de afaceri ş.a. Directorul F.B.I., J. Edgar Hoover le-a numit „capodopere ale spionajului”.

În steganografia actuală există o mare varietate de tehnici. Una din ele *ascunde mesajele printre biţii imaginilor digitale*. Imaginile sunt reprezentate printr-o formă matriceală de *pixels* (***p****icture* ***x*** ***el****ements*), însemnând puncte din care se realizează imaginea. O imagine foto-CD Kodak are 3072 x 2048 pixeli, dar o imagine mai puţin clară poate să aibă 400 x 300 pixeli. Fiecare pixel este codificat printr-o secvenţă de biţi care fixează culoarea. În cea mai simplă formă, codificarea se realizează prin 24 de biţi, care, conform sistemului RBG – Red (roşu), Blue (albastru), Green (verde) –, înseamnă atribuirea a câte 8 biţi pentru fiecare culoare. Cei 8 biţi, care formează un octet, determină realizarea a 256 de posibilităţi; prin combinarea lor rezultă aproximativ 17 milioane de nuanţe de culori. Printr-o astfel de variantă se pot obţine performanţe foarte mari, dar, unor biţi li se poate da o altă destinaţie, pentru a se codifica mesaje scurte, fără să afecteze semnificativ imaginea.

În structura octeţilor, valoarea biţilor este diferită în alcătuirea imaginii finale. De regulă, ultimul bit, cel mai din dreapta, nu are efect semnificativ, întrucât, în cel mai rău caz schimbă culoarea cu unu în spectrul general al culorii, pe când cel din stânga are influenţă mult mai mare

[2] Simmons, G.J. – „The Prisoners’ Problem and the Subliminal Channel”, in *Proceedings of Crypto ‘83*, Plenum Press (1984), pp. 51-67.

în schimbarea culorii. Se spune că schimbarea bitului cel mai nesemnificativ al unei culori ar fi echivalent cu schimbarea secundarului unui ceas cu o secundă. Ce înseamnă o oră cu o secundă în plus sau în minus!?!

Biţii succesivi ai mesajului secret pot fi plasaţi pe poziţia biţilor cel mai puţin semnificativi ai octeţilor următori, fără să altereze semnificativ imaginea. Putem face un calcul simplu al potenţialilor biţi utilizabili pentru ascunderea mesajului, ştiut fiind faptul că sunt 400 x 300 pixeli, fiecare cu câte 3 octeţi (de la care se pot valorifica 3 biţi, câte unul de la fiecare octet), rezultând 400 x 300 x 3 = 360.000 biţi. Alocând câte 8 biţi pentru un caracter al textului, rezultă că se poate realiza un mesaj lung de 360.000 : 8, adică 45.000 de caractere.

Pentru exemplificare, să considerăm că primii 3 octeţi (24 biţi) ai imaginii au următoarea structură:

| 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | 1 | 1 | 1 | 1 | 0 | 0 | 1 | **0** | 1 | 1 | 1 | 0 | 0 | 0 | 0 | **1** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Să analizăm efectul scrierii mesajului ABC, folosind biţii cei mai nesemnificativi, a opta poziţie, marcaţi cu bold. În codul ASCII:

A este 01000001

B este 01000010

C este 01000011

Deci, mesajul ABC înseamnă şirul

| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Din păcate, dat fiind numărul mic de biţi disponibili în exemplul dat, doar 3, înseamnă că vom putea plasa numai primii trei biţi ai literei A, adică 010, astfel:

| 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | 1 | 1 | 1 | 1 | 0 | 0 | 1 | **1** | 1 | 1 | 1 | 0 | 0 | 0 | 0 | **0** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Se poate observa că doar doi biţi din cei trei mai puţin semnificativi s-au schimbat, respectiv ultimul bit al celui de-al doilea octet şi al celui de-al treilea. Pentru decodificarea mesajului, se vor extrage doar biţii aflaţi pe a opta poziţie a fiecărui octet, ceea ce cu calculatorul este o procedură foarte simplă. Printr-o astfel de operaţiune biţii iniţiali ai imaginii nu mai pot fi reconstituiţi.

Pentru cei ce doresc să se obişnuiască cu mediul de lucru al steganografiei, recomandăm vizitarea site-ului *http://members.tripo.com/steganography/stego/s-tools4.html*. De aici, intraţi pe *Software* şi veţi putea găsi o mare varietate de programe din acest domeniu, prin care puteţi afla ce imagini conţin mesaje ascunse sau, dacă doriţi, vă ascundeţi texte după imagini sau invers.

Pentru a reda efectul steganografiei, al scrierii textelor ascunse prin imagini, în figura 5.4, redăm fotografiile Pământului efectuate de cosmonauţii misiunii Apolo 17, pe 7 decembrie 1972; imaginea din stânga este fotografia normală, iar cea din dreapta are inclus un text de peste 30 de pagini.

Totuşi, steganografia nu este la fel de sigură cum este criptarea prin chei, dar ea a fost (şi este) folosită în multe acte criminale. Ea poate servi şi la ascunderea existenţei unui fişier pe hard disk pentru toţi cei ce nu-i ştiu numele şi parola.

a) Înainte de includerea textului b) După includerea textului

**Fig. 5.4 Imaginea pământului de pe Apolo 17, diferite din punct de vedere al conţinutului**

- Identificaţi pe Internet programe care folosesc tehnica LSB pentru transmiterea mesajelor ascunse.
- Credeţi că există situaţii în activitatea organizaţiilor economice în care să fie utilă folosirea steganografiei? Exemplificaţi, justificaţi.

### 5.3.6.2 Filigranarea

Un filigran este un model distinct încapsulat într-un document, imagine, video sau audio de către cel ce se află la originea datelor. Filigranul poate avea câteva scopuri, printre care: indicarea proprietarului datelor, ţinerea evidenţei copiilor datelor, verificarea integrităţii datelor. Filigranele folosite în bancnote au scopul de a întări încrederea posesorilor că se află în faţa banilor originali şi nu a unora contrafăcuţi, scopul fiind de securizare împotriva unor tentative de falsificare. Un filigran poate fi invizibil cu ochiul liber sau insesizabil de ureche, dar sunt mijloace de detectare şi extragere a lui pentru a se verifica autenticitatea datelor sau a se afla sursa lor.

Datele filigranate sunt o funcţie a unui identificator şi/sau cheie care este unic(ă) pentru autor. Aceste valori sunt necesare pentru detectarea sau extragerea filigranului. Dacă mai multe copii ale datelor sursă au fost filigranate separat, fiecare dintre ele va fi prelucrată cu o cheie proprie, ceea ce conduce la concluzia că fiecare copie are „amprenta" ei. Prin ţinerea evidenţei fiecărei chei folosite pentru fiecare beneficiar este uşor de urmărit cine a încălcat dreptul de proprietate.

Se folosesc filigrane fragile sau solide. Cele fragile sunt mai uşor de schimbat, dar sunt folosite doar pentru a vedea dacă datele au fost schimbate, în timp ce filigranele robuste rezistă tuturor manipulărilor şi mutărilor la care sunt supuse.

Filigranarea este similară cu steganografia şi se bazează pe tehnici de proiectare apropiate. De exemplu, o metodă de filigranare, aplicabilă datelor digitale, constă în inserarea unui ID şi a unei chei în structura unui fişier imagine, sunet, video. Dacă ID-ul şi cheia sunt cunoscute, este uşor de văzut dacă ele sunt prezente printre date.

În spaţiul cibernetic, filigranele sunt folosite pentru stabilirea încălcărilor dreptului de autor. *Digimarc Technologies* (*www.digimarc.com* şi *www.digimarc-id.com*) are un produs pentru protejarea imaginilor puse de proprietar în propriul său site. Deţinătorii copyright-ului inserează filigranul lor, folosind *PhotoShop* al *Adobe*-ului, sau un alt editor de imagine care încorporează tehnologia *Digimarc*. Când receptorul foloseşte acelaşi editor pentru vizualizarea imaginilor va fi afişat simbolul de copyright al autorului. Prin selectarea simbolului se realizează legătura cu *Digimarc*, de unde vor afla cine este deţinătorul dreptului de autor. De asemenea, *Digimarc* are un motor de căutare, *MarcSpider*, care caută imagini filigranate furate de la autorii lor.

*Aris Technologies, Inc.* (*www.aris-techno.fr/*) a realizat o tehnologie similară împotriva piraţilor de muzică. Softul lor, *MusiCode*, încapsulează informaţii-sursă (cum sunt titlul, artistul, compania de înregistrare) în fişierul audio. Softul este folosit pe Internet printr-un motor de căutare care combate piraţii de melodii din acest mediu.

Realizări sunt foarte diverse, dar scopul prezentării de faţă este doar acela de a informa pe cei interesaţi de protejarea creaţiei lor că au la dispoziţie instrumente de apărare.

Identificaţi pe Internet programe cu ajutorul cărora să introduceţi filigrane în imaginile digitale.

### 5.3.6.3 Securitatea tipăririi hârtiilor de valoare

Abordarea acestui subiect în cărţile de protecţie şi securitate este aproape inexistentă. Singurele materiale deosebit de interesante poartă semnătura lui Renesse[3], deşi există o mulţime de tratări parţiale ale subiectelor menţionate. Probabil că acesta a fost şi raţionamentul lui Ross Anderson[4] de a face o sinteză a acestor concepte într-un capitol distinct.

Problematica este veche, preocupările lăsând urme de mii de ani, aşa cum am relatat în capitolul dedicat clasificării informaţiilor, trecând peste teritoriile Mesopotamiei, Chinei antice şi ajungând să fie utilă tuturor ţărilor într-o mare varietate de forme.

Sigiliile aveau rolul autentificării înscrisurilor vremii. Dacă în Europa şi America ele au doar farmecul istoriei, în Japonia, China şi Coreea încă se folosesc pentru documente foarte importante, şefii statelor aplicându-le pe toate actele speciale ce se arhivează. În multe ţări, sigilarea este încă utilizată în protejarea actelor poştale şi, în general, a produselor ambalate. În această categorie, intră o largă gamă de produse, de la parfumuri, ţigări, băuturi alcoolice sau răcoritoare, la componente de avioane sau calculatoare.

Mulţi producători de calculatoare vor să ofere un plus de siguranţă cumpărătorilor apelând la tipărirea securizată, tehnici de ambalare şi sigilii. Hologramele, filigranele şi alte sisteme de securizare sunt din ce în ce mai folosite.

De asemenea, producătorii de soft nu se rezumă doar la criptarea produselor sau la filigranarea lor digitală. Ei apelează la unele măsuri de protecţie împotriva pirateriei, realizând etichetele cu hologramă care trebuie să nu se dezlipească uşor, ci, dimpotrivă să se rupă la desigilare.

Majoritatea mijloacelor de securizare nu au pretenţia că vor stopa pirateria, dar scopul lor este de a se proba încălcarea unor norme comerciale şi juridice.

Un alt subiect îl constituie uşurinţa contrafacerii produselor de securizare, tocmai apelându-se la tehnologiile moderne, cum sunt copiatoarele, scanner-ele, imprimantele ş.a.

Dacă se urmăreşte istoria unui element de securizare se va observa cum lupta dintre cei ce l-au conceput şi pirateria de pe piaţă a condus la o continuă evoluţie a lor. Ideea lui Napoleon, la începutul secolului XIX, de introducere a bancnotelor de hârtie, a fost una salutată de contemporanii lui, dar ce se întâmplă acum în lume demonstrează cât de puternică a devenit industria falsificărilor. Fotografia, inventată în 1839, a stat la baza multor documente cu rol de identificare şi autentificare, dar ea a condus la numeroase contrafaceri, ceea ce a determinat apariţia imprimantelor color şi a gravărilor metalice. Dar nici pozele color n-au putut să ofere linişte decât pentru o scurtă perioadă de timp, situaţie în care s-au inventat alte tehnici optice, cum ar fi echipamentele pentru realizarea hologramelor. Apărătorii şi atacatorii ţin pasul cu ultimele realizări din domeniu. Că reuşesc şi unii şi alţii sunt o mulţime de dovezi. Cel mai mediatizat a fost cazul bancnotelor britanice din anii 1990 – dintre cele mai securizate. Ele aveau un fir metalic transparent, de 1 mm lăţime, care parcă era cusut, fiecare bucăţică vizibilă cu



[3] Renesse, R. – *Optical Document Security*, 2nd ed., Artech House, 1997

Renesse, R. – „Verifying versus Falsyfying Banknotes", in *Optical Security and Counterfeit Deterrence Techiques II*, (1998), IS&T (The Society for Imaging Science and Technology) and SPIE (The International Society for Optical Engineering), v 3314, IS1314, 0-8194-2754-3, pp. 71-85.

[4] Anderson, R. – *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley&Son, Inc., New York, 2001.

ochiul liber având 8 mm, formând astfel o linie verticală din puncte metalice. Dacă se privea în lumină ea desena o linie metalică continuă. Cine se gândea că aşa-ceva poate fi contrafăcut? Şi, totuşi, nişte „specialişti" au pus bazele unei foarte profitabile industrii. Ei au folosit un proces ieftin de imprimare la cald a liniei metalice continue pe care au întrerupt-o în bucăţele de câte 8 mm, folosind cerneală albă. Zeci de milioane de lire sterline au fost contrafăcute pe parcursul câtorva ani. După descoperirea cazului, europenii se gândesc la o eventuală deplasare peste Oceanul Atlantic a răufăcătorilor, deoarece dolarul american este tipărit cu doar trei culori.

Este greu de stabilit care este modelul de manifestare a pericolelor, cât timp falsificatorii sau atacatorii pot fi organizaţii finanţate de guverne pentru contrafacerea bancnotelor altor ţări, întreprinderi mici şi mijlocii care pot să facă milioane de dolari măsluind vignete, holograme sau diverse timbre de marcare a mărfurilor sau pot fi amatori care să dispună de tehnica necesară la ei acasă sau la un loc de muncă nu prea bine supravegheat. Descoperirea lor este anevoioasă, deoarece numărul de obiecte contrafăcute este mic în raport cu cele adevărate. Banii falşi nu pot înşela un specialist din bănci, dar ei tocmai din această cauză se plasează în locuri cu oameni naivi sau în localuri mai întunecate şi zgomotoase, cum sunt barurile de noapte.

Se consideră că în cazul bancnotelor false *există trei niveluri de verificare* prin care falsurile pot sau nu să treacă. Ele sunt următoarele:

- *nivelul primar de verificare* este înfăptuit de persoanele neinstruite sau cu prea puţină experienţă în actele de vânzare-cumpărare;
- *nivelul secundar al verificării* se exercită de personal competent şi motivat, cum este cazul experimentaţilor operatori de la ghişeele băncilor sau inspectorii calificaţi ai produselor industriale marcate cu etichete şi/sau timbre fiscale. Ei pot să dispună de echipamente speciale, cum sunt lămpile cu raze ultraviolete, creioane cu reactivi chimici, scannere sau PC-uri special dotate. Oricum, astfel de echipamente nu pot fi prea numeroase şi nici prea costisitoare, iar falsificatorii le ştiu puterea.
- *al treilea nivel al verificării* se efectuează în laboratoare speciale ale producătorilor de elemente de securitate pentru băncile ce realizează emisiuni monetare. Echipamentele folosite sunt mult mai scumpe decât cele amintite anterior şi nu pot da rateuri. O astfel de verificare depistează absolut toate contrafacerile, numai că ea se exercită asupra cazurilor cu totul speciale.

Documentele speciale şi hârtiile de valoare folosesc, de regulă, produse de tipărire dintre cele ce urmează:

- *intaglio* sau *gravura cu acizi* se foloseşte pentru fixarea cu mare forţă a cernelii pe hârtie, lăsând în urmă o imprimare în relief cu o mare rezoluţie. Este tehnica folosită cel mai mult la tipărirea banilor sau realizarea paşapoartelor;
- *literă presată*, prin care cerneala este depusă prin rularea caracterelor în relief şi presarea hârtiei pe care se face tipărirea, astfel încât să rămână şi urmele presării. Tehnica este folosită pentru tipărirea numerelor ce indică valoarea bancnotelor. Mărimea lor şi culoarea sunt atipice, ca elemente suplimentare de securitate, eliminând posibilitatea realizării lor cu materiale sau mijloace existente pe piaţă;
- *procesarea simultană* constă în transferarea completă a cernelii simultan pe ambele feţe ale bancnotei, ceea ce va conduce la o tipărire cu suprapunere perfectă. Se spune că reproducerea lor cu imprimantele color din comerţ este aproape imposibilă. În plus, prin duze speciale, cerneala color este dispusă variat de-a lungul unei linii;
- *ştampilele de cauciuc* sunt folosite pentru andosarea documentelor sau pentru ştampilarea fotografiilor de pe documente;
- *gofrarea şi laminarea*. Gofrarea sau scrierea în relief şi laminarea sunt folosite pentru fixarea fotografiilor şi marcarea caracterelor pe carduri pentru a scumpi costurile contrafacerilor. Gofrarea poate fi fizică sau prin tehnica laserului pentru fixarea fotografiilor pe documente de identificare;

- *filigranele*, tratate într-un paragraf anterior, sunt exemple de utilizare a unor elemente speciale pentru protejarea hârtiilor de valoare. Ele sunt zonele transparente sau marcate cu materiale speciale de pe o hârtie. Se pot folosi şi fire fluorescente. Un exemplu aparte îl constituie Australia (ţară în care au fost tipărite şi unele bancnote româneşti), unde însemnele de 10 dolari sunt tipărite pe suport de plastic cu zone transparente.

Dintre *tehnicile mai moderne*, amintim:

- *cernelurile schimbătoare optic*, tehnică folosită pentru unele porţiuni ale bancnotelor canadiene de 20 dolari, care îşi schimbă culoarea de la verde la galben, în funcţie de unghiul din care este privit obiectul. La noi, tehnica este cunoscută şi sub numele de gât de răţoi sau guşă de porumbel;
- *cerneala cu proprietăţi magnetice sau fotoacustice*;
- *imprimarea unor semne vizibile cu echipamente speciale*, aşa cum este microtipărirea de pe bancnotele americane, care necesită o sticlă magnetizabilă pentru a urmări semnele, precum şi tipărirea în cerneluri ultraviolete, infraroşii sau magnetice – ultima fiind folosită pentru tipărirea culorii negre de pe bancnotele americane;
- *firele sau foliile metalice*, de la simplele irizări în culorile curcubeului până la folii cu efecte optice variabile, aşa cum sunt *hologramele* sau *kinegramele*, precum cele de pe bancnotele de 20 şi 50 de lire sterline. Hologramele se produc, de regulă, optic şi reprezintă obiecte întregi pe un plan îndepărtat, iar kinegramele sunt realizate cu calculatorul şi oferă imagini diferite în funcţie de unghiul din care sunt văzute;
- *marca digitală a copyright-ului* variază ca formă de prezentare şi este recunoscută de copiatoare, scannere şi imprimante, care se opresc la întâlnirea ei, refuzând reproducerile ilegale;
- *unicitatea*, asigurată prin dispunerea aleatoare de fibră magnetică pe hârtie, ceea ce face ca toate exemplarele realizate prin semnături şi tipăriri digitale să fie unice, apelând la unele tipuri de coduri bară.

Problema protejării nu este atât de simplă, pe cât pare la prima vedere, pentru că ea trebuie să ţină cont şi de aspecte estetice, de rezistenţă la întrebuinţare ş.a. Din experienţele acumulate de-a lungul timpului, s-au desprins următoarele lecţii:

- marcajele de securitate trebuie să „spună” ceva, să fie purtătoare ale unui mesaj relevant pentru produs. Este mai plăcută tipărirea cu irizări ale curcubeului decât alte semne invizibile;
- ele trebuie să-şi găsească locul potrivit, să facă parte firească din ansamblul documentului, astfel încât şi fixarea în mintea utilizatorului să fie naturală;
- efectul lor trebuie să fie evident, distinct şi inteligibil;
- nu trebuie să intre în concurenţă cu alte produse realizate cât de cât similar, pentru a nu da curs imitărilor sau confuziilor;
- ele trebuie să fie standardizate.

În cazul bancnotelor, teoria spune că sunt necesare aproximativ 20 de modalităţi de securizare care nu sunt mediatizate. Câteva dintre ele sunt aduse la cunoştinţa inspectorilor de specialitate. Cu timpul, acestea sunt aflate şi de falsificatori. Mai mult, după un număr variabil de ani, ei află aproape toate cele 20 de elemente, moment în care bancnotele se retrag de pe piaţă şi se înlocuiesc cu alt model. Cercetările din domeniu anunţă o posibilă apariţie a unui sistem unic de marcare, constând într-un strat chimic special, conţinând proteine sau chiar molecule DNA, prin care se vor codifica serii ascunse, citibile de către orice tip de maşină de verificare a lor.

Identificaţi în activitatea organizaţiilor economice documente importante, care au introduse elemente de securizare.

## 5.4 Sisteme de criptare prin chei secrete (simetrice)

O astfel de criptografie, după cum sugerează şi numele din paranteză, apelează la o singură cheie la ambele capete ale comunicării: emiţătorul şi receptorul. Emiţătorul sau expeditorul criptează textul clar cu ajutorul unei chei secrete, iar receptorul sau destinatarul va decripta mesajul criptat folosind aceeaşi cheie, firesc, reuşita este asigurată de secretizarea cheii. Succesul cheilor simetrice este şi mai mare dacă ele se schimbă mai des. Ideal ar fi ca o cheie simetrică să fie folosită o singură dată.

Un sistem de criptare prin cheie secretă are în structura sa informaţie publică şi privată. *Informaţia publică*, de regulă, constă în:

- un algoritm folosit pentru criptarea textului clar în mesaj criptat;
- posibil, un exemplar al textului clar şi textului criptat corespunzător;
- posibil, o variantă criptată a textului clar care a fost aleasă de către un receptor neintenţionat.

*Informaţiile private* sunt:

- cheia sau variabila de criptare;
- o anumită transformare criptografică dintr-o mulţime de transformări posibile.

Succesul sistemului se bazează pe dimensiunea cheii. Dacă ea are mai mult de 128 biţi este una destul de sigură, ceea ce înseamnă siguranţă în exploatare. Ea se adaugă rapidităţii cu care se efectuează criptarea şi volumului mare de date asupra cărora poate opera. Iată trei caracteristici esenţiale ale sistemelor bazate pe chei simetrice: siguranţă, rapiditate, volum mare de date criptate.

Singura problemă a sistemului constă în folosirea în comun a cheii de criptare de către emiţător şi receptor, ceea ce înseamnă că emiţătorul trebuie să folosească o paletă largă de chei pentru o mare diversitate a utilizatorilor. Există o tehnică de intermediere prin chei publice, dar nu intrăm în detalii. Oricum, trebuie să se ştie că sistemele bazate pe chei simetrice nu oferă mecanismele necesare autentificării şi nerepudierii.

Cel mai cunoscut sistem bazat pe chei simetrice este *Data Encryption Standard* (*DES*), dezvoltat din sistemul criptografic *Lucifer* al firmei IBM.

### 5.4.1 Sistemul DES

DES este un sistem de criptare prin chei simetrice, conceput în 1972, ca o dezvoltare a algoritmului *Lucifer*, realizat de Horst Feistel la IBM. DES este utilizat în scop comercial pentru informaţii neclasificate. El descrie algoritmul de criptare a datelor (*DEA*, *Data Encryption Algorithm*) , fiind numele dat de *Federal Information Processing Standard* pentru 46-1, adoptat în 1977 ca *FIPS PUB 46-1*. DEA este, de asemenea, definit ca *Standard ANSI*, cu codul *ANSI X3.92 – ANSI* fiind *American National Standards Institute*. În 1993, Institutul Naţional pentru Standarde şi Tehnologie din SUA recertifică DES, dar el nu va mai fi recertificat după implementarea noului sistem *AES, Advanced Encryption Standard*.

DES operează în următoarele moduri:

- criptarea prin blocuri înlănţuite (*Cipher Block Chaining – CBC*);
- criptarea - carte electronică de coduri (*Electronic Code Block – ECB*);
- criptarea cu feedback la ieşire (*Output Feedback – OFB*).

Datorită vulnerabilităţii DES, din noiembrie 1998, guvernul SUA nu-l mai foloseşte, înlocuindu-l cu *Triplu DES*, adică trei criptări folosind DEA, până la introducerea *AES – Advanced Encryption Standard*.

### 5.4.2 Sistemul AES

AES este un cifru bloc ce va înlocui DES-ul, dar se preconizează că *Triplu DES* va rămâne în uz cu aprobarea guvernului SUA, prin specificaţia FIPS 46-3.

Iniţiativa AES a fost demarată în ianuarie 1997 de către NIST (*National Institute of Standards and Technology*), prin solicitarea variantelor de algoritmi de criptare care să intre în competiţie. Până în august 1998, NIST a anunţat 15 candidaturi, iar în 1999 au fost selectaţi 5 finalişti: MARS, RCG, Rijndael, Serpent şi Twofish. Runda a doua de analiză publică a algoritmilor a fost închisă în 15 mai 2000. La data de 2 octombrie 2000, NIST a anunţat selecţia *Rijndael Block Cipher*, având ca autori doi cercetători belgieni, Dr. Joan Daemen şi Dr. Vincent Rijmen. Acesta va fi algoritmul AES propus, devenind un nou standard FIPS, utilizat de guvernul SUA să protejeze informaţii sensibile, dar neclasificate. Se speră că el va fi adoptat şi de alte organizaţii publice sau private, atât din SUA, cât şi de pe alte continente.

*Algoritmul Rijndael* a fost conceput să îndeplinească următoarele proprietăţi:

- rezistenţă împotriva tuturor atacurilor cunoscute;
- simplitatea proiectării;
- mare compactare a codurilor şi o viteză sporită pe o mare varietate de platforme.

Cifrul Rijndael poate fi catalogat ca un cifru bloc iterativ cu lungimi variabile ale blocurilor şi ale cheii, alese independent, de 128, 192 sau 256 biţi. În valori din sistemul de numerotaţie zecimal există:

- aproximativ $3{,}4 \times 10^{38}$ chei posibile de 128 biţi;
- aproximativ $6{,}2 \times 10^{57}$ chei posibile de 192 biţi;
- aproximativ $1{,}1 \times 10^{77}$ chei posibile de 256 biţi.

Pentru a aprecia rigurozitatea algoritmului Rijndael, este cazul să amintim că, dacă un calculator poate să spargă sistemul de criptare DES prin încercarea a $2^{56}$ chei într-o secundă, acelaşi calculator va avea nevoie de $149 \times 10^{12}$ ani pentru a sparge algoritmul Rijndael. Să nu uităm că universul este creat de ... doar $13 \times 10^{9}$ ani, adică de 13 miliarde de ani.

Cifrul Rijndael va putea să fie implementat în realizarea chip-urilor de mare viteză, indiferent de domeniul utilizării, sau ca un co-procesor compact pe cartelele inteligente.

### 5.4.3 Cifrul IDEA

Cifrul IDEA (*International Data Encryption Algorithm*) este sigur, secret şi foloseşte o cheie de 128 biţi ce se aplică blocurilor de text clar de câte 64 de biţi. El a fost realizat în 1992 de James Massey şi Xuejia Lai, preluând algoritmii anteriori numiţi *Proposed Encryption Standard* (*PES*) şi *Improved Proposed Encryption Standard* (*IPES*).

Prin lungimea cheii, de 128 biţi, cifrul IDEA este mai greu de spart decât DES, motiv pentru care el a fost preluat de Phil Zimmerman în sistemul *Pretty Good Privacy* (PGP) pentru criptarea e-mail-urilor.

## 5.5 Sisteme de criptare prin chei publice (asimetrice)

Spre deosebire de sistemele de criptare bazate pe chei secrete, care presupun o singură cheie cunoscută de emiţător şi receptor, sistemele bazate pe chei publice folosesc două chei: una publică şi alta privată.

*Cheia publică* este pusă la dispoziţia oricărei persoane care doreşte să transmită un mesaj criptat.

*Cheia privată* este utilizată pentru decriptarea mesajului, iar nevoia de a face schimb de chei secrete este eliminată.

Pentru înţelegerea sistemului, sunt necesare următoarele lămuriri:

- cheie publică nu poate decripta un mesaj criptat;
- se recomandă ca o cheie privată să nu deriveze dintr-o cheie publică;
- un mesaj care a fost criptat printr-o anumită cheie poate fi decriptat cu altă cheie;
- cheia privată nu este făcută publică.

Dacă notăm cu C un text criptat şi cu P un text clar (P este notaţia consacrată pentru *plain text*), iar Kp este cheia publică şi Ks cheia privată (secretă), procesul este ilustrat astfel: *C = Kp(P)* şi *P = Ks(C)*. Şi invers este adevărat: *C = Ks(P)* şi *P = Kp(C)*.

Criptografia prin chei publice este posibilă în aplicaţiile care funcţionează într-un singur sens. O funcţie în sens unic este aceea care este uşor de calculat într-o direcţie, dar este dificil de calculat în sens invers. Pentru o astfel de funcţie, dacă $y = f(x)$, este simplu de determinat valoarea lui *y* dacă se cunoaşte *x*, dar este foarte dificil să-l determini pe *x* cunoscându-l pe *y*. Într-o astfel de situaţie se află căutările telefonice. Este uşor să găseşti numărul cuiva dacă ştii numele şi adresa, dar este foarte dificil să găseşti pe cineva într-o carte de telefon cunoscându-i doar numărul de telefon. Pentru ca funcţiile cu sens unic să fie utile în contextul criptografiei bazate pe chei publice ele trebuie să aibă o *trapă*, adică un mecanism secret care să permită realizarea cu uşurinţă a funcţiei inverse funcţiei în sens unic. Printr-o astfel de modalitate se poate obţine *x* dacă se dă *y*.

În contextul criptografiei bazate pe chei publice este foarte dificil să se calculeze cheia privată din cheia publică dacă nu se ştie trapa.

De-a lungul anilor s-au dezvoltat mai mulţi algoritmi pentru cheile publice. Unii dintre ei se folosesc pentru semnătura digitală, pentru criptare sau în ambele scopuri.

Din cauza calculelor numeroase solicitate de criptarea prin chei publice, aceasta este de la 1.000 la 10.000 de ori mai înceată decât criptografia prin chei secrete. Astfel, au apărut *sistemele hibride* care folosesc criptografia prin chei publice pentru transmiterea sigură a cheilor secrete utilizate în criptografia prin chei simetrice.

Dintre algoritmii importanţi ai cheilor publice, amintim Diffie-Hellman, RSA, El Gamal Knapsak şi curba eliptică, foarte utilizaţi fiind primii doi algoritmi.

### 5.5.1 Schimbul de chei Diffie-Hellman

Metoda schimbului de chei Diffie-Hellman, cunoscută şi ca metoda de distribuţie a cheilor publice, poartă numele a doi specialişti de la Standford University, Whitfield Diffie şi Martin Hellman. În anul 1976, ei au inventat o metodă prin care două părţi pot cădea de comun acord să comunice prin mesaje secrete fără să fie nevoie de o terţă parte, de un schimb off-line sau de transmiterea vreunei valori secrete între ele.

Independent, Ralph Merkle a venit cu o soluţie de distribuţie a cheilor publice, numai că metoda propusă implica substanţiale cheltuieli pentru efectuarea calculelor şi a transmisiei. Varianta realizată de Diffie şi Hellman a fost numită *sistemul distribuţiei cheilor publice* sau *al schimburilor de chei publice*.

Metoda Diffie-Hellman se bazează pe conceptul perechii de chei publică-privată. Protocolul începe cu fiecare parte care generează independent câte o cheie privată. În pasul următor, fiecare calculează câte o cheie publică, aceasta fiind o funcţie matematică a cheilor private respective. Urmează schimbul de chei publice. În final, fiecare dintre cele două persoane calculează o funcţie a propriei chei private şi a cheii publice a celeilalte persoane. Matematica este cea care va face să se ajungă la aceeaşi valoare, care este derivată din cheile lor private. Ele vor folosi valoarea ca pe cheie a mesajului.

Diffie şi Hellman folosesc exponenţierea în aritmetica modulară pentru a calcula cheile publice şi cheia mesajului. Aritmetica modulară este ca şi aritmetica standard, cu excepţia faptului că foloseşte numere numai în intervalul 0 la N, numit modulo. Atunci când o operaţie produce un rezultat care este mai mare sau egal cu N, N este scăzut repetat din rezultat până când valoarea se încadrează în intervalul 0 la N-1 (ca şi cum s-ar împărţi la N şi se ia în seamă

restul). De exemplu, 3+4 mod 5 = 2. Dacă rezultatul este negativ, N se adaugă acestuia până când se va încadra în intervalul 0 la N-1. De exemplu, 3-8 mod 7 = -5 mod 7 = 2.

În aritmetica modulară, exponenţierea este o funcţie într-un singur sens. Aceasta înseamnă că este uşor de calculat un număr $y = g^x \ mod \ N$ pentru o valoare secretă *x*, însă este mult mai dificil să se calculeze *x* din *y*, dacă numerele sunt suficient de mari, ca de exemplu o lungime de câteva sute de cifre (noi presupunem că *g* şi *N* sunt cunoscute). Aceasta este referită ca şi problema logaritmului discret pentru că *x* este logaritm din *y* în baza *g* (mod *N*), iar numerele sunt finite şi întregi.

Cu metoda Diffie-Hellman a schimbului de chei publice, Alice şi Bob stabilesc cheia mesajului secret după cum urmează. Alice generează o cheie secretă *xa* şi Bob o cheie secretă *xb*. După aceasta, Alice calculează o cheie publică *ya*, care este *g* ridicat la puterea *xa* modulo *p*, unde *p* este un număr prim (adică nu poate fi descompus în produsul a două numere), *g* fiind mai mic decât *p*. Identic, Bob calculează o cheie publică *yb*, prin ridicarea lui *g* la puterea *xb* modulo *p*. Ei vor schimba valorile publice ale acestora. Apoi, Alice ridică cheia publică a lui Bob la puterea exponentului său, *xa* modulo *p*, în timp ce Bob ridică cheia publică a lui Alice la exponentul său, *xb* modulo *p*. Amândoi vor obţine acelaşi rezultat, *g* ridicat la puterea *xa* şi *xb*, iar rezultatul obţinut va fi folosit de amândoi drept cheia K a mesajului. Matematic, totul se va exprima astfel:

$ya = g^{xa} \ mod \ p$

$yb = g^{xb} \ mod \ p$

$K = ya^{xb} \ mod \ p = yb^{xa} \ mod \ p = g^{xa*xb} \ mod \ p$

Deşi în practică se folosesc numere foarte lungi, de câteva sute de cifre, pentru a ajuta la înţelegerea modului de funcţionare, vom folosi numere mici.

*Exemplul 1*

Să presupunem că p = 7, g = 3, cheia lui Alice xa = 1 şi a lui Bob xb = 2

Vom avea:

- Alice calculează cheia sa publică: $ya = g^{xa} \ mod \ p = 3^1 \ mod \ 7 = 3$
- Bob calculează cheia sa publică: $yb = g^{xb} \ mod \ p = 3^2 \ mod \ 7 = 2$
- Alice calculează $K = yb^{xa} \ mod \ p = 2^1 \ mod \ 7 = 2$
- Bob calculează $K = ya^{xb} \ mod \ p = 3^2 \ mod \ 7 = 2$

sau

$K = g^{xa*xb} \ mod \ p = 3^{2x1} \ mod \ 7 = 9 \ mod \ 7 = 2.$

*Exemplul 2*

Să presupunem că p = 5, g = 4, cheia lui Alice xa = 3 şi a lui Bob xb = 2

- Alice calculează cheia sa publică: $ya = g^{xa} \ mod \ p = 4^3 \ mod \ 5 = 4$
- Bob calculează cheia sa publică: $yb = g^{xb} \ mod \ p = 4^2 \ mod \ 5 = 1$
- Alice calculează $K = yb^{xa} \ mod \ p = 1^3 \ mod \ 5 = 1$
- Bob calculează $K = ya^{xb} \ mod \ p = 4^2 \ mod \ 5 = 1$

sau

$K = g^{xa*xb} \ mod \ p = 4^{3x2} \ mod \ 5 = 4096 \ mod \ 5 = 1.$

Se observă că în ambele cazuri K ia valori identice, 2, respectiv 1.

Metoda Diffie-Hellman, precum şi variantele ei sunt utilizate în câteva protocoale de securitate a reţelelor şi în produse comerciale, inclusiv la AT&T 3600 Telephone Security Device, la Fortezza card – o variantă de carduri criptate, şi la Pretty Good Privacy pentru criptarea e-mail-urilor şi a unor fişiere.

## 5.5.2 RSA

RSA provine de la numele de familie ale inventatorilor săi, Rivest, Shamir şi Adleman[5].

[5] Rivest, R.L., Shamir, A., Adleman, L.M. – „A Method for Obtaining Digital Signatures and Public Key Cryptosystems", in *Communication of the ACM*, v.21, n.2, feb. 1978, pp. 120-126, apud Krutz, R.L., Vins, R.D. – *The CISSP Prep Guide*, John Wiley&Son, Inc., New York, 2001.

Pe vremea când Diffie şi Hellman au inventat metoda distribuţiei prin chei publice, aceştia au gândit şi la un alt concept mult mai performant, dar n-au găsit soluţia implementării lui – criptografia prin chei publice. Prin aceasta, fiecare persoană are o pereche de chei publică-privată, unică, pe termen lung. Componenta publică, transmisibilă prin Internet şi partajată cu toată lumea, este folosită pentru criptarea datelor, în timp ce componenta privată, greu de calculat pe baza cheii publice, este folosită pentru decriptare. Criptografia prin chei publice este numită şi „criptografie prin două chei" şi „criptografie asimetrică". Metodele convenţionale, descrise anterior, care apelează la o singură cheie, sunt referite ca şi „criptografie printr-o singură cheie", „criptografie prin cheie privată", „criptografie prin cheie secretă", „criptografie simetrică" şi „criptografie convenţională".

La scurt timp după ce Diffie şi Hellman au lansat ideea revoluţionară a criptografierii prin chei publice, trei profesori de la MIT (Massachusetts Institute of Technology), Ronald Rivest, Adi Shamir şi Leonard Adleman, au venit cu soluţia implementării ei. Varianta propusă se numea RSA. Concomitent, Hellman şi Merkle au inventat o altă metodă, numită „*trapdoor knapsacks*", bazată pe alt model matematic. Oricum, modelul lor a fost spart la începutul anilor 1980.

Pentru a transmite un mesaj cu text clar către Bob, folosind sistemul cheilor publice, gen RSA, Alice generează cheia K a mesajului şi o foloseşte prin intermediul criptosistemului convenţional, cum ar fi DES, pentru criptarea mesajului. Utilizând criptografia prin chei publice, ea, de asemenea, criptează K, sub cheia publică a lui B, denumită $K_{Bobpub}$. Apoi, ea transmite atât cheia criptată, cât şi mesajul criptat către Bob. Bob, la rândul său, apelează la propria lui cheie privată, denumită $K_{Bobpriv}$, pentru a decripta cheia K a mesajului, apoi el foloseşte cheia K pentru decriptarea mesajului. Modelul este redat sub formă grafică în figura 5.5.

Teoretic, Alice poate să transmită textul către Bob folosind criptarea prin cheia publică a lui Bob, apelând doar la criptografia prin cheie publică. În practică, însă, nu se întâmplă aşa, din cauza începerii procesului de transmitere prin mulţimea calculelor de efectuat. E mult mai rapid să foloseşti o metodă convenţională de mare viteză pentru criptarea mesajului, rezervând metoda cheii publice doar pentru distribuţia cheii. În plus, nu se consideră o practică prea inspirată să foloseşti aceeaşi cheie pentru criptarea mesajelor de-a lungul unei mari perioade de timp, din cauza sporirii şanselor de a fi atacată. Perechea de chei publică-privată este uneori numită „cheia cheii de criptare", pentru a o deosebi de cheia mesajului (cheia datelor criptate).

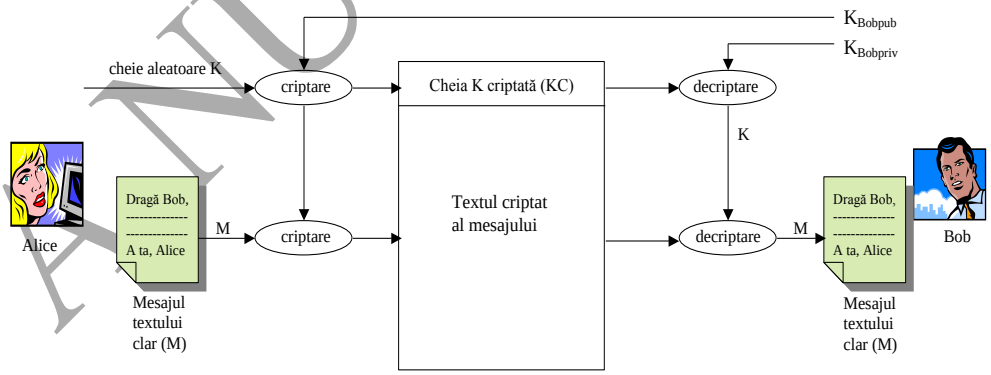


**Fig. 5.5 Alice transmite un mesaj lui Bob folosind o combinaţie de cheie singulară şi criptografiere prin cheie publică (prelucrare după Denning, D. – *Op. cit.*, p. 302)**

Ca şi Diffie-Hellman, sistemul RSA calculează exponenţierile în aritmetica modulară folosind numere cu lungimea de câteva sute de cifre. În RSA, totuşi, fiecare persoană are un modulo N personal, care este produsul a două numere prime secrete. Cheia K a mesajului este criptată prin ridicarea ei la puterea exponentului public a lui Bob (*eb*), modulo *Nb*, iar decriptarea se efectuează prin ridicarea ei la puterea exponentului privat al lui Bob (*db*), modulo

*Nb*. Presupunând că *C* va prelua valoarea cheii textului criptat, aceasta se va exprima matematic astfel:

$C = K^{eb} \bmod Nb$ (criptarea lui K)

$K = C^{db} \bmod Nb$ (decriptarea)

Pentru ca exponentul folosit la decriptare (*db*) să poată reface exponenţierea cu *eb* la criptare, formula *eb * db = 1 mod (pb-1)(qb-1)* trebuie să fie realizată; în care *Nb = pb * qb* pentru numerele prime *pb* şi *qb*.

În aceste condiţii, oricine ştie *eb, pb* şi *qb* poate să folosească formula pentru a deduce *db*. Din acest motiv, *pb* şi *qb* nu se divulgă, chiar dacă *eb* şi *Nb* sunt făcute publice. Calcularea factorilor primi ai lui *Nb* se consideră a fi, din punct de vedere matematic, nerezolvabilă pentru numere foarte mari.

Vom folosi valori mici ale numerelor din exemplul următor pentru a uşura înţelegerea mecanismului. Să presupunem că Bob a ales numerele prime secrete *pb* = 5 şi *qb* = 3, de unde rezultă că *Nb = pb * qb* = 5 * 3 = 15. Apoi alege exponentul secret *db* = 29 şi îl calculează pe *eb* după formula *eb * db = 1 mod (pb-1)(qb-1),* ceea ce va conduce la *eb* * 29 = 1 mod (4 * 2), 29 * *eb = 1 mod 8*. Prin încercări succesive rezultă *eb = 5*.

Dacă Alice doreşte să transmită cheia K = 2 către Bob, ea o va cripta cu exponenţierea din cheia publică a lui Bob, efectuând calculele:

$$C = K^{eb} \bmod Nb = 2^5 \bmod 15 = 32 \bmod 15 = 2$$

Când Bob obţine cheia criptată o va decripta folosindu-şi cheia secretă drept exponent, prin calculul:

$K = C^{db} \bmod Nb = 2^{29} \bmod 15 = 2$ (Se aplică mod (2 ** 29, 15)).

Se observă că s-a obţinut valoarea K = 2 a cheii transmisă de Alice.

### 5.5.3 Semnătura digitală

Inventarea criptografiei prin chei publice a adus două importante mutaţii valoroase. Prima, discutată anterior, permite transmiterea unui secret către o altă persoană fără să fie nevoie de o a treia persoană de încredere sau de un canal de comunicaţie off-line pentru a transmite cheia secretă. A doua mutaţie s-a produs pe planul calculării semnăturii digitale.

O *semnătură digitală* este un bloc de date (alcătuit din cifre binare, ceea ce în engleză înseamnă *binary digit*, de unde şi digitală – exprimată printr-un şir de cifre) ce se ataşează unui mesaj sau document pentru a întări încrederea unei alte persoane sau entităţi, legându-le de un anumit emiţător. Legătura este astfel realizată încât semnătura digitală poate fi verificată de receptor sau de o terţă persoană şi nu se poate spune că a fost uitată. Dacă doar o cifră binară nu corespunde, semnătura va fi respinsă în procesul de validare. Semnătura digitală stabileşte autenticitatea sursei mesajului. Dacă o persoană nu-şi dă în vileag cheia personală privată nimeni nu poate să-i „imite" semnătura. O semnătură digitală nu înseamnă şi recunoaşterea dreptului de proprietate asupra textului transmis, ci ea atestă faptul că persoana semnatară a avut acces la el şi l-a semnat. Documentul poate fi şi sustras de undeva. Totuşi, atunci când semnarea este cuplată cu crearea documentului, semnătura poate oferi o probă evidentă a originii documentului. În această categorie intră fotografiile luate cu camere digitale bazate pe chei private. În acest caz, proba este de necontestat. Aşa se procedează când se intenţionează realizarea protecţiei împotriva manipulării imaginilor cu ajutorul calculatorului. La fel pot fi camerele video, radio-receptoarele şi alţi senzori care pot semna ieşirea pentru a-i certifica originea.

Deşi semnătura digitală este implementată prin sistemul criptografiei cu chei publice, transformările ce au loc sunt diferite de cele de la criptare. În timp ce la criptare fiecare parte are o pereche de chei publică-privată, în cazul semnăturii digitale, componenta privată este întrebuinţată pentru semnarea mesajelor, iar cea publică este folosită de o altă parte pentru a verifica semnătura. Modul de funcţionare este redat în figura 5.6.

După prezentarea suplimentară a algoritmilor semnăturii digitale să parcurgem paşii „dialogului" purtat de Alice cu Bob. Alice intenţionează să semneze un mesaj. Ea va începe prin calcularea unei valori rezumat a mesajului, care este determinată printr-o funcţie publică de dispersie (*hashing*). În acest moment nu se folosesc chei. În pasul următor, ea va utiliza o cheie privată pentru semnătură $KS_{Alicepriv}$, pentru a calcula o transformare criptografică a valorii rezumat a mesajului. Rezultatul, care este semnătura sa pe mesaj, se ataşează mesajului. Din acest moment, mesajul semnat poate fi transmis altei persoane, inclusiv Bob, sau poate fi stocat într-un fişier.

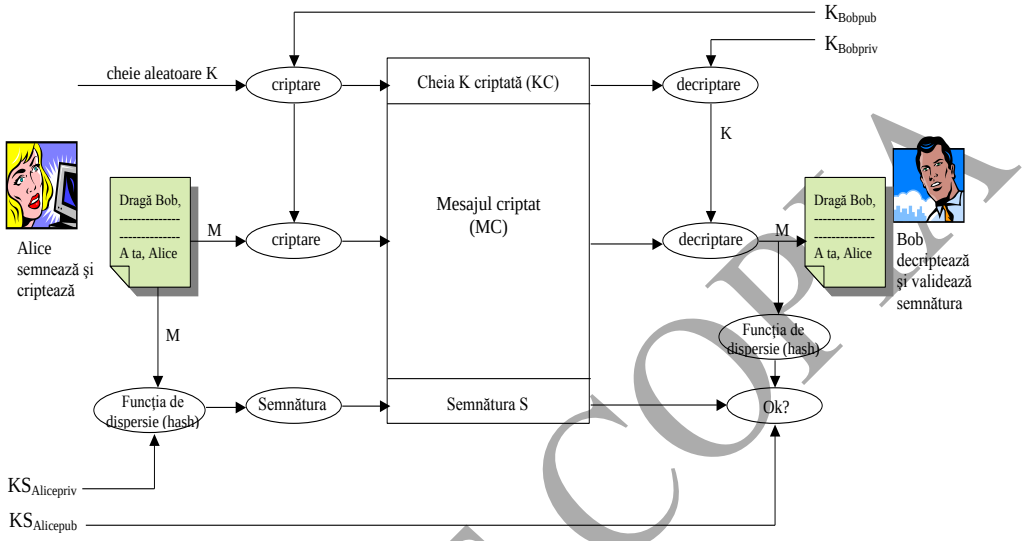


**Fig. 5.6 Alice transmite către Bob un mesaj semnat şi criptat. Mesajul este criptat printr-o singură cheie de criptare, iar cheia prin criptarea cu cheie publică. Mesajul este semnat cu sistemul semnăturii digitale prin cheie publică (prelucrare după Denning, D.– Op. cit., p. 332)**

Să presupunem că Bob va recepţiona mesajul ei. El poate să valideze semnătura lui Alice făcând apel la cheia ei publică pentru semnătură, $KS_{Alicepub}$, ce va fi folosită ca intrare într-o funcţie criptografică prin care se va testa dacă valoarea rezumat determinată de el este aceeaşi cu valoarea codificată prin semnătura lui Alice. Dacă da, va accepta semnătura. Se observă că nici o cheie de-a lui Bob nu este folosită în procesul de validare a semnăturii transmise de Alice, ci doar cheile ei. În schimb, când Alice transmite cheia unui mesaj secret către Bob, ea va folosi doar cheile lui Bob.

Dacă Alice doreşte să transmită un mesaj către Bob, mesaj care să fie semnat şi criptat, procesul presupune utilizarea cheilor pentru semnătură ale lui Alice ($KS_{Alicepriv}$, $KS_{Alicepub}$), cheilor lui Bob de criptare a cheii ($K_{Bobpub}$) şi o cheie a mesajului, K. În sinteză, iată paşii:

- Alice generează o cheie aleatoare a mesajului, K. Alice criptează mesajul M cu cheia K, obţinând mesajul criptat, MC;
- Alice criptează cheia K folosind cheia publică a lui Bob de criptare a cheii, $K_{Bobpub}$, rezultând cheia criptată, KC;
- Alice procesează o semnătură S folosind cheia sa privată pentru semnătură, $KS_{Alicepriv}$;
- Alice transmite către Bob KC, MC şi S;
- Bob foloseşte cheia sa privată de criptare a cheii, $K_{Bobpriv}$, pentru a decripta KC şi a obţine K;
- Bob foloseşte K pentru decriptarea MC şi obţinerea textului-clar, M;
- Bob foloseşte cheia publică pentru semnătură a lui Alice, $KS_{Alicepub}$, pentru validarea semnăturii S.

Tot acest proces este folosit de sistemul de criptare e-mail-uri, aşa că Alice şi Bob nu vor efectua operaţiunile enunţate, ci le face calculatorul. Pentru a dispune de aceste servicii este necesară contactarea unor firme specializate. Microsoft recomandă Verisign, cu site-ul *www.verisign.com*, deşi sunt mai multe oferte. Oricum e necesară obţinerea unui ID digital. La click-ul pe *Sign* apare semnul sigiliului special pentru semnătură, iar la comanda *Send,* vi se oferă un meniu prin care puteţi începe dialogul pentru obţinerea ID-ului digital pentru semnătură, prin click pe butonul *Get Digital ID*.

Pentru a studia cadrul legal al utilizării semnăturii electronice în România, puteţi obţine informaţiile dorite de pe site-ul *www.legi-internet.ro/lgsemel.htm*.

## 5.5.4 Sisteme de certificare a cheilor publice

Un sistem criptografic bazat pe chei publice poate fi compromis de o persoană (A) care transmite o cheie publică altei persoane (B) către un alt partener (C). În acest caz (C) va folosi cheia publică a lui (B) pentru a cripta mesajul, cu intenţia de a ajunge înapoi la (B), numai că (A), folosindu-şi propria cheie privată, va face ca receptorul să fie el, reuşind astfel să decripteze mesajul care era adresat lui (B).

Pentru a se evita o astfel de ciudăţenie, se recurge la procesul certificării, prin care persoanele sunt legate de cheile lor publice. Documentul oferit de o *Autoritate de Certificare* acţionează ca orice alt act emis de un notar şi se efectuează după aceleaşi reguli, adică pe baza verificării identităţii persoanei solicitante, concretizându-se prin atribuirea unei chei publice pentru persoana respectivă. Unitatea de certificare semnează certificatul cu propria cheie privată. Din această cauză, persoana este verificată ca emiţător dacă este necesară cheia ei publică pentru deschiderea sesiunii de transmitere a mesajelor criptate şi/sau semnăturilor electronice. Certificatul conţine numele subiectului, cheia lui publică, numele autorităţii de certificare, perioada de valabilitate a certificatului. Pentru a verifica semnătura autorităţii de certificare, cheia ei publică trebuie să fie verificată încrucişat cu o altă autoritate de certificare. În SUA formatul certificatelor este reglementat prin standardul X.509. Certificatele sunt păstrate într-un Registru (Repository), alături de lista certificatelor revocate. În principiu, operaţiunile pentru obţinerea certificatelor digitale şi validarea tranzacţiilor sunt redate în figura 5.7.

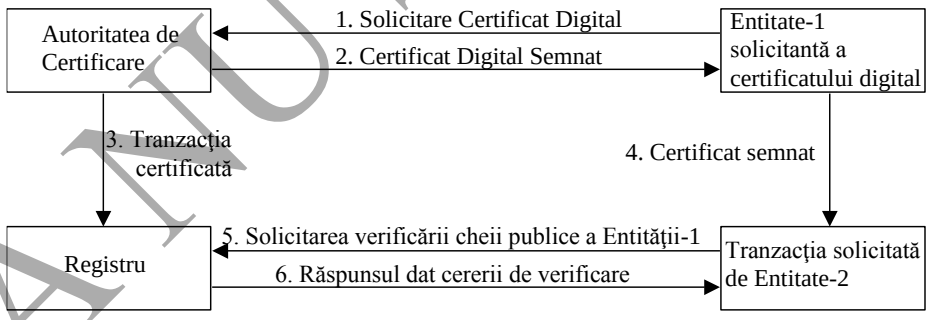


**Fig. 5.7 Prezentarea unei tranzacţii cu certificate digitale**

## 5.5.5 Infrastructura cheilor publice (PKI)

Infrastructura cheilor publice (*PKI – Public Key Infrastructure*) îşi propune să rezolve probleme manageriale din domeniul cheilor publice, integrând semnături şi certificate digitale cu o mare diversitate de alte servicii specifice comerţului electronic, prin care se solicită oferirea integrităţii, controlului accesului, confidenţialităţii, autentificării şi a nerepudierii tranzacţiilor electronice.

Infrastructura cheilor publice cuprinde certificatele digitale, autorităţile de certificare, autorităţile de înregistrare, politici şi proceduri cu chei publice, revocarea certificatelor,

nerepudierea, marcarea timpului, certificarea încrucişată, aplicaţii de securitate, LDAP (*Lightweight Directory Acces Protocol*).

LDAP oferă un format standard de accesare a directoarelor certificatelor. Aceste directoare sunt stocate pe serverele LDAP dintr-o reţea, serverele de pe aceste reţele oferind chei publice şi certificate X.509 pentru companii.

Certificatele cheilor publice pot fi eliberate în regim online sau off-line. În sistem off-line, o persoană trebuie să se legitimeze cu carnetul de şofer sau alt act de identitate. În varianta online, certificatele se pot oferi ca răspuns al unei cereri formulate prin e-mail sau direct de pe un site specializat. Detalii multiple, inclusiv adrese de unităţi specializate puteţi obţine de pe site-ul *www.pki-page.org/#EU*.

În SUA, majoritatea certificatelor sunt emise de Verisign, Inc., recomandată şi de Microsoft. Compania oferă *trei clase de certificate personale*, numite *digital IDs*, toate legate de e-mail:

- *clasa 1 de certificate* verifică adresa e-mail a utilizatorului, fără să solicite alte elemente de autentificare. După exprimarea interesului pentru un certificat, sistemul trimite o confirmare cu un PIN pe adresa de e-mail a persoanei. Utilizatorul se întoarce la site-ul anterior (al companiei) şi oferă PIN-ul, după care este generat un *ID digital* şi se memorează în calculatorul utilizatorului;
- *clasa 2 de certificate* cere utilizatorului să mai introducă şi *Social Security Number* (codul oferit de *Internal Revenue Service*), adresa şi seria carnetului de şofer;
- *clasa 3 de certificate digitale* este destinată companiilor ce publică software, oferindu-le un grad mult mai mare de securitate, dar există şi o variantă pentru persoane fizice ocupate cu transferuri bancare, contracte ş.a. Este o clasă mult mai sigură.

Pentru detalii, vizitaţi site-ul *www.verisign.com*.

Oricum, realizarea unei infrastructuri a cheilor publice la nivel internaţional, dar şi naţional, este o mare problemă, nu din punct de vedere tehnic sau managerial, ci al legislaţiei.

Daţi exemple de utilizare a tehnologiilor criptografice descrise mai sus.

## 5.6 Atacuri criptografice

Sistemele criptografice bune trebuie să fie astfel proiectate încât să fie aproape imposibil de spart. În practică, este realizabilă o astfel de performanţă fără eforturi prea mari, dar teoretic orice sistem bazat pe metode criptografice poate fi spart prin încercări succesive ale cheilor. Dacă se face uz de *forţa brută* pentru a încerca toate cheile, puterea calculatoarelor necesare creşte exponenţial cu lungimea cheii.

O cheie de 32 de biţi presupune verificarea a $2^{32}$ (aproximativ $10^9$) paşi, ceea ce se poate realiza şi cu un calculator aflat la domiciliu.

Un sistem bazat pe o cheie cu 40 de biţi are nevoie de $2^{40}$ paşi, ceea ce ar însemna cam o săptămână folosind un calculator mai performant de la domiciliu.

Un sistem cu 56 de biţi pentru cheie, cum este DES, necesită un efort mult mai mare. Cu un număr mai mare de calculatoare personale, lucrând în sistem distribuit, în câteva luni este spart, iar cu echipamente speciale, într-un timp mult mai scurt.

Se spune că toate sistemele actuale cu chei de 64 de biţi sunt vulnerabile în faţa multor tipuri de organizaţii. Cele cu 80 de biţi par asigurate pentru câţiva ani, iar cele de 128 de biţi sunt invulnerabile în faţa atacurilor cu forţă brută pentru un număr nedefinit, încă, de ani.

Totuşi, în cele mai multe sisteme, incidentele se întâmplă nu din cauza lungimii cheii, ci a algoritmului folosit. Am prezentat într-un paragraf anterior algoritmul Rijndael, care, cu 256 de biţi, se pare că este posibil de spart în $149 \times 10^{12}$ ani, ştiut fiind că Universul s-a creat în urmă cu $13 \times 10^{9}$ ani. Nimeni nu ştie însă cât de vulnerabil este un sistem în faţa spărgătorilor de profesie, a criptanaliştilor. Ei se descurcă în a decripta comunicaţii criptate fără să cunoască cheile corespunzătoare, apelând la mai multe *tehnici criptanalitice*.

Pentru cei ce implementează noi sisteme criptografice sunt prezentate câteva dintre cele mai cunoscute tehnici de criptanaliză de atacuri.

*Forţa brută*. Se încearcă orice combinaţii posibile, de regulă, secvenţial, pentru aflarea algoritmului. Cu cât cheia este mai lungă, cu atât este mai dificilă aflarea ei.

*Text clar cunoscut*. Atacatorul cunoaşte sau poate ghici textul clar pentru o parte din textul criptat. Important este să decripteze restul textului folosind aceste informaţii, adică să afle cheia folosită.

*Text clar ales*. Atacatorul este în măsură să aibă orice text doreşte criptat cu cheie necunoscută. Misiunea lui este să afle cheia folosită la criptare. Se recomandă a se evita punerea la dispoziţia criptanaliştilor a unui text clar şi a variantei criptate.

*Text clar cu selecţie adaptată*. Este o formă a textului clar ales, numai că selecţia textului clar se schimbă în funcţie de rezultatele anterioare.

*Numai text criptat*. Aceasta este situaţia în care atacatorul nu are nici o idee asupra conţinutului mesajului şi trebuie să „lucreze” doar cu textul criptat. În practică este deseori posibil să se intuiască bucăţi din textul criptat, în special părţi din antetul documentelor sau formule de final. Multe spargeri se bazează pe analiza frecvenţei apariţiei caracterelor, dar la sistemele actuale de criptare rezultatele sunt aproape nule.

*Text criptat selectat*. Se selectează părţi din textul criptat pentru a încerca aflarea cheii, având acces la aceleaşi bucăţi de text clar.

*Text criptat cu selecţie adaptată*. O formă similară celei anterioare, dar selecţia porţiunilor din textul criptat pentru tentativa de decriptare va ţine cont de rezultatele anterioare.

*Atacul „zi-de-naştere”*. De regulă, se aplică probabilităţii ca două mesaje diferite folosind aceeaşi funcţie de dispersie să producă un rezumat comun al mesajului. Termenul „zi-de-naştere” provine de la faptul că, statistic vorbind, într-o cameră cu 23 de persoane există o probabilitate mai mare de 50% ca două persoane să aibă aceeaşi zi de naştere.

*Întâlnire-la-mijloc*. Se aplică schemelor cu dublă criptare, prin criptarea unui text clar cunoscut de la un anumit capăt cu fiecare cheie, K, posibilă şi compararea rezultatului cu ceea ce se obţine „la-mijlocul-textului” prin decriptarea textului criptat, folosind orice cheie, K, posibilă.

*Om-la-mijloc*. Un atacator care va exploata avantajul oferit de sistemul de lucru al celor mai multe reţele – memorează şi dă mai departe – va intercepta mesajele şi versiunile modificate ale mesajului original în timp ce se află între două părţi în aşteptarea comunicaţiilor securizate.

*Criptanaliza diferenţială*. Se aplică sistemelor criptografice bazate pe chei private, prin urmărirea unei perechi de texte criptate care au fost obţinute prin criptarea aceleiaşi perechi, dar de text clar, cu diferenţele de rigoare, iar din analiza acestora se încearcă a se afla sistemul de criptare.

*Criptanaliza liniară*. Folosindu-se perechi de text clar cunoscut şi textele criptate corespunzătoare, se încearcă aproximarea liniară a unei părţi din cheie.

*Criptanaliza diferenţială liniară*. Se folosesc cele două metode descrise anterior.

*Factorizarea*. Se folosesc metode matematice pentru determinarea factorilor primi ai numerelor mari.

*Statistica*. Se exploatează slăbiciunile funcţiilor de randomizare folosite la generarea cheilor.

*Atac împotriva sau folosind anumite echipamente*. În ultimii ani, au apărut tot mai multe echipamente mobile de criptare şi, odată cu ele, o nouă categorie de atacuri îndreptate asupra

acestora. De regulă, atacurile se bazează pe culegerea datelor rezultate din jurul echipamentelor de criptat (ca, de exemplu, radiaţiile).

*Erori în sistemele de criptare*. Uneori, existenţa unor erori în sistemul de criptare poate să-i conducă pe criptanalişti la descoperirea cheilor de criptare.

*Calculatoare cuantice*. Calculatoarele pe bază de cuante se află în atenţia multor cercetători, deoarece ele vor fi mult mai puternice decât actualele calculatoare seriale. Puterea se obţine prin paralelismul inerent al mecanicii cuantice. Aşa că, în loc să se efectueze sarcinile câte una pe unitate de timp, cum funcţionează sistemele seriale, calculatoarele pe bază de cuante le efectuează simultan. Deocamdată, s-au realizat doar calculatoare mici, dar când se vor realiza sisteme foarte mari actualii algoritmi de criptare vor fi într-un real pericol. În acelaşi timp, optimiştii văd partea frumoasă a lucrurilor: sistemele de criptare vor fi mult mai performante, dispunând de astfel de calculatoare. Deja, teoretic, s-au realizat sisteme de criptare într-un astfel de mediu.

*Calculatoare bazate pe molecule DNA*. Leonard Adleman, unul dintre inventatorii sistemului de criptare RSA, a venit cu ideea folosirii DNA drept calculatoare. Moleculele de DNA pot fi văzute ca şi calculatoare paralele foarte puternice. Practic, ideea este, deocamdată, greu realizabilă. Dacă vor deveni realitate discuţiile sunt aceleaşi ca şi la calculatoarele cuantice.

În practică, sunt multe alte tipuri de atacuri şi tehnici de criptanaliză. Se consideră că descrierile anterioare ar fi suficiente pentru proiectanţii sistemelor criptografice dacă ar ţine cont de ele în totalitate, ceea ce este aproape imposibil.

Pe baza informaţiilor din literatura de specialitate, realizaţi un top al celor mai dese atacuri criptografice.



## Rezumat

Scopul criptografierii este de a proteja informaţiile transmise fără să poată fi citite şi înţelese decât de către persoanele cărora le sunt adresate. Teoretic, persoanele neautorizate le pot citi, însă, practic, citirea unei comunicaţii cifrate este doar o problemă de timp – efortul şi timpul aferent necesare unei persoane neautorizate să decripteze mesajul criptat.

Există *două tipuri principale de tehnologii criptografice* sunt *criptografia prin chei simetrice* (chei secrete sau chei private) şi *criptografia prin chei asimetrice* (chei publice).

Cele mai cunsocute *metode de criptare* sunt: substituţia, transpoziţia (permutarea), cifrul lui Verman, cifrul carte, codurile, ascunderea informaţiilor (steganografia, filigranarea, securitatea tipăririi hârtiilor de valoare).

Dintre cele mai cunoscute *sisteme bazate pe chei secrete* (simetrice) pot fi amintite: DES (Data Encryption Standard), AES (Advanced Encryption Standard), cifrul IDEA (International Data Encryption Algorithm).

Ca *sisteme de criptare prin chei publice* (asimetrice) pot fi enumerate: schimbul de chei Diffie-Hellman, RSA, semnătura digitală, sistemele de certificare a cheilor publice, infrastructura cheilor publice (PKI – Public Key Infrastructure).

*Sistemele criptografice* bune trebuie să fie astfel proiectate încât să fie aproape imposibil de spart. În practică, este realizabilă o astfel de performanţă fără eforturi prea mari, dar teoretic orice sistem bazat pe metode criptografice poate fi spart prin încercări succesive ale cheilor.

Cele mai cunoscute *tehnici de criptanaliză de atacuri* sunt: forţa brută, text clar cunoscut, text clar ales, text clar cu selecţie adaptată, numai text criptat, text criptat selectat sau cu selecţie adaptată, atacul "zi-de-naştere", întâlnire-la-mijloc, om-la-mijloc, criptanaliza diferenţială, liniară sau mixtă, factorizarea, statistica, atac împotriva sau folosind anumite echipamente etc.

CAPITOLUL VI

# Asigurarea securităţii sistemelor informaţionale publice şi private

Cunoscută fiind importanţa securităţii fizice, în capitolul de faţă vor fi tratate iniţail subcomponentele ei – amplasarea centrelor de prelucrare automată a datelor, securitatea echipamentelor –, după care vor fi abordate aspecte ale securităţii softului şi personalului. Sistemul, în integritatea sa, va avea un tratament special, într-un paragraf distinct, iar altul va prezenta responsabilităţile dintr-o organizaţie pe linia prelucrării automate a datelor. Ca obiective, ne dorim de la cititorii noştri:

- dobândirea de cunoştinţe privind securitatea locului de amplasare a centrelor de prelucrare;
- cunoaşterea modalităţilor de asigurare a securităţii echipamentelor şi softului;
- familiarizarea cu măsurile ce vizează securitatea pe linia personalului;
- identificarea principalelor metode de asigurare a securităţii la nivelul sistemului informatic;
- crearea suportului necesar pentru aplicarea măsurilor administrative pe linia securităţii.

## 6.1 Securitatea locului de amplasare a centrelor de prelucrare a datelor

Despre măsuri speciale de asigurare a securităţii centrelor de prelucrare automată a datelor există numeroase materiale în literatura de specialitate, îndeosebi străină. Nu ne propunem să prezentăm în detaliu toate aspectele legate de această problemă, ci doar pe cele mai edificatoare.

### 6.1.1 Alegerea amplasamentului centrelor de calcul

Problema amplasării corecte a centrului de calcul nu intră în atribuţiile responsabilului cu securitatea sistemului. De regulă, centrele de calcul se amplasează în clădiri special construite, preferându-se terenurile virane. Totuşi, practica demonstrează că, de cele mai multe ori, centrele de calcul se amplasează în clădiri construite cu alt scop, în care au mai fost sau nu folosite calculatoare şi care dispun sau nu de sisteme de protecţie speciale. De asemenea, clădirile sunt folosite şi în alte scopuri, găzduind mai multe servicii ale aceleiaşi unităţi sau chiar mai multe unităţi, cu activităţi diferite, uneori chiar de ordinul sutelor, cum a fost cazul World Trade Center. În astfel de situaţii, apar anumite restricţii, unele imperfecţiuni, motiv pentru care trebuie să se ia în considerare următoarele aspecte:

1. Locul de amplasare să fie pe un teren solid, fără riscul alunecărilor, nu deasupra tunelurilor, a sistemelor principale de colectare a apei reziduale sau a altor elemente de risc.
2. Nivelul faţă de cotele de inundaţie trebuie să fie evident.
3. Mediul de amplasare, de asemenea, nu trebuie să fie afectat de cutremure, zgomote, vibraţii, câmpuri electromagnetice (ale radarelor) sau de poluare a aerului. Zona trebuie să fie liniştită, şi nu una cunoscută pentru numeroasele incidente sociale. Vecinii sunt liniştiţi? Cu ce se ocupă?
4. Cum funcţionează serviciile de utilităţi în zona de amplasare? Curentul şi apa au un regim sigur de funcţionare? Drumurile în ce stare sunt? Serviciile speciale de intervenţie

(pompieri, salvare, poliţie) sunt amplasate în apropiere? Au experienţa pentru a interveni în cazul unor incidente dintr-un centru de calcul?

5. Zona de amplasare trebuie să fie suficient de mare, astfel încât în preajma clădirii să existe, pe orice latură, cel puţin 10 metri de spaţiu liber, iar parcările să nu fie mai aproape de 30 de metri. Dacă ar fi posibil, se recomandă ca întreaga clădire a centrului de calcul să fie înconjurată din toate părţile de clădirile firmei, izolând-o, în acest mod, de lumea din afară.

Cum credeţi că se modifică cerinţele de securitate de mai sus în cazul data center-urilor moderne? Propuneţi un set de cinci recomandări valabile pentru asigurarea securităţii amplasării centrelor de date.

## 6.1.2 Proiectarea centrului de calcul

După alegerea locului de amplasare, se poate trece la schiţarea machetei clădirii care să găzduiască sistemul electronic de calcul. Cât ar fi de entuziaşti proiectanţii, îndeosebi arhitecţii, uneori, în afara gustului lor deosebit pentru estetic, trebuie rugaţi să mai respecte şi alte elemente, şi anume:

1. Clădirea trebuie să fie una solidă, realizată din materiale neinflamabile. Sala calculatorului central (a serverelor) se recomandă să nu aibă ferestre şi pe absolut toate părţile să fie înconjurată de alte săli ale centrului de prelucrare respectiv.
2. Numărul intrărilor şi ieşirilor din clădire trebuie să fie minim, respectându-se, totuşi, normele pe linie de stingere a incendiilor. Pentru introducerea în clădire a echipamentului şi a mobilierului mare se poate proiecta o intrare specială, dar ea nu va fi folosită şi pentru persoane. Intrarea principală a acestora trebuie să dispună şi de o aşa-zisă „zonă tampon”, unde să aibă loc procedurile de control şi acceptare a intrării în unitate.
3. Cheile, îndeosebi cele ce înlesnesc accesarea mai multor puncte de intrare, trebuie să fie tratate cu acelaşi interes ca şi lucrurile sau informaţiile protejate. Toate cheile se dau numai sub semnătură persoanelor ce le primesc, întocmindu-se, în acelaşi timp, şi un registru special al posesorilor de chei, care, la rândul lor, vor prezenta şi autorizarea posesiei cheilor.
4. Parterul şi etajul întâi, pe cât posibil, nu trebuie să aibă ferestre externe pentru a se evita intrarea prin forţarea lor, iar, dacă există, se recomandă ca ele să fie realizate din cărămizi de sticlă, cărora li s-ar putea adăuga măsuri suplimentare (cadre metalice) de protecţie.
5. Sălile cu calculatoare nu se recomandă să fie amplasate la demisolul clădirii. Locul ideal de amplasare începe cu parterul, el fiind cel mai lejer mod de accesare din punctul de vedere al personalului, dar şi de eventualii intruşi, motiv pentru care etajul unu este cel mai sigur.
6. În interiorul centrului trebuie să se efectueze o judicioasă compartimentare a spaţiului, nepermiţându-se accesul direct al nici uneia dintre camere. Este cazul bibliotecii de suporturi, sălii calculatorului, celei de pregătire date, al zonei imprimantelor, al birourilor administrative, al birourilor programatorilor ş.a. Se recomandă ca accesul în astfel de zone să fie facilitat prin sisteme de chei electronice.
7. Clădirile trebuie să fie prevăzute cu sisteme de alarmă în caz de incendiu sau de pătrundere neautorizată. Sistemele de alarmă trebuie să fie amplasate în zona intrării principale în clădire şi din motivul supravegherii continue a lor. Supravegherea zonei exterioare a clădirii şi a principalelor locuri din interior se va realiza prin sistemul de

televiziune cu circuit închis sau prin monitoare de supraveghere continuă. Lor li se adaugă şi corpuri speciale de pază.

8. Un rol deosebit îl vor avea procedurile de verificare a sistemelor de alarmă, precum şi cele de răspuns în caz de incident, numindu-se comandamente speciale în acest scop. Foarte importantă este descoperirea alarmelor false de incendiu, produse numai cu scopul creării condiţiilor de derută în sistem, astfel încât acesta să fie atacat cu uşurinţă de către intruşi.
9. Se impune crearea unui sistem sigur de control al securităţii transportului unor resurse (suporturi magnetice, rapoarte, documentaţie ş.a.). Persoana care efectuează transportul trebuie să aibă autorizare specială.
10. Un control special se impune şi pentru preîntâmpinarea deplasării neautorizate a unor componente din sistem.
11. Sistemele de asigurare a serviciilor de furnizare a apei, energiei electrice, gazului şi facilităţile de comunicaţii trebuie să fie amplasate subteran. Canalele de acces la ele trebuie să fie, de asemenea, încuiate şi supravegheate. Conductele de apă şi sistemul de canalizare nu trebuie să traverseze spaţiile ce găzduiesc averile informatice ale firmei, ci să le înconjoare. Dacă ocolirea nu este posibilă, se impune montarea unor ventile suplimentare.
12. Copiile de siguranţă trebuie să fie păstrate în clădiri speciale, la cel puţin 100 de metri de cea a centrului de prelucrare a datelor.
13. O atenţie deosebită se va acorda şi tablourilor de control căldură, aer condiţionat, linii telefonice şi transformatoarelor de curent electric.
14. Hârtia va fi depozitată departe de sala calculatorului, iar resturile de hârtie trebuie să aibă tratamentul descris anterior.
15. În sala calculatorului sunt interzise fumatul şi consumul de lichide şi mâncare. Pentru păstrarea ţigărilor, chibriturilor, brichetelor vor fi create locuri speciale, în afara sălii calculatorului.
16. Sistemele de control al prafului sunt deosebit de importante, îndeosebi în sala calculatorului, recomandându-se pardoseala electrostatică din policlorură de vinil şi evitându-se lemnul din configuraţia sălii, precum şi covoarele şi perdelele. Echipamentele, care prin funcţionare produc şi impurităţi, trebuie să fie amplasate cât mai departe de echipamentele foarte sensibile.

Cum credeţi că se modifică cerinţele de securitate de mai sus în cazul data center-urilor moderne? Propuneţi un set de cinci recomandări valabile pentru asigurarea securităţii proiectării centrelor de date.

### 6.1.3 Protecţia şi securitatea mediului de lucru al calculatoarelor

Serviciile şi utilităţile dintr-un centru de prelucrare automată a datelor joacă un rol foarte important în configuraţia sistemelor, constituind de multe ori punctele nevralgice ale acestora. Proasta funcţionare a lor paralizează şi cele mai performante echipamente de prelucrare automată a datelor şi din această cauză se recomandă luarea unor măsuri suplimentare, dintre care amintim:

1. *Lumina*. Comutatoarele şi tablourile electrice trebuie să fie numai sub controlul personalului sistemului, iar generatoarele proprii de energie trebuie să intervină în cazul căderii sistemului normal de furnizare a ei. Printre măsurile şi mai riguroase figurează apelarea la acumulatoare sau baterii, folosite numai pentru iluminat, când toate sursele de curent alternativ nu mai pot fi utilizate.

2. *Căldura.* Limitele de temperatură trebuie să fie respectate cu stricteţe, conform recomandărilor producătorilor, de regulă între 19-24 grade Celsius.
3. *Sistemul de aer condiţionat.* Chiar şi sistemele foarte moderne funcţionează optim numai în anumite condiţii de temperatură şi umiditate. Se recomandă un sistem propriu de aer condiţionat pentru întreaga zonă de prelucrare automată a datelor.
4. *Furnizarea energiei electrice.* De regulă, sistemul energetic este destul de sigur, dar se impune utilizarea unor generatoare suplimentare de energie, a UPS-urilor, a filtrelor de tensiune ş.a.

Una dintre recomandările anterioare se referea la evitarea construirii clădirilor din materiale uşor inflamabile. În plus, mai pot fi adăugate următoarele sfaturi:

- evitarea depozitării hârtiei în sala calculatorului;
- păstrarea loturilor mari de hârtie în locuri îndepărtate de sala calculatorului, iar pentru prelucrările zilnice ele să fie cât mai mici;
- asigurarea unei curăţenii exemplare în sala calculatorului.

Paza împotriva incendiilor trebuie să fie în responsabilitatea unor persoane special desemnate, dar, la fel de bine, se va conta pe sprijinul autorizat al comandamentului pompierilor din localitate. Numai cu acceptul acestora vor fi iniţiate toate măsurile de pază împotriva incendiilor, cum sunt:

1. Utilizarea uşilor şi pereţilor rezistenţi la incendiu. Ele trebuie să reziste sub foc cel puţin o oră. Uşile trebuie să fie suficiente ca număr pentru a asigura părăsirea cât mai rapidă a clădirii, dispunând de semnale optice luminoase, indicatoare de sens, care să funcţioneze pe bază de baterii. Sistemul de aer condiţionat, dacă devine un real pericol prin funcţionarea sa, trebuie să se blocheze automat, dar să se şi deblocheze atunci când este necesară eliminarea fumului.
2. Se va întocmi un plan de intervenţie în caz de incendiu, în care se vor cuprinde condiţiile de evacuare, de stingere a incendiului şi de protejare a valorilor deosebite din sistem. Personalul va fi instruit în acest sens.
3. Asigurarea cu echipamente şi materiale speciale pentru intervenţie în caz de incendiu, un rol aparte avându-l stingătoarele de incendii electrice şi ne-electrice. Personalul trebuie să le cunoască. De regulă, pentru incendiile la instalaţiile electrice se recomandă stingătoarele bazate pe bioxid de carbon, iar gazul se stinge cu apă.
4. Instalarea în toată clădirea a detectoarelor de fum şi de temperaturi foarte ridicate. Ele au rol de semnalizare şi depistare a momentului în care să se declanşeze sistemul de luptă împotriva incendiilor (în sala calculatorului este cunoscut sistemul de stingere bazat pe gaz halogen, cu rol de protejare a echipamentelor de prelucrare automată a datelor). Se recomandă şi stingătoarele cu apă, dar numai atunci când incendiul ia proporţii şi nu mai contează dacă echipamentele vor fi afectate mai mult sau mai puţin.
5. Orientarea preocupărilor şi spre celelalte zone importante ale centrului, nu numai asupra sălii calculatorului. Uneori sursele de incendii sunt mai numeroase în afara sălii calculatorului.

Analizaţi modul în care sunt respectate măsurile de mai sus într-o organizaţie cunoscută de dumneavoastră.

## 6.2 Securitatea echipamentelor

Datorită importanţei lor deosebite, componentele sistemelor electronice de calcul trebuie să beneficieze de un tratament aparte.

Se ştie că o cale sigură de compromitere a securităţii unui sistem electronic de calcul este de natură fizică, modificându-i anumite elemente din configuraţie astfel încât, faţă de configurarea dată de utilizator, să se creeze căi de acces pentru cei rău intenţionaţi sau să se blocheze mijloacele de asigurare a securităţii sistemului. În acest sens, se pot modifica circuitele electronice, se pot adăuga mici „şmecherii" (circuite cu rol special, emiţătoare, microfoane), se pot realiza derivaţii ale canalelor de comunicaţie, pot fi scurt-circuitate componentele cu rol de protecţie, citirea pe ascuns a memoriei în care sunt păstrate parolele sistemului, scoaterea controlului existent pe terminale pentru depistarea pătrunderilor neautorizate.

Echipamentele, în pofida reclamei făcute de producători, sunt predispuse la căderi, fie datorită unor defecţiuni de fabricaţie, fie instalării greşite, fie datorită defectării în timpul transportului. Dar, cel mai grav, echipamentele pot „cădea" în timpul exploatării lor, devenind atât ele, cât şi datele conţinute în memorie inutilizabile. Uneori şi softul cu care se lucrează poate fi pierdut.

Sunt dese cazurile când echipamentele nu au certificat de origine, fie în întregime, fie numai pentru unele dintre miile de componente din structura lor. Incertitudinea aplanează asupra a ceea ce s-a cumpărat şi consecinţele sunt şi mai grave atunci când distribuitorul este un ilustru necunoscut.

Întreţinerea sau depanarea sistemului sunt asigurate, de regulă, de specialişti din afară. Cu multă uşurinţă ei pot realiza toate operaţiunile menţionate anterior pentru paralizarea sistemului.

Apărarea împotriva tuturor pericolelor descrise are un rol vital în buna funcţionare a sistemului. Totuşi, trebuie pornit de la faptul că toate componentele sistemelor, la rândul lor, pot dispune de elemente proprii de asigurare a securităţii.

### 6.2.1 Asigurarea echipamentelor împotriva intenţiilor de modificare a lor

Toate componentele sistemelor de prelucrare automată a datelor trebuie protejate, fie împotriva hoţilor, fie a vandalilor. Sunt unele elemente care necesită însă o grijă deosebită. De exemplu, terminalele nu sunt la fel de importante ca şi calculatorul central sau serverele sistemului.

Echipamentele pot fi protejate împotriva modificării lor astfel:

- Birourile ce conţin hardware trebuie să fie încuiate, sigilate cu benzi de hârtie sau cu plumb. Sigiliile vor fi verificate periodic pentru depistarea accesului neautorizat. Cele mai moderne sigilii sunt cele holografice care conţin imagini unice, imposibil de recreat.
- Echipamentele trebuie să fie, pe cât posibil, mai dispersate, îndeosebi în cazul lucrului cu informaţii speciale.
- Elementele din configuraţia fizică a sistemului care sunt deosebit de importante, cum ar fi cazul plăcii cu circuite, pot fi fotografiate la intervale regulate de timp pentru a compara fotografiile mai multor perioade în vederea depistării eventualelor modificări.

Este posibil ca fiecare echipament periferic să aibă atribuit un număr unic de identificare, interpretabil de către calculator la deschiderea sesiunii de lucru şi confirmat ulterior când se solicită o operaţiune la/de la perifericul respectiv. Fiecare imprimantă, terminal sau legătură din reţea trebuie să aibă definite categoriile de informaţii cu care pot lucra sau funcţiile din sistem ce se realizează prin intermediul lor. Numerele unice de identificare înlesnesc tratarea diferenţiată a perifericelor sau a celorlalte componente. De exemplu, terminalele amplasate în diverse locuri din unitate, pentru a veni în sprijinul oricărui utilizator comun al firmei, nu trebuie să aibă şi dreptul de accesare a sistemului de operare al calculatorului central sau să restaureze date în scopul manipulării lor. De asemenea, imprimantele din diverse birouri nu pot folosi datele secrete care au un regim sever la tipărire.

O măsură suplimentară de control va consta în stabilirea momentelor din zi când un echipament periferic sau un utilizator a accesat sistemul. Oricum nu este recomandat să se

permită angajaţilor firmei să lucreze peste program, iar când aceasta se impune va fi sub un control riguros.

### 6.2.2 Controlul integrităţii echipamentelor

Calculatoarele pot să-şi verifice singure starea în care se află celelalte componente, prin autodiagnoză, astfel încât să poată descoperi ce nu funcţionează cum trebuie. Printre activităţile realizate de calculatoare vor fi verificarea modului de lucru, inclusiv urmărirea funcţiilor de realizare a securităţii sistemului, precum şi facilităţile de control al accesului.

Autodiagnoza este utilă pentru:

- confirmarea cu precizie a identităţii echipamentelor, suporturilor şi utilizatorilor - elementele de bază ale sistemului;
- verificarea dacă utilizatorii folosesc doar echipamentele, softul şi datele la care ei au acces de drept şi preîntâmpinarea accesului neautorizat;
- asigurarea că orice tentativă de acces sau utilizare neautorizată a echipamentelor, softului sau datelor este blocată şi că supraveghetorii sistemului vor fi anunţaţi imediat.

Simpla realizare a funcţiilor de mai sus nu înseamnă neapărat şi perfecţiunea sistemului de securitate, dar constituie suficiente măsuri de apărare a sistemului împotriva atacurilor rău intenţionate.

Există şi producători de calculatoare care asigură facilităţi de diagnoză de la distanţă a stării sistemului, ceea ce în mod normal se realizează de către echipele de service, pentru a se asigura că totul funcţionează corect şi că nu se conturează posibilitatea apariţiei unor defecţiuni. O astfel de metodă este benefică pentru unitate, întrucât duce la reducerea costurilor şi se realizează mult mai rapid decât în varianta apelării la inginerii de întreţinere. Totuşi, diagnoza de la distanţă este destul de periculoasă pentru securitatea sistemului, intruşilor oferindu-li-se o şansă în plus să acceseze orice element din configuraţie, aceştia având la dispoziţie o linie specializată. Aşadar, aparentul cost redus poate să însemne pierderi mult mai mari.

### 6.2.3 Proceduri de întreţinere a echipamentelor

Activităţile de întreţinere şi reparare a oricărui echipament pot genera o mulţime de semne de întrebare privind siguranţa, securitatea şi disponibilitatea datelor din sistem. Din această cauză este foarte important să se controleze accesul la echipamente şi software şi să se supravegheze îndeaproape specialiştii care asigură întreţinerea sau repararea sistemului.

O primă măsură va consta în deschiderea unui registru de întreţinere, în care să se înregistreze toate detaliile privind o astfel de activitate. Ele se vor referi la data şi timpul efectuării lor, numele tehnicienilor, motivul vizitei lor, acţiunile şi reparaţiile ce au avut loc, inclusiv componentele hard care au fost adăugate, reparate, înlocuite sau reînnoite. Fiecare înregistrare din registru va fi contrasemnată de responsabilul cu securitatea sistemului. Registrul trebuie să fie consultat periodic pentru descoperirea eventualelor nereguli.

Ca şi în cazul diagnozei de la distanţă, în timpul întreţinerii sau reparării sistemului trebuie să fie scoase datele şi softul de pe benzi sau pe discuri de orice tip, iar cele din memoria principală, de asemenea, salvate, reiniţializându-se sistemul numai în acest scop. Specialiştilor ce efectuează întreţinerea nu trebuie să li se înlesnească accesul la datele speciale ale unităţii, în mod deosebit la parolele acesteia.

Dacă sistemul este defect şi măsurile de precauţie enumerate nu mai pot fi luate, se recomandă ca specialiştii unităţii să fie alături de cei ce asigură întreţinerea pentru a şti cu exactitate ce anume efectuează. În acest scop, ei chiar pot fi întrebaţi de ce efectuează operaţiunile respective.

Activităţile de întreţinere trebuie să aibă un plan, în totală concordanţă cu planul de funcţionare al întregului sistem. De regulă, producătorii specifică termenele la care să se

realizeze întreţinerea fiecărei componente. Numai responsabilul sistemului poate accepta efectuarea unor operaţiuni înainte de termen, precum şi repararea, înlocuirea sau înnoirea unor elemente din sistem.

Se recomandă ţinerea evidenţei materialelor de rezervă, chiar a imprimantelor, terminalelor sau monitoarelor, iar consumabilele să fie comandate la timp pentru a nu se produce disfuncţionalităţi în sistem.

Testarea securităţii sistemului trebuie să se realizeze înainte ca acesta să înceapă prelucrarea datelor reale ale unităţii.

Numele specialiştilor în întreţinere, precum şi al furnizorilor de utilităţi, trebuie să fie afişate la vedere pentru o contactare a lor în orice moment, de către persoanele autorizate să facă acest lucru.

Dacă inginerii de întreţinere solicită scoaterea din unitate a unor componente sau a documentaţiei firmei, în primul rând, trebuie să ne asigurăm că ele nu conţin date importante ale firmei. Este mult mai recomandat ca datele aflate pe unele suporturi să fie distruse, decât să se mizeze pe discreţia specialiştilor. Costă mai mult, dar e mai sigur.

„Cârpirea" softului este o altă problemă importantă. Sunt cazuri când trecerea peste un punct din program va duce la funcţionarea lui corectă în continuare, dar nimeni nu ştie exact cum funcţionează. Şi încă ceva: depinde şi de cine face „cârpeala" programului şi cu ce scop. Şi astfel de operaţiuni se scriu în registrul de întreţinere.

### 6.2.4 Toleranţa la cădere a echipamentelor

Cel mai cunoscut este sistemul din aviaţie care, în cazul când o componentă se defectează, dispune de alta care să-i preia funcţia. Unele piese, cum sunt cele de control al zborului sau a componentelor hidraulice, au câteva piese înlocuitoare, astfel încât o catastrofă majoră ar putea să apară numai după ce toate aceste piese de siguranţă s-au defectat. Toleranţa la cădere a avioanelor este asigurată astfel încât să nu aibă loc prăbuşirea lor.

În cazul calculatoarelor aceasta este o calitate foarte importantă, absolut vitală pentru existenţa sistemelor performante. Toleranţa la cădere sau la defecte trebuie să contribuie la prevenirea pierderilor sau denaturării datelor şi, pentru aceasta, orice apăsare de tastă trebuie să fie înregistrată undeva, astfel încât să poată fi restaurată prin anumite proceduri. Toleranţa la cădere trebuie să facă în aşa fel încât să permită funcţionarea sigură, controlată şi supravegheată, în timpul reparării, asigurându-se astfel funcţionarea continuă a calculatorului care a înregistrat o defecţiune, chiar şi una majoră, în timp ce se lucrează pentru îndepărtarea ei. În practică, aşa-ceva este destul de greu de realizat, dar, dacă numărul componentelor cu rol vital în existenţa sistemului s-ar reduce şi ar avea mai mulţi înlocuitori, operaţiunea este, totuşi, posibilă.

În sensul celor spuse până acum, sunt tipuri de calculatoare care funcţionează cu două unităţi centrale de prelucrare, în tandem, ambele prelucrând în acelaşi timp aceleaşi date şi programe. Pe această cale, la eventuala cădere a uneia dintre ele, cealaltă va funcţiona singură până când a doua va fi repusă în funcţiune. Echipamentele sunt amplasate în săli apropiate şi folosesc aceleaşi condiţii de lucru, cum ar fi: aer condiţionat, linii de comunicaţie, tipuri de unităţi de bandă şi de discuri, surse de energie electrică şi alte utilităţi. Cât timp majoritatea sistemelor cad din cauza unei plăci de memorie sau de circuite logice sau din cauza unor mici incidente înregistrate la softul de sistem sau de aplicaţii, funcţionarea în tandem evită căderea sistemului în întregime.

Alte componente ale sistemelor electronice de calcul sunt astfel construite încât să-şi exercite unele funcţii în formă dublă. Un exemplu îl oferă metoda înregistrării „în oglindă" pe disc, prin care două discuri sunt scrise în acelaşi timp pentru prevenirea pierderilor de date, dacă s-ar defecta capetele de citire-scriere ale unuia.

Echipamentele folosite în condiţii dificile, cum sunt cele mobile din domeniul militar, sunt amplasate în containere speciale, deosebit de rezistente la şocuri, apă şi praf. Sistemul de cablare va fi protejat prin ţevi metalice, iar căderile de energie vor fi suplinite de un sistem energetic propriu.

Toate măsurile luate pentru eventualele căderi trebuie să fie în deplină concordanţă şi cu importanţa întregului sistem de prelucrare automată a datelor.

### 6.2.5 Contractele

Unul dintre cele mai neplăcute momente referitoare la configuraţia sistemului îl reprezintă lungile discuţii purtate cu cei ce le-au livrat, atunci când sistemul se defectează sau nu funcţionează la parametrii aşteptaţi. Sunt cunoscute suficiente mici necazuri din lumea calculatoarelor, numai că producătorii de sisteme n-au nici un interes să le popularizeze, fie din dorinţa de a nu-şi păta reputaţia, fie mizând pe faptul că ele nu vor fi uşor sesizate.

Aproape că a devenit o regulă supraestimarea caracteristicilor calculatoarelor. Vânzătorii sunt, de cele mai multe ori, nesinceri sau prea încrezători în produsele ce le comercializează, imboldul venind de la producători, care îşi prezintă produsele ca fiind cele mai bune, în raport cu ale concurenţilor de pe piaţă.

De vină sunt şi beneficiarii care, deseori, subestimează sau nu cunosc ceea ce vor. De cele mai multe ori, vor sistemele cele mai ieftine, dar îşi schimbă părerea când le pun în funcţiune, ajungând la concluzia că era mai bine dacă acesta ar dispune şi de nişte funcţii ale căror beneficii le simte nevoia.

Totul s-ar termina cu bine dacă, din fazele incipiente ale procurării sistemului, s-ar concepe contracte care să scutească toate părţile de discuţii interminabile.

Din prima fază, clientul trebuie să ofere distribuitorului de sisteme următoarele elemente:

1. O foarte clară definire a sistemului dorit:

a) descrierea funcţiilor solicitate acestuia şi componentele cu rol prioritar din structura sa. Dacă este nevoie de un procesor de texte, atunci trebuie cerut aşa-ceva, dacă se cere un soft de birotică, trebuie menţionat ca atare; oricum, nu trebuie să ne aşteptăm ca un soft de un tip anume să ne onoreze toate pretenţiile de prelucrare automată a datelor;

b) descrierea intenţiilor de extindere a sistemului în viitor, îndeosebi dacă se vrea crearea unei reţele de calculatoare;

c) detalii privind gradul de încărcare a sistemului în perspectivă, specificându-se numărul utilizatorilor, tipul activităţilor de executat, cerinţele reţelei, importanţa ce o va avea sistemul şi, de aici, cerinţele pe linie de întreţinere şi reparare a lui.

2. Stabilirea nivelului de securitate dorit în sistem, astfel încât furnizorul să ştie ce să ofere.
3. Păstrarea tuturor documentelor referitoare la negocierile cu furnizorul de componente. Se poate merge până acolo încât să se specifice minutele de întâlniri, comentariile şi observaţiile de pe parcurs, conversaţiile telefonice, cu data corespunzătoare, cât timp au durat şi cu cine s-au purtat, ce literatură s-a consultat, ce prezentări au fost făcute de către furnizor ş.a.
4. Cuantificarea, dacă este posibilă, a efectelor defectării totale a sistemului sau a nefuncţionării lui la parametrii promişi. Furnizorii trebuie să ia cunoştinţă de aceste efecte.
5. Se vor consemna toate elementele descrise anterior într-o comandă proforma sau într-o cerere de ofertă, astfel încât furnizorul să ştie din timp ce trebuie să ofere sistemul şi să facă promisiunea onorării tuturor cerinţelor.
6. De asigurat că serviciile garantate prin contract pot fi onorate într-un timp bine determinat, stabilind cu exactitate ce misiuni revin specialiştilor, definind obligaţiile

contractuale, responsabilităţile şi termenele de plată. De toate aceste aspecte trebuie să se ocupe o persoană ce va fi numită în acest sens.

Analizaţi modul în care se asigură securitatea echipamentelor într-o organizaţie cunoscută de dumneavoastră.

## 6.3 Securitatea software-ului

Softul unui calculator cuprinde instrucţiunile sub care funcţionează întregul sistem. Aceste instrucţiuni, sub formă de programe, îi vor spune calculatorului ce trebuie şi ce nu trebuie să facă cu datele, cum să le păstreze, ce regim au ieşirile din prelucrările intermediare sau finale. Întreaga activitate a calculatorului se va realiza prin intermediul programelor. Calculatorul nu poate gândi nicidecum. Din această cauză în soft vor fi incluse şi unele măsuri pe linia realizării securităţii.

### 6.3.1 Obiectivele securităţii prin software

Există trei funcţii principale pe care softul trebuie să încerce a le asigura. Ele se referă mai de grabă la confidenţialitatea datelor, decât la integritatea sau disponibilitatea lor.

1. *Accesul*. Softul trebuie să discearnă între utilizatorii autorizaţi şi intruşi, iar în ultimul caz să le blocheze accesul.
2. *Delimitarea*. Softul trebuie să delimiteze diversele activităţi ale utilizatorilor şi să îi trateze după nivelul lor de autorizare la categoriile speciale de date ce urmează a fi prelucrate. Ca atare, şi baza de date va fi compartimentată după reguli foarte riguroase pe linia securităţii sistemului.
3. *Auditarea*. Poate mai clar ar fi „proba auditării”, întrucât a treia funcţie se referă la capacitatea sistemului de a reţine ce persoane, cât timp, cu ce date au lucrat şi ce au urmărit.

Un soft de sistem eficient trebuie să blocheze relele intenţii, să prevină accesul neautorizat şi să înregistreze tot ce efectuează pentru a avea ulterior forţă probantă.

### 6.3.2 Limitele softului pentru asigurarea securităţii

O lungă perioadă de timp, de problemele securităţii sistemelor electronice de calcul s-au ocupat doar persoanele implicate în prelucrarea automată a datelor, însă de mai mult timp se simţea nevoia transferării lor în zona softului sistemelor, mutaţie ce a avut loc, dar căreia imediat a şi început să i se aducă obiecţiuni de genul:

- softul este foarte scump. Chiar şi programele destul de simple ocupă mii de linii-program, toate realizate de către om, dar cele de asigurare a securităţii sunt deosebit de complexe şi, firesc, de scumpe;
- de regulă, programele conţin şi erori;
- testele de verificare a lor nu sunt perfecte;
- softul pentru securitate diminuează capacităţile şi viteza de lucru a întregului sistem;
- producătorii de hard şi soft nu dispun de standarde pe linia securităţii sistemelor;
- utilizatorii nu au cunoştinţe suficient de detaliate despre hard şi soft încât să poată sesiza cele mai inteligente subtilităţi cu intenţie de fraudă incluse în softul cumpărat;

- eventualele disfuncţionalităţi ale softului pentru securitatea sistemului oferă posibilitatea specialiştilor în întreţinerea sistemului să intre în intimitatea lui, deci şi să-l poată influenţa;
- poate lucra perfect doar „la suprafaţă”, el conţinând aspecte esenţiale compromiţătoare invizibile;
- softul poate să conţină pericole deosebit de mari care nu pot fi sesizate şi nici nu sunt periculoase o lungă perioadă de timp de la instalarea lui (bombele logice, caii troieni ş.a.);
- „loviturile” prin soft sunt insesizabile prin mijloacele obişnuite de percepţie ale omului;
- în final, datorită curentului sistemelor deschise, a conectării într-o mare varietate de reţele şi a gestionării unor baze de date masive de către mii de persoane, măsurile de realizare a securităţii prin software pentru aceste sisteme gigant sunt extrem de greu de realizat.

În aceste condiţii, când cheltuielile sunt foarte mari, când cu mare greutate se asigură o oarecare doză de încredere în soft, apar ca fiind mai ieftine şi mai eficiente alte măsuri de realizare a securităţii sistemelor de prelucrare automată a datelor. Chiar dacă softul joacă un rol destul de important, nicidecum nu trebuie neglijate şi alte modalităţi. Până şi furnizorii spun că virtuţile softului sunt relativ dependente de calităţile beneficiarului, dar că măsuri sigure sunt cele de încuiere a uşilor, de urmărire a personalului ş.a.

Cât timp nici cele mai importante sisteme de prelucrare automată a datelor, cum sunt cele din domeniul militar sau bancar, nu au protecţie de 100%, apare ca o necesitate stringentă apelarea şi la alte metode. Şi încă un detaliu: cât timp hoţii au demonstrat că sunt mai puternici decât producătorii softului de securitate, cum să existe o încredere mai mare în ultimii, deci şi în produsele lor !?!

### 6.3.3 Măsuri generale de asigurare a securităţii softului

Practica menţionează o întreagă serie de măsuri de protejare a sistemului de operare şi a altor programe de la distrugeri sau acţiuni subversive, după cum urmează:

- toate activităţile de programare (modificare, scriere, utilizare etc.) trebuie să fie executate sub cele mai riguroase norme de disciplină, consemnate în scris la nivel de unitate şi prin contractul de angajare. Controlul activităţii de programare este foarte important pentru viitorul unităţii;
- programele deosebit de importante şi documentaţia aferentă trebuie să fie supuse aceloraşi reguli de protecţie fizică aşa cum au şi calculatoarele pe care se rulează;
- copiile de siguranţă ale programelor şi datele corespunzătoare, bineînţeles că nu trebuie uitată şi documentaţia, trebuie să fie păstrate în aceleaşi condiţii ca şi originalele;
- etapele realizării programelor trebuie să fie derulate sub un riguros control, verificate şi testate în toate stadiile de realizare, pentru asigurarea încrederii în rezultatul final;
- întregul proces de elaborare a programelor trebuie să fie însoţit de documentaţia aferentă;
- realizarea programelor se va efectua pe calculatoare care nu execută şi alte activităţi în acelaşi timp;
- programele trebuie să fie însoţite de numele realizatorilor lor sau ale celor ce le-au adus unele modificări;
- benzile şi discurile ce conţin sistemul de operare trebuie să fie identificabile dintr-o privire din multitudinea de suporturi de date, iar accesul la ele trebuie să fie foarte limitat, conform principiului „trebuie să ştie”;
- o copie de bază a sistemului de operare trebuie să fie păstrată în condiţii sigure de către responsabilul sistemului şi cel cu securitatea, sistemul de operare în uz fiind o copie a

acesteia, cu care, din când în când, se confruntă pentru a se depista eventualele modificări neautorizate;

- se impune utilizarea a cât mai multor teste şi rutine de securitate pentru a verifica integritatea sistemului de operare în folosinţă;
- nu trebuie să se permită crearea copiilor softului sistemului de operare de către personalul care utilizează sistemul, îndeosebi cel ce lucrează la distanţă. În acest scop, chiar sistemul de operare trebuie să conţină măsuri de autoprotecţie la intenţiile de copiere;
- orice „fisură" a sistemului de operare trebuie să fie adusă la cunoştinţă proiectanţilor sistemului, producătorilor de echipamente, utilizatorilor, iar gradul de expunere la riscuri trebuie să fie adus la cunoştinţă conducerii firmei;
- normele interne trebuie să prevadă ca mai mult de o persoană să se ocupe de implementarea şi testarea sistemului de operare, pentru reducerea riscului realizării unor activităţi subversive la nivel de persoană;
- iniţializarea sistemului de operare şi oprirea lui, de asemenea, presupun proceduri foarte riguroase de respectat. La fel se va proceda şi la reîncărcarea sistemului după o defecţiune;
- registrul sistemului trebuie să consemneze absolut toate operaţiunile la care acesta este supus în timpul funcţionării (defecţiuni, erori, căderi, reluări, pauze, timp lung de răspuns, semnale sonore neobişnuite ş.a.);
- nu trebuie lăsat sistemul să funcţioneze cu aşa-zisele „defecte acceptabile".

Primele bariere ridicate prin softul calculatorului sunt cele concepute pentru identificarea persoanelor care solicită permisiunea de utilizare a sistemului. Numai persoanelor autorizate trebuie să li se faciliteze accesul în sistem şi numai la anumite categorii de date. În acest context, un utilizator poate fi o persoană sau un grup de lucru la un proiect comun sau cu drepturi de exercitare a aceloraşi funcţii, rutine sau programe pe calculator.

Analizaţi modul în care se asigură securitatea software-ului într-o organizaţie cunoscută de dumneavoastră.

## 6.4 Securitatea personalului

Atunci când punem problema personalului ne gândim îndeosebi la angajaţii unităţii, dar tot aici pot fi incluse şi alte categorii din afară, capabile de orice. La nivelul anilor 2000, se înregistrau următoarele categorii de incidente sau de persoane producătoare de prejudicii:

1. *Violenţa*. De cele mai multe ori se concretizează prin amplasarea bombelor sau provocarea de incendii în centrele de prelucrare automată a datelor
2. *Furtul de obiecte*. Aici intră sustragerea unor obiecte cum sunt suporturile magnetice, terminalele, calculatoarele personale, îndeosebi laptopurile, semiconductorii şi nu banii.
3. *Delapidarea*. Angajaţii „şterpelesc" bani din sistemul informatic.
4. *Escrocheria*. Furnizorii de hard şi soft înşeală printr-o descriere eronată a produselor pe care le comercializează.
5. *Abuzul*. Angajaţii, apelând la statutul de utilizatori ai sistemului, folosesc resursele acestuia pentru plăceri personale sau pentru a obţine un profit.
6. *Modificarea*. Schimbarea înregistrărilor memorate.
7. *Spionajul*. Aici se încadrează spionajul industrial sau străin pentru a afla secretele de fabricaţie, programele sau manualele de utilizare.

8. *Violarea legislaţiei privind exportul*. Vânzarea componentelor hard şi soft deosebit de importante către potenţiale ţări străine ostile.
9. *Hackerii* sunt cei care trec frontierele sistemelor electronice, îndeosebi de calcul sau de telecomunicaţii.
10. *Phreakerii* (*phonecracker*) sunt cei ce prin abuz pătrund în sistemele de telefonie, separându-se de categoria hackeri.
11. *Crackerii* sunt cei ce sparg codurile de acces şi sistemele de apărare ale sistemelor electronice de calcul. Phreakerii şi crackerii sunt subspecializări ale hackerilor, dar mult mai periculoase.
12. *Lamer* desemnează categoria rataţilor în piraterii, de regulă, un hacker slab. Şi când sunt crackeri, neavând o „instrucţie" riguroasă, se comportă lamentabil, ca orice autodidact.
13. *Wannabe* reprezintă hackerii începători. Ei vor, dar nu prea pot, întrucât au cunoştinţe limitate. În schimb, dispun de un timp nelimitat şi fac zgomot despre succesele înregistrate, ceea ce contribuie la prinderea lor cu uşurinţă. În unele materiale ei sunt cunoscuţi şi sub numele de *script kiddies*.
14. *Respingerea* constă în indisponibilizarea resurselor sistemului de către angajaţi, prin sabotaj.
15. *Folosirea frauduloasă* a calculatoarelor pentru comiterea de crime, păstrarea unor evidenţe a materialelor interzise sau pornografice.
16. *Violarea copyright-ului* prin difuzarea ilegală a copiilor programelor.
17. *Infracţiuni economice sau legislative*, cum sunt violarea legilor antitrust, corupţie, mituire de către companiile producătoare de hard, soft, servicii.

Dintr-un studiu al cazurilor privind securitatea sistemelor informaţionale, efectuat între anii 1975-1985, s-a ajuns la următoarele concluzii:

Până în anii 1980, mobilul celor mai multe crime informatice îl constituia furtul de bani. Sumele variază de la aproximativ 50000 dolari, procuraţi prin introducerea unor date fictive de către funcţionarii sistemului, până la zeci de milioane de dolari, obţinuţi prin sistemul transferului electronic de fonduri. Tot în perioada anilor 1975-1978, la loc de frunte se află actele de spionaj, iar în 1976, îndeosebi în Europa, se înregistrează pierderi imense datorită bombardării sistemelor de prelucrare automată a datelor

În anii 1980-1981, se înregistrează cel mai mare nivel al furtului de circuite integrate din Silicon Valley, California, abundând piaţa cu astfel de componente, vândute ilegal.

În 1982, crima anului a fost din domeniul spionajului industrial, prin faptul că hoţii sustrăgeau secretele de fabricaţie pentru a câştiga, ulterior, piaţa.

În 1983, escrocheria se află pe locul întâi, producătorii dezinformând cumpărătorii pe linia performanţelor produselor scoase la vânzare.

În 1984, pe primul loc s-a situat încălcarea legilor referitoare la export, scoţându-se din SUA mari cantităţi de calculatoare, care erau sub embargo, şi erau livrate în Europa de Est şi URSS.

În 1985, încălcarea copyright-ului s-a aflat pe primul loc, cu scopul copierii neautorizate şi vânzării pe piaţă a copiilor pirat.

La nivelul anilor 1997-2002, din studiile întreprinse de Institutul de Securitate a Calculatoarelor şi FBI, rezultă că s-au produs mutaţii importante în domeniul atacurilor sau folosirii ilegale a sistemelor de prelucrare automată a datelor, conform situaţiei din tabelul 6.1. Pierderile înregistrate se regăsesc în tabelul 6.2. O situaţie similară este prezentată în tabelul 6.3, pentru perioada 2003 – 2007.

Cei chestionaţi au declarat că sursele de atac sunt din următoarele categorii: angajaţi nemulţumiţi (89%), hackeri independenţi (72%), corporaţii de pe teritoriul SUA (48%), corporaţii străine (29%), organizaţii guvernamentale străine (21%).

*Tabel nr. 6.1 – Tipuri de acţiuni frauduloase în domeniul informaţiilor*

| Tipul acţiunii frauduloase | Număr respondenţi cu pierderi* | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 |
| Furtul datelor personale | 21 | 20 | 23 | 22 | 32 | 26 | 61 |
| Sabotarea datelor din reţea | 14 | 25 | 27 | 28 | 26 | 28 | 61 |
| Interceptarea telecomunicaţiilor | 8 | 10 | 10 | 15 | 16 | 5 | - |
| Penetrarea sistemului din afară | 22 | 19 | 28 | 29 | 42 | 59 | 88 |
| Accesarea abuzivă a reţelei din interior | 55 | 67 | 81 | 91 | 98 | 89 | 180 |
| Fraudă financiară | 26 | 29 | 27 | 34 | 21 | 25 | 61 |
| Respingerea serviciilor solicitate | - | 36 | 28 | 46 | 35 | 62 | 111 |
| Înşelătorii | 4 | - | - | - | - | - | - |
| Viruşi | 165 | 143 | 116 | 162 | 186 | 178 | 254 |
| Acces neautorizat din interiorul sistemului | 22 | 18 | 25 | 20 | 22 | 15 | 72 |
| Fraudă în telecomunicaţii | 35 | 32 | 29 | 19 | 18 | 16 | 34 |
| Interceptarea activă a comunicaţiilor | - | 5 | 1 | 1 | 0 | 0 | - |
| Furturi de laptopuri | 165 | 162 | 150 | 174 | 143 | 134 | 250 |

* Au fost primite răspunsuri de la peste 500 de organizaţii

*Sursa*: Datele sunt preluate de pe site-ul Computer Security Institute, „2002 CSI/FBI Computer Crime and Security Survey", vol. VIII, no. 1, Spring 2002 şi raportul CSI/FBI din 2003

*Tabel nr. 6.2 – Total pierderi anuale din frauda informaţională, 1997 - 2002*

| Tipul acţiunii frauduloase | Total pierderi anuale* | | | | | |
|---|---|---|---|---|---|---|
| | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 |
| Furtul datelor personale | 20048000 | 33545000 | 42496000 | 66708000 | 151230100 | 170827000 |
| Sabotarea datelor din reţea | 4285850 | 2142000 | 4421000 | 27148000 | 5183100 | 15134000 |
| Interceptarea telecomunicaţiilor | 1181000 | 562000 | 765000 | 991200 | 886000 | 6015000 |
| Penetrarea sistemului din afară | 2911700 | 1637000 | 2885000 | 7104000 | 19066600 | 13055000 |
| Accesarea abuzivă a reţelei din interior | 1006750 | 3720000 | 7576000 | 27984740 | 35001650 | 50099000 |
| Fraudă financiară | 24892000 | 11239000 | 39706000 | 55996000 | 92935500 | 115753000 |
| Respingerea serviciilor solicitate | - | 2787000 | 3255000 | 8247500 | 4283600 | 18370500 |
| Înşelătorii | 512000 | - | - | - | - | - |
| Viruşi | 12948150 | 7874000 | 5274000 | 29171700 | 45288150 | 49979000 |
| Acces neautorizat din interiorul sistemului | 3991605 | 50565000 | 3567000 | 22554500 | 6064000 | 4503000 |
| Fraudă în telecomunicaţii | 22660300 | 17256000 | 773000 | 4028000 | 9041000 | 346000 |
| Interceptarea activă a comunicaţiilor | - | 245000 | 20000 | 5000000 | 0 | 0 |
| Furturi de laptopuri | 6132200 | 5250000 | 13038000 | 10404300 | 8849000 | 11766500 |
| Total | 100119555 | 136882000 | 123799000 | 265586240 | 377828700 | 455848000 |

* Au fost primite răspunsuri de la peste 500 de organizaţii

*Sursa*: Datele sunt preluate de pe site-ul Computer Security Institute, „2002 CSI/FBI Computer Crime and Security Survey", vol. VIII, no. 1, Spring 2002

La nivelul anului 2007, studiul realizat de Institutul de Securitate a Calculatoarelor arată că:

- principala generatoare de pierderi la nivelul celor aproape 500 de companii analizate este *frauda financiară*, care a surclasat, pentru prima dată după 7 ani, atacurile viruşilor;
- atacurile prin malware devin din ce în ce mai focalizate, adresându-se unor ţinte concrete;
- utilizarea abuzivă, în interes personal, a reţelelor şi sistemelor de e-mail ale organizaţiilor de către angajaţi, pentru pornografie şi descărcare ilegală de software, este problema cea mai stringentă.

*Tabel nr. 6.3 – Total pierderi anuale din frauda informaţională, 2003 - 2007*

| Tipul acţiunii frauduloase | Total pierderi anuale* | | | | |
|---|---|---|---|---|---|
| | 2003 | 2004 | 2005 | 2006 | 2007 |
| Furtul datelor confidenţiale (în 2007 cu excepţia furtului de dispozitive mobile) | - | - | - | 6034000 | 5685000 |
| Furtul datelor personale | 70195900 | 11460000 | 30933000 | - | - |
| Sabotarea datelor din reţea | 5148500 | 871000 | 340600 | 260000 | 1056000 |
| Penetrarea sistemului din afară | 2754400 | 901500 | 841400 | 758000 | 6875000 |
| Accesarea abuzivă a reţelei şi a sistemului e-mail din interior | 11767200 | 10601055 | 6856450 | 1849810 | 2889700 |
| Fraudă financiară | 10186400 | 7670500 | 2565000 | 2556900 | 21124750 |
| Respingerea serviciilor solicitate (DoS) | 65643300 | 26064050 | 7310725 | 2992010 | 2888600 |
| Viruşi (viermi,spyware) | 27382340 | 55053900 | 42787767 | 15691460 | 8391800 |
| Acces neautorizat din interiorul sistemului | 406300 | 4278205 | - | - | 1042700 |
| Fraudă în telecomunicaţii | 701500 | 3997500 | 242000 | 1262410 | 651000 |
| Furturi de laptopuri sau dispozitive mobile | 6830500 | 6734500 | 4107300 | 6642660 | 3881150 |
| Phishing | - | - | - | 647510 | 2752000 |
| „Zombie" (bot) în interiorul organizaţei | - | - | - | 923700 | 2869600 |
| Furtul informaţiilor proprietarilor prin furtul dispozitivelor mobile | - | - | - | - | 2345000 |
| Furtul informaţiilor confidenţiale prin furtul dispozitivelor mobile | - | - | - | - | 2203000 |
| Modificarea site-urilor Web | - | 958100 | 115000 | 162500 | 725300 |
| Folosirea abuzivă a reţelelor wireless | - | 10159250 | 544700 | 469010 | 542850 |
| Folosirea abuzivă a mesageriei instant | - | - | - | 291510 | |
| Folosirea abuzivă a aplicaţiilor Web publice | - | 2747000 | 2227500 | 269500 | 251000 |
| Sniffing de parole | - | - | - | 161210 | 168100 |
| Şantaj | - | - | - | - | 160000 |
| Atacuri exploit asupra serverului DNS | - | - | - | 90100 | 104500 |
| Acces neautorizat la informaţii | - | - | 31233100 | 1061700 | - |
| Ascultarea convorbirilor telefonice | 76000 | - | - | - | - |
| Interceptarea activă a convorbirilor telefonice | 705000 | - | - | - | - |
| Altele | - | - | - | 885000 | - |
| Total | 201797340 | 141496560 | 130104542 | 52494290 | 66930950 |

* Numărul de organizaţii care au răspuns sondajului variază (2003:251, 2004:269, 2005:639, 2006:313, 2007:194)

*Sursa*: Datele sunt preluate de pe site-ul Computer Security Institute, rapoartele CSI/FBI din perioada 2003 – 2007. Din păcate, din 2008 rapoartele nu mai sunt oferite decât contra cost.

În 2008, Robert Richardson, directorul CSI, a publicat un alt raport în care prezintă ponderile diverselor tipuri de atacuri în totalul incidentelor de securitate apărute în interiorul a peste 500 de organizaţii:

*Tabel nr. 6.4 – Ponderile atacurilor în totalul incidentelor de securitate, 2004 - 2008*

| Tipul acţiunii frauduloase | 2004 | 2005 | 2006 | 2007 | 2008 |
|---|---|---|---|---|---|

| Tipul acţiunii frauduloase | 2004 | 2005 | 2006 | 2007 | 2008 |
|---|---|---|---|---|---|
| Respingerea serviciilor solicitate (DoS) | 39% | 32% | 25% | 25% | 21% |
| Furturi de laptopuri | 49% | 48% | 47% | 50% | 42% |
| Fraudă în telecomunicaţii | 10% | 10% | 8% | 5% | 5% |
| Acces neautorizat | 37% | 32% | 32% | 25% | 29% |
| Viruşi (viermi,spyware) | 78% | 74% | 65% | 52% | 50% |
| Fraudă financiară | 8% | 7% | 9% | 12% | 12% |
| Accesarea abuzivă a sistemului din interior | 59% | 48% | 42% | 59% | 44% |
| Penetrarea sistemului din afară | 17% | 14% | 15% | 13% | 13% |
| Sabotarea | 5% | 2% | 3% | 4% | 2% |
| Furtul informaţiilor proprietarilor | 10% | 9% | 9% | 8% | 9% |
| • prin furtul dispozitivelor mobile | | | | | 4% |
| • din alte surse | | | | | 5% |
| Folosirea abuzivă a reţelelor wireless | 15% | 16% | 14% | 17% | 14% |
| Modificarea site-urilor Web | 7% | 5% | 6% | 10% | 6% |
| Folosirea abuzivă a aplicaţiilor Web | 10% | 5% | 6% | 95 | 11% |
| „Zombie" (bot) în interiorul organizaţei | | | | 21% | 20% |
| Atacuri asupra serverului DNS | | | | 6% | 8% |
| Folosirea abuzivă a mesageriei instant | | | | 25% | 21% |
| Sniffing de parole | | | | 10% | 9% |
| Pierderea sau furtul datelor clienţilor | | | | 17% | 17% |
| • de pe dispozitivele mobile | | | | | 8% |
| • din alte surse | | | | | 8% |

* Au fost primite răspunsuri de la peste 500 de organizaţii

*Sursa*: Datele sunt preluate de pe site-ul Computer Security Institute, „2008 CSI Computer Crime and Security Survey",

Extrageţi câteva tendinţe din tabelele de mai sus. Comentaţi-le.

### 6.4.1 Responsabilităţi manageriale pe linia personalului

Pe linia asigurării securităţii din punctul de vedere al personalului trebuie să se urmărească următoarele aspecte:

- selecţia;
- verificarea prin prisma securităţii;
- supravegherea continuă;
- instruirea şi conştientizarea.

În mediile de lucru cu calculatoare, există principii fundamentale care guvernează problematica măsurilor de securitate pe linie de personal, cum sunt:

1. *Principiul „trebuie să ştie"* face ca posesia sau cunoaşterea informaţiilor, indiferent de categoria din care fac parte, să fie limitată strict şi să fie înlesnită doar celor care au atât autorizarea, cât şi nevoia evidentă de a le şti, astfel încât să-şi poată exercita corect sarcinile de serviciu. Statutul deosebit al unei persoane în firmă nu-i conferă şi dreptul nelimitat de cunoaştere a informaţiilor speciale. De asemenea, într-un astfel de caz nu va fi pusă problema „respectării vârstei".
2. *Principiul „trebuie să meargă"* limitează accesul personalului în zone diferite de lucru din unitate, în special în centrele de prelucrare automată a datelor, lăsând acces liber

doar celor care trebuie să meargă în aceste locuri pentru a-şi exercita sarcinile de serviciu. Controlul trebuie să fie la fel de riguros şi în zonele unde sunt păstrate datele, chiar dacă unii invocă faptul că fac parte din categoria utilizatorilor acestora.

3. *Principiul „celor două persoane"* vine să preîntâmpine posibilitatea ca o singură persoană să comită acte ilegale în sistem, îndeosebi prin operaţiuni importante. Chiar dacă o persoană răspunde de exercitarea unor atribuţii de serviciu, ea va efectua activităţi speciale numai în prezenţa unei persoane autorizate. Aceasta nu înseamnă un membru al echipei de pază, ci o persoană cu cel puţin aceleaşi cunoştinţe profesionale cu ale executantului de drept. Activităţile speciale, neexecutabile de o singură persoană vor fi prezentate ulterior. Pentru preîntâmpinarea „înţelegerilor" dintre cele două persoane, se recomandă schimbarea lor cât mai des posibil.
4. *Principiul schimbării obligaţiilor de serviciu* consemnează că o persoană nu trebuie să exercite o perioadă prea lungă de timp aceleaşi sarcini de serviciu.

### 6.4.2 Măsuri pe linia securităţii din punct de vedere al personalului

În vederea asigurării unor măsuri deosebite pe linia securităţii din punct de vedere al personalului, se impune parcurgerea unor stadii:

**Stadiul 1:** *Identificarea locurilor de muncă cu regim special şi a calităţilor persoanelor îndreptăţite a le ocupa*

**Stadiul 2:** *Selecţia personalului*

Operaţiunea se va realiza înainte de angajare, în timpul procesului de recrutare de personal nou, dar şi retroactiv.

Dacă actele la angajare sunt completate corect, unitatea poate să-şi găsească suficiente elemente pentru filtrarea personalului. Documentele de angajare vor conţine date medicale şi informaţii generale despre persoană. Date suplimentare pot fi oferite de referinţele obţinute de la precedentul loc de muncă şi apoi de la o persoană care să reprezinte o instituţie credibilă (şcoală, justiţie, poliţie, armată). Dacă se consideră necesar pot fi efectuate şi investigări prin firme private.

Totuşi, multe elemente edificatoare se pot obţine prin intervievarea solicitanţilor de locuri de muncă. Aspectele urmărite pot fi structurate astfel:

1. Descrierea locului de muncă anterior, funcţia deţinută, evoluţia profesională. Se vor urmări, îndeosebi, eventualele întreruperi de activitate, altele decât concediile sau diverse motive obiective. Spitalizările şi arestările vor fi urmărite cu mare atenţie pentru aflarea cauzei acestora.
2. Verificarea referinţelor şi a diplomelor depuse la dosar. Sunt foarte dese cazurile de declaraţii false despre o vechime avută la unităţi inexistente sau diplome de la aşa-zisele „şcoli ale vieţii". Nimic nu va fi crezut fără probe suplimentare.

   Se va continua cu determinarea:

   a) *competenţei*. Diplomele ataşate, cu note foarte mari pe ele, nu au acoperire în calităţile profesionale ale persoanei – constatare efectuată prin probe de lucru asemănătoare ultimului loc de muncă, precum şi rezolvarea unor stări imprevizibile.
   b) *punctualitatea* şi *absenteismul* vor scoate în relief câtă încredere i se poate acorda individului.
   c) *abaterile disciplinare* vor încerca să evidenţieze posibilitatea încadrării persoanei în legalitate, în normele de conduită socială (dacă a fost amendat, dacă a avut procese civile sau penale).
   d) *situaţia medicală* va scoate la lumină stările de instabilitate mentală, bolile cronice care pot să aibă o motivaţie socială sau financiară pentru solicitanţii posturilor.

Calea prin care se pot obţine aceste informaţii constă în oferirea unei poliţe de asigurare de viaţă, plătită de firmă, care necesită o examinare medicală.

e) care este cauza părăsirii vechiului loc de muncă?
f) fostul loc de muncă l-ar primi din nou pe solicitant sau i-ar cere referinţe suplimentare?
g) există obligaţii ale solicitantului faţă de fosta unitate?
h) persoana a mai fost angajată la companii private şi, dacă da, când şi de ce le-a părăsit?
i) care au fost relaţiile cu foştii colegi de muncă - a fost posibilă integrarea în echipă? Era agreat şi respectat? Avea conflicte cu reprezentanţii unor grupuri de persoane? Dacă este programator, există cazuri când din cauza unui program de-al său să se fi blocat activitatea întregului centru de prelucrare?

3. Originea individului, modul său de existenţă, persoanele cunoscute, legăturile sale de familie au ceva în comun cu concurenţii firmei la care cere angajarea? Pentru străini se pot solicita şi actele doveditoare ale naţionalităţii.
4. Există unele indicii ale consumului abuziv de alcool sau droguri?
5. Solicitantul este membru în asociaţii profesionale sau economice? Are puncte de vedere politice foarte puternic susţinute, care? A exercitat anterior unele activităţi publice sau funcţionăreşti (consultant, reprezentant sindical ş.a.) care să-i fi întrerupt preocupările profesionale sau să-l determine să fie uşor influenţabil în rezolvarea unor posibile conflicte viitoare?
6. Care îi este viaţa de familie? Ce activităţi sociale şi sportive îi plac? Dau ele semne de sănătate excesivă sau chiar inexplicabilă, indică o extravaganţă ieşită din comun?
7. Comportamentul la volan, în ipostaza de conducător auto, poate să scoată în relief stări emotive sau de maturitate, controlabilitate, judecată rapidă ş.a.
8. Dacă este posibil, se va studia situaţia financiară a solicitantului (dacă are împrumuturi pe perioade lungi sau scurte, dacă are cartele de credit sau de debit, dacă face parte din cercuri financiare). Sunt servicii speciale care pot oferi astfel de informaţii.
9. Dacă a lucrat în poliţie sau armată, trebuie urmărită (cu probe) cauza întreruperii acestor activităţi.

Literatura recomandă apelarea la companii private care să exercite astfel de activităţi pentru aflarea informaţiilor reale despre solicitanţii locurilor de muncă. De asemenea, într-o oarecare măsură, se poate folosi şi detectorul de minciuni, deşi nu trebuie să se pună prea mare bază pe ceea ce indică acesta.

Se poate apela la formularea unor teste de personalitate sau psihometrice, din care să rezulte calităţile de care dă dovadă individul. Testul este foarte bun dacă la sfârşit se va comunica şi participanţilor rezultatul, pentru a-şi afla punctele tari sau slabe.

În final, câteva cuvinte despre referinţele aduse de angajaţi şi scrisorile de recomandare:

1. Referinţele se află sub controlul candidatului la concurs, el rugând pe cineva să le formuleze, deci sunt uşor părtinitoare.
2. Obiectivele urmărite de actuala firmă, interesată să angajeze, nu se pot regăsi printre elementele referinţelor. Totuşi, o referinţă bună trebuie să scoată în relief calităţile de care poate da dovadă persoana, iar cel mai des se întâmplă când se încearcă a se scăpa de salariaţii slabi; o referinţă categoric proastă este cea care scoate în relief calităţile deosebite ale persoanelor, dar care nu au posibilitatea să fie demonstrate în mediul de lucru existent.
3. Referinţele sunt scrise în „limbaje” diferite, în funcţie de stilul persoanei, deseori fiind necesară interpretarea cu atenţie a diverselor construcţii, de genul „a încercat din greu” (eşec), „a obţinut rezultate mulţumitoare” (rezervă), „a demonstrat o inteligenţă medie” (mai mulţi colţi decât idei), „în general s-a achitat de sarcinile…” (în loc de critică sau

„despre cei plecaţi numai de bine"). La astfel de exprimări angajările aproape că nu au motivaţie.

**Stadiul 3:** *Atribuirea responsabilităţilor pe linia securităţii*

După cum informaţiile unui sistem fac parte din categorii diferite, la fel şi persoanele care lucrează cu ele trebuie să fie grupate ca atare. În vederea adjudecării posturilor-cheie pe linie de securitate a datelor, trebuie să se ştie că există trei categorii de angajaţi:

1. *Neverificabilii* sunt acei angajaţi cu un statut nu prea clar, ei neputând fi verificaţi în detaliu prin prisma onestităţii, încrederii, integrităţii, loialităţii faţă de unitate – motiv pentru care lor nu li se poate acorda accesul la informaţiile speciale ale firmei.
2. *Fără dubii*. Într-o astfel de categorie intră persoanele care au trecut cu brio toate verificările efectuate asupra lor (în limitele controalelor exercitate) şi li se pot oferi anumite sarcini pe linia accesului la o parte a informaţiilor speciale.
3. *Extrem de credibili*. După verificări complexe asupra trecutului unei persoane, ale familiei sale, vieţii personale, moralităţii şi rezultatelor înregistrate la vechile locuri de muncă, dacă totul este perfect, aceasta poate fi considerată de încredere şi i se poate facilita accesul la cele mai intime date ale firmei. Adevărul este că încrederea şi onestitatea pot fi verificate pe parcurs, şi nu la data efectuării verificărilor, ceea ce înseamnă o oarecare doză de risc din partea celor ce deleagă astfel de responsabilităţi.

În orice caz, altfel vor fi trataţi angajaţii cu vechime în unitate şi altfel cei angajaţi de curând sau cu regim sezonier, sau cu jumătate de normă.

**Stadiul 4:** *Proceduri la angajare*

Într-un contract de angajare a unui salariat trebuie să se stipuleze cu claritate următoarele:

1. responsabilităţile persoanei şi sarcinile pe linia asigurării securităţii valorilor patrimoniale şi, bineînţeles, a informaţiilor, astfel încât:
   a) să dispară orice dubiu privind persoana care trebuie să exercite o funcţie anume;
   b) să aducă la cunoştinţa angajaţilor, din faza de asociere cu unitatea, ce probleme caracterizează activitatea firmei;
   c) să-i pregătească pentru dobândirea unor calităţi noi, cerute de unitatea care angajează;
2. regulamentul de ordine interioară a unităţii şi condiţiile în care încetează contractul de muncă;
3. restricţii privind comportamentul persoanei în cazul încetării contractului de muncă, îndeosebi pe linia nedezvăluirii informaţiilor speciale competitorilor actualei firme, respectându-se aşa-zisa „clauză a confidenţialităţii";
4. aducerea la cunoştinţă a documentaţiilor de specialitate, a documentelor, a situaţiilor de întocmit, care trebuie să aibă aprobarea în avans a şefului său.

Angajatul trebuie să semneze contractul, ceea ce înseamnă că l-a citit, l-a înţeles, inclusiv că a luat cunoştinţă de problemele securităţii sistemului. După acest moment, de regulă, urmează o perioadă de probă, de până la trei-şase luni, după care se va face pronunţarea privind statutul definitiv al persoanei.

**Stadiul 5:** *Instruirea şi conştientizarea personalului*

Pentru atingerea obiectivului acestui stadiu se stabilesc programe speciale de instruire şi conştientizare pentru asigurarea încrederii în personalul unităţii pe linia asigurării securităţii sistemului de prelucrare automată a datelor În acest scop, se pot folosi numeroase modalităţi de ducere la îndeplinire a obiectivului: de la cursuri cu durate şi termene fixe, până la pavoazări la tot pasul a interiorului unităţii ş.a.

**Stadiul 6:** *Supravegherea*

Unităţile mai mari au în uz sisteme programate de evaluare a performanţelor angajaţilor, astfel încât să-i poată orienta profesional cât mai corect şi pentru a face promovările cele mai motivate. Tot printr-un astfel de sistem se va efectua şi urmărirea aspectelor referitoare la

încrederea în persoane şi poziţia lor faţă de securitatea sistemului, evitându-se incidentele nefericite din sistemele de prelucrare automată a datelor.

Cu caracter neplanificat sunt urmăririle şi supravegherile zilnice ale personalului, pentru descoperirea potenţialelor pericole din partea salariaţilor.

În caz de promovare, se vor face reevaluări ale sarcinilor pe linia securităţii informaţiilor.

Programul de educaţie privind securitatea îşi propune să contribuie la creşterea vigilenţei personalului şi să declare orice vede ca fiind împotriva securităţii firmei, indiferent de poziţia persoanei implicate în aşa-ceva.

**Stadiul 7:** *Încetarea contractului de muncă*

Procedurile legale de încetare a contractului de muncă trebuie să fie introduse pentru persoanele care părăsesc unitatea în astfel de condiţii, un rol esenţial revenind acordurilor dintre părţi în regim post-angajare a persoanei, îndeosebi raportul fostului angajat cu concurenţii firmei.

După recuperarea cheilor de acces urmează anularea parolelor de intrare în sistemele de prelucrare automată a datelor. În acelaşi timp, restul angajaţilor trebuie să fie anunţaţi că persoana respectivă nu mai are statutul de salariat al firmei, deci relaţiile lor de serviciu sunt anulate. Se recomandă, chiar, efectuarea unor schimbări ale posturilor de lucru din mediul din care a plecat o persoană.

**Stadiul 8:** *Consideraţii finale*

1. *Contractul angajaţilor*. Nu trataţi oamenii ca şi cum ei au fost angajaţi la o companie, ci ca şi când ar lucra la propria lor firmă. Acordaţi o atenţie deosebită personalului de întreţinere a sistemului, personalului care efectuează curăţenia, care pătrund în centrele de prelucrare automată a datelor fără să aibă supravegheri speciale. Identic se va proceda şi în cazul consultanţilor din afară.
2. *Operatorii de la terminale* nu trebuie să fie omişi cât de periculoşi pot fi pentru sistem, îndeosebi pentru faptul că pot să-şi păstreze anonimatul. O grijă deosebită trebuie să se acorde şi personalului care lucrează la întreţinerea terminalelor.
3. *Vizitatorii*. Toate persoanele care pătrund în mediul sistemelor de prelucrare automată a datelor, fie că sunt cunoscute sau de ocazie, trebuie să fie supuse procedurilor de asigurare a securităţii sistemului, efectuându-se, chiar, verificarea lor şi admiterea sau nu a pătrunderii în sistem. Se recomandă ca vizita lor să aibă loc numai însoţit de un reprezentant al firmei.
4. *„Controlul extern" asupra angajaţilor*. Pot fi situaţii când persoane care nu sunt abilitate cu cunoştinţe elementare de prelucrare automată a datelor să poată fi foarte periculoase pentru securitatea sistemului, fiind ghidate de cineva din afara unităţii asupra modului cum trebuie să procedeze.
5. *Acţiuni hotărâte*. Dacă asupra unei persoane sunt unele dubii privind securitatea, nu trebuie lăsat timpul să-şi spună cuvântul, încercând să ne convingem de realitatea bănuielilor, ci trebuie acţionat dintr-o dată. Parolele de acces ale persoanelor autorizate pot fi retrase de responsabilul cu securitatea sistemului fără să-i anunţe în prealabil pe cei deposedaţi, bineînţeles, dacă există motive de bănuială asupra loialităţii.
6. *Tratamentul loial în sens descendent şi ascendent (pe bază de reciprocitate)*. Angajatorii trebuie să-şi trateze angajaţii corect şi onest ca să se aştepte să fie trataţi în mod similar. În special, personalul din domeniul prelucrării automate a datelor, care este deosebit de inteligent, are nevoie de un astfel de tratament.
7. *Vizite ale locului de muncă*. Perspectiva de jos este cu totul diferit văzută de cei de sus, de aceea ei trebuie să coboare la nivelul locurilor de execuţie din ateliere. Se spune că şi vulturul dacă este privit de sus este greu de observat, dar de jos, pe fondul cerului silueta lui este foarte clară.

8. *Te faci că-i plăteşti, se fac că muncesc şi că sunt corecţi*. Încrederea personalului poate fi câştigată prin recompensarea lor la cote ridicate, scoţându-le în relief valoarea lor şi câştigându-le încrederea.
9. *Nu jucaţi fals*. În istoria securităţii sistemelor, persoanele care au oferit cele mai multe „cacealmale" angajaţilor au fost şi cele mai des furate sau spionate.
10. *Lăsaţi, totuşi, unele portiţe de ieşire pentru situaţii deosebite*. Personalul nu trebuie să se teamă atât de tare de consecinţele unor încălcări, din neglijenţă, a măsurilor de securitate. Măsurile exagerate nu aduc întotdeauna cele mai bune rezultate. Nu puneţi mare preţ pe anonime, dar nici nu le neglijaţi.
11. *Nu crede fără să cercetezi*. Niciodată nu se recomandă să se facă presupuneri, fără să se cerceteze fondul problemei. Presupunerea, deseori, este primul pas spre „mocirlă".
12. *Bazează-te, totuşi, pe judecată şi instinct*, ceea ce înseamnă că dacă ai văzut un animal care seamănă cu lupul, umblă în haită cu lupii, urlă ca lupii, sigur el e lup!

Celor ce intenţionează să-şi găsească un loc de muncă adecvat cunoştinţelor acumulate de-a lungul anilor, dar şi pentru firmele interesate să găsească pe cei mai buni specialişti în securitatea sistemelor, le recomandăm să consulte două site-uri foarte cunoscute pe Internet: *dice.com* şi *monster.com*.

- Dacă aţi face parte dintr-o comisie de selecţie a candidaţilor pentru un post de **director de sucursală bancară**, **ce elemente aţi folosi în intervievarea** lor, în aşa fel încât să angajaţi o persoană cât mai potrivită din punctul de vedere al securităţii informaţionale? Daţi exemple de **4 informaţii sensibile (confidenţiale sau secrete)** cu care intră în contact un **director de sucursală bancară**, justificând motivul pentru care consideraţi importante respectivele informaţii. Menţionaţi **2 măsuri** pe care le puteţi lua pentru a vă feri de divulgarea acestor informaţii de către proaspătul angajat.
- Reluaţi exemplul de mai sus pentru un **agent de vânzare**, un **contabil şef** şi un **administrator de bază de date**.

## 6.5 Securitatea la nivelul întregului sistem informatic

Un sistem informatic de încredere este format din totalitatea echipamentelor, programelor, componentelor fizice realizate prin soft (firmware) şi a mecanismelor procedurale care concură la asigurarea securităţii prelucrării automate a datelor.

În SUA, Centrul de Apărare a Securităţii Calculatoarelor al Agenţiei Naţionale de Securitate a emis unele recomandări astfel încât să se ştie ce înseamnă o bază informatică de încredere. Prin intermediul lor, centrul a stabilit *clase de evaluare* în care să poată fi încadrate produsele de realizare a securităţii sistemelor informatice, după ce sunt supuse unor teste speciale. Astfel, au fost definite patru clase, de la D la A, şi câteva subclase, cum ar fi A1 şi A2. Clasa D este cea mai de jos. În cadrul claselor, numerele mai mari sugerează un sistem mai sigur.

Clasele şi subclasele stabilite sunt:

D. Nesigure sau neevaluate.

C. Capabil să asigure controlul accesului discreţionar.

C1. Orice sistem de operare comercial care asigură separarea fazelor de execuţie ale sistemului de cele ale utilizatorilor obişnuiţi.

C2. Orice sistem de operare comercial dublat de un pachet suplimentar pentru asigurarea securităţii.

B. Capabil să realizeze controlul obligatoriu al accesului.

B1. Toate informaţiile sunt astfel etichetate încât să corespundă unei anumite categorii de securitate.

B2. Securitatea organică. Echipamentele şi softul sunt concepute şi realizate astfel încât să asigure o securitate obligatorie.

B3. Domenii de securitate. Similar cu B2, numai că este mai bună prin extinderea componentelor cărora li se asigură securitatea.

A. Securitatea verificată. Măsurile de securitate sunt consemnate în scris şi aprobate ca fiind eficiente.

A1. Verificarea proiectării. De regulă, înseamnă controlul codurilor-sursă din programele de sistem care au funcţii de securitate.

A2. Verificarea implementării. În acest caz sunt examinate programele de sistem executabile şi se urmăreşte dacă ele coincid cu codul-sursă verificat.

### 6.5.1 Izolarea sistemelor informatice

Obiectivul principal al creării unor bariere izolatoare pentru sistemele informatice constă în luarea unor măsuri care să prevină posibilitatea utilizatorilor de programe de a efectua unele schimbări în condiţiile lor de execuţie sau a datelor prelucrate, de a specifica statutul, actual şi viitor, al celorlalţi utilizatori ai programului sau de a prelua controlul asupra datelor altora, ca o excepţie de la regulile normale de acces.

Pentru realizarea acestor obiective, fiecare adresă de program al utilizatorului, numele programatorului, conţinutul registrelor, datele utilizatorilor trebuie să fie protejate împotriva folosirilor neautorizate, în sensul neasigurării transparenţei lor atunci când altui utilizator i se va aloca acelaşi spaţiu de lucru.

Pentru ca un sistem informatic să fie considerat asigurat din punctul de vedere al izolării lui, trebuie să fie îndeplinite două condiţii:

1. să se folosească un anumit mod de asigurare a securităţii prelucrării pentru a izola sistemul de inamicii săi din afară;
2. să se apeleze la strategii de apărare, prin izolarea utilizatorilor între ei şi de sistemul de operare al calculatorului. Utilizatorii care prelucrează date ce aparţin categoriilor speciale trebuie să fie izolaţi în mod deosebit.

Sunt posibil de aplicat cel puţin şase strategii de izolare, ele putând fi mai multe. În categoria celor şase intră:

- selectarea modului de prelucrare;
- izolarea temporară;
- izolarea spaţială;
- izolarea realizată prin caracteristicile arhitecturii sistemului;
- izolarea criptografică;
- restricţii la privilegiile sistemului.

*Selectarea modului de prelucrare*. Atunci când prelucrarea se efectuează în mod local sau în sistem de teleprelucrare, de către unul sau mai mulţi utilizatori în acelaşi timp (în mod serial sau multiprogramare), accesul direct (on-line) sau prin programare sau neprogramare influenţează, în mod vădit, gradul de izolare a sistemului.

*Izolarea temporară* se aplică, de regulă, în cazul prelucrărilor speciale, dar poate fi folosită şi în modul multiprogramare asupra terminalelor ce intră sau ies într-o/dintr-o reţea, în funcţie de un calendar, care se întocmeşte luând în considerare categoria datelor şi principiul „trebuie să ştie”.

*Izolarea spaţială* se realizează prin dedicarea componentelor de prelucrare şi izolarea lor faţă de un alt utilizator.

*Arhitectura sistemului* este cea care facilitează multiprogramarea, contribuind la izolarea utilizatorilor faţă de sistemul de operare şi între ei înşişi, asigurându-se prelucrarea datelor secrete pe niveluri de securitate.

*Izolarea criptografică* este folosită, în principal, pentru realizarea izolării prelucrărilor de la distanţă de intruşii din afară, atunci când liniile de comunicaţie depăşesc perimetrul de securitate. Ea poate fi folosită, de asemenea, pentru izolarea utilizatorilor din sistem, în special atunci când aceştia au niveluri diferite de responsabilitate pe linia securităţii.

*Restricţiile de privilegiu* constituie o cale de identificare distinctă a utilizatorilor-programatori de cei neprogramatori. Eficienţa procedurilor se realizează prin arhitectura sistemului.

## 6.5.2 Controlul accesului sistemelor informatice

Controlul accesului la sistemele de prelucrare automată a datelor este un act de decizie a conducerii. În ultimă instanţă, şeful unei companii are responsabilitatea definirii informaţiilor care trebuie să se afle sub control, cine să-l efectueze, prin ce persoane şi în ce condiţii se atribuie drepturi speciale de control şi cum pot fi ele revocate. În practică, responsabilitatea se deleagă spre nivelurile inferioare, spre şefii compartimentelor şi administratori.

În fiecare regulă privind accesul trebuie să se reflecte două principii esenţiale:

1. *Privilegiul minim*. Numai acele informaţii sau operaţiuni de prelucrare pe care utilizatorul trebuie să le exercite şi îi revin ca sarcini de serviciu vor fi lăsate la dispoziţia sa, iar ele vor fi stabilite de responsabilii de drept, şi nu de utilizator.
2. *Expunerea minimă*. Din momentul în care un utilizator are acces la informaţii speciale sau la alte materiale cu regim similar, acesta are responsabilitatea de a le proteja. Nici o altă persoană, în timpul sesiunii de lucru, nu va trebui să ia cunoştinţă de ceea ce se prelucrează, se memorează sau se transmite în altă parte. Mai mult chiar, o atenţie deosebită se va acorda restricţiilor referitoare la măsurile de securitate, îndeosebi la caracteristicile deosebit de performante sau la slăbiciunile pe care le au. În acest caz nu este loc de publicitate.

În general, controlul accesului se poate realiza prin modalităţi de genul tabelelor de autorizare, al listelor de control al accesului, al profilurilor de securitate.

*Tabelele de autorizare*, numite şi tabele de securitate, există în formatul cod-maşină; ele sunt componente ale sistemului de operare, alături de alte programe de control, cu rol de urmărire a bunei funcţionări a sistemului. Importanţa lor rezidă şi în faptul că au un nivel de protecţie similar celor mai bine protejate programe de control.

Tabelele de autorizare se află sub directa preocupare a unor veritabili specialişti, iar pentru utilizatori este important să se cunoască faptul că tabelele trebuie să reflecte, în acest mediu de lucru, ceva identic listelor de control al accesului la valorile deosebite ale firmei în varianta prelucrării manuale a datelor şi a profilelor de securitate ale utilizatorilor.

*Listele de control al accesului*. Responsabilul cu securitatea sistemului trebuie să actualizeze permanent o listă de control al accesului pentru fiecare program executat pe calculator şi pentru fiecare fişier de date. Ele trebuie să conţină:

- elementele de identificare a anumitor valori patrimoniale;
- identificarea fără echivoc a oricărui utilizator autorizat;
- ceea ce se permite fiecărui utilizator să facă cu o anumită valoare patrimonială;
- condiţiile în care se garantează accesul.

*Profilurile de securitate* trebuie să fie în atenţia responsabilului cu securitatea pentru fiecare utilizator autorizat. Profilul va fi definit prin patru elemente:

1. identificarea utilizatorului;
2. identificarea tuturor proiectelor pe utilizatorii care le posedă;
3. identificarea tuturor categoriilor în care se încadrează utilizatorii, inclusiv cele referitoare la responsabilităţile pe linie de securitate a sistemului;
4. identificarea tuturor fişierelor la care utilizatorul poate să aibă acces şi ce anume poate să efectueze asupra lor.

Noţiunile de „proiect” şi „categorie” din enunţurile de mai sus au acelaşi statut ca şi utilizatorii şi, deci, trebuie să aibă şi ele profilul lor.

De fiecare dată când un utilizator intră în contact cu calculatorul de la un terminal conversaţional sau printr-un lot de lucrări, operaţiunea de certificare a identităţii se impune cu acuitate. Informaţia necesară identificării este parola.

Parolele sunt folosite pentru a permite accesul în sistemele de calcul, la fişierele şi bazele de date ale acestuia. N-ar fi exclus ca ele să fie folosite în viitor şi pentru accesarea înregistrărilor sau câmpurilor acestora, cu condiţia de a fi eficiente şi ieftine. Parolele trebuie să fie asociate cu utilizatorii, proiectele şi categoriile de informaţii.

Despre parole s-a vorbit mai pe larg într-un capitol anterior.

În general, nu trebuie să se permită accesul în sistem până când nu se verifică dacă parola face parte dintr-o listă de parole sau se certifică un alt element de identificare.

Trebuie instituite criterii de condiţionare a accesului local sau de la distanţă, precum şi a celui intern (memorie primară, memorie virtuală, memorie secundară şi suporturi externe).

De o importanţă deosebită, după ce s-a autorizat accesul, este obţinerea unui privilegiu de acces, prin intermediul codurilor speciale, consemnate în tabelele de autorizare.

## 6.5.3 Detecţia ameninţărilor şi supravegherea sistemului

Deşi pare nepotrivită, dar nu lipsită de adevăr, afirmaţia că fraudele din mediile informatizate ar putea fi detectate este destul de riscantă. Ca argumente sunt aduse preocupările de urmărire cu atenţie a ameninţărilor sistemului, analiza anumitor tendinţe, cercetarea incidentelor înregistrate şi auditarea.

### 6.5.3.1 Urmărirea ameninţărilor

Toate sistemele trebuie să dispună de capacitatea de înregistrare a tentativelor de atac, într-un format intern, să le supună, apoi, unor examinări riguroase şi să reconstituie informaţiile principale pe baza ceea ce s-a înregistrat în format-maşină. Cât timp este destul de greu de spus ce înseamnă ameninţare şi ce nu, toate operaţiunile care ar putea afecta securitatea sistemului trebuie să fie înregistrate, inclusiv intrările în sesiunile de lucru, solicitările de fişiere şi tranzacţiile de la terminale.

Când operaţiunile principale referitoare la securitatea sistemului sunt înregistrate automat de către sistemele de prelucrare automată a datelor, registrul trebuie să fie protejat împotriva intervenţiei neautorizate a utilizatorilor sau operatorilor. Aceasta se poate realiza prin înregistrarea datelor speciale pe discuri optice de tip WORM (imposibil de modificat) sau pe benzi magnetice pe care se poate scrie, fără posibilitatea derulării benzii înapoi, sau prin apelarea la calculatoare cu rol special, sub directa supraveghere a responsabilului cu securitatea sistemului.

Referitor la recunoaşterea potenţialelor ameninţări, un bun sistem trebuie să fie capabil să depisteze următoarele şase condiţii:

1. terminarea anormală a unor lucrări;
2. o cădere anormală a sistemului;
3. defectarea mecanismului de asigurare a securităţii echipamentelor şi softului;
4. tentativele de intrare în dialog cu sistemul, dar care nu sunt încununate de succes;
5. tentativele de obţinere a accesului neautorizat la fişierele ce conţin date speciale;
6. tentativele de utilizare neadecvată a unor instrucţiuni sau seturi de instrucţiuni privilegiate.

Atunci când sistemul recunoaşte că sunt îndeplinite condiţiile de depăşire a securităţii lui, el trebuie să fie capabil să identifice terminalul de la care se înregistrează tentativa de furt şi categoria infracţiunii. De asemenea, va trebui să furnizeze identitatea utilizatorului care încearcă

să violeze sistemul de securitate, data şi ora evenimentului, precum şi ce fişier a fost ţinta atacului.

De regulă, sunt monitorizate zece tipuri de violări ale sistemului de securitate:

1. a treia tentativă eşuată de deschidere a sesiunii de lucru a sistemului;
2. un răspuns eronat la cererea de reautentificare a utilizatorului;
3. folosirea greşită a unor instrucţiuni privilegiate;
4. tentativa de depăşire a spaţiului de memorie alocat utilizatorului ce a deschis sesiunea de lucru;
5. tentativa de folosire neautorizată a fişierelor cu date secrete;
6. defectarea oricărui mecanism de protecţie;
7. orice încercare de a citi mai întâi noua zonă de memorie care i-a fost alocată, fără să fi scris ceva în ea;
8. incapacitatea sistemului de a încheia cu succes verificarea programelor sistemului;
9. aceeaşi incapabilitate de a verifica tabelele de securitate ale sistemului;
10. tentativa eşuată de introducere a unui nivel mai mare al stării de exploatare privilegiată.

În plus, responsabilul cu securitatea trebuie să încurajeze sistemul de întindere a curselor pentru eventualii intruşi, ceea ce ar însemna state de plată false, parole false şi altele care să-i tenteze pe atacatori.

În acelaşi timp, din partea sistemului vor fi extrase cât mai variate tentative de înşelare a sistemului de securitate, apelându-se la echipe speciale, numite „echipe de tigri". Oricum şi acestea vor fi urmărite îndeaproape, întrucât fără să se simtă supravegheate pot fi tentate să săvârşească acte ilegale.

### 6.5.3.2 Analiza tendinţelor

A căuta ceva ce nu este într-un loc, deşi ar trebui să fie sau ceva ce este şi n-ar trebui, presupune folosirea instrumentelor statistice în cazurile suspecte.

Parametrii statistici principali sunt media sau valoarea aşteptată (scontată) a timpului scurs între incidente sau a capacităţii de utilizare a resurselor şi deviaţia standard a oricăreia dintre mediile amintite. O informaţie preţioasă se obţine şi prin compararea mediilor în mai multe perioade de timp, dacă ele se măresc sau se micşorează ori au o comportare explicabilă în ciclu.

Datele supuse analizei pot fi obţinute pe patru căi:

- registrele componentei de supraveghere a sistemului şi documentele ajutătoare;
- registrele terminalelor sau datele consemnate în documentele întocmite manual pentru o astfel de activitate, confirmate prin semnături;
- înregistrările contabile ale modului de utilizare a resurselor sistemului;
- date privind funcţionalitatea sistemului, inclusiv cele privind defectarea hardului sau softului, precum şi măsurile luate sau reparaţiile efectuate.

În calculele de efectuat, *media* înseamnă însumarea valorilor observate şi împărţirea valorii astfel obţinute la numărul valorilor observate.

*Deviaţia standard* este rădăcina pătrată a sumei diferenţelor la pătrat dintre medie şi fiecare valoare observată, de împărţit la numărul valorilor observate minus unu.

Prin instrumentele statistice amintite pot fi descoperite cinci clase de deviaţii relevante de la securitatea sistemului, după cum urmează:

1. pentru activitatea sistemului ca un tot;
2. activităţile utilizatorilor;
3. activitatea unor terminale anume;
4. operaţiunile cu fişierele ce conţin date secrete;
5. operaţiuni care implică utilizarea programelor cu regim special.

Prin reprezentarea grafică a valorilor obţinute se pot constata discrepanţe relevante privind:

1. timpul dintre două reparaţii ale sistemului;

2. timpul dintre două încercări eşuate de intrare în sistem;
3. timpul dintre întreruperi;
4. timpul scurs între erorile de comunicaţie;
5. folosirea timpului de prelucrare, măsurat în secunde, de înmulţit cu miile de cuvinte ce au fost folosite (kilo-cuvinte);
6. timpul de conectare pe lucrare ş.a.

Există sisteme capabile să-şi măsoare randamentul, prin raportarea timpului folosit în mod productiv la cel neproductiv al sistemului. Scăderea randamentului poate să constituie un semnal de alarmă pe linia securităţii sistemului.

Relevant este şi numărul de lucrări abandonate într-o perioadă de timp, ceea ce ar scoate în evidenţă fie proasta funcţionare a sistemului de operare, fie o greşită utilizare a lui în intenţia de a avea acces la fişierele secrete ale firmelor.

Pentru o uşoară controlabilitate a sistemului se recomandă constituirea unor aşa-zise profiluri ale violatorilor sistemului. Ele sunt realizate pe utilizatori, tipuri de utilizatori (ocazionali, moderaţi, puternici) şi lucrările foarte importante din sistem.

*Profilul unui singur utilizator* rezidă în evidenţierea unor aspecte ce pot să conducă la uşoara descoperire a vinovatului. Ele se referă la înregistrarea codului de identificare a utilizatorului şi tipul lui; numărul şi tipul actelor violente; identificarea fişierelor urmărite prin actele de violenţă.

*Tipurile utilizatorilor* trebuie surprinse prin profiluri distincte, întrucât posibilităţile de a greşi sunt direct proporţionale cu gradul de utilizare a sistemului, cu timpul în care utilizatorul se află în legătură cu acesta.

Se poate porni de la ideea că numai cine nu munceşte nu greşeşte, deci dacă se înregistrează mai multe greşeli la un utilizator deosebit al sistemului acesta ar fi un lucru normal. Din cauza necesităţilor de efectuare a unor analize complexe, utilizatorii vor fi grupaţi pe tipuri, ştiindu-se cam câţi aparţin fiecărui tip, iar violarea sistemului va fi urmărită prin numărul şi tipul lor, precum şi atacurile la securitate pe fiecare utilizator.

Este de reţinut faptul că, dacă numărul atacurilor prin parole din cursul unei zile a sporit, cauza o poate constitui schimbarea la termen a parolelor, când, firesc, mai multe tentative de deschidere a sesiunii de lucru cu vechile parole vor fi sortite eşecului. Şi în acest caz, dacă se ştie cam cât de multe erori s-au înregistrat în perioadele anterioare după schimbarea parolelor, iar acum numărul lor este mult mai mare, s-ar putea trage concluzia că intruşii consideră că acesta ar fi momentul propice să încerce vigilenţa sistemului.

*Profilurile lucrărilor* vor fi consemnate într-un registru special, în care se vor înregistra:

1. identificatorul utilizatorului: pentru a se putea stabili responsabilităţile;
2. kilo-cuvintele-secundă esenţiale: pentru a se putea observa dacă s-au introdus coduri neautorizate;
3. timpul de execuţie: pentru a ne asigura că nu au fost efectuate lucrări neautorizate;
4. numele programelor apelate: pentru a se cunoaşte dacă s-au apelat numai procedurile permise şi nici o altă acţiune n-a avut loc;
5. fişierele de date create şi accesate, precum şi numărul de citiri, scrieri sau adăugări la sfârşit în fiecare fişier: se va urmări dacă s-au accesat fişiere secrete;
6. ieşirile obţinute: pentru a ne asigura că nu s-au copiat sau listat cantităţi mari de date din fişierele secrete.

### 6.5.3.3 Investigarea

Cazurile anormale care pot fi supuse investigării le cuprind pe cele de excepţie, considerate ca ieşite din comun faţă de tendinţa statistică a lor. Atât numărul prea mare de violări ale sistemului, cât şi cel prea mic trebuie să fie supuse investigării. În primul caz fiind semne de prea

multe tentative eşuate de depăşire a sistemului de protecţie, în al doilea s-ar putea trage concluzia depăşirii profesioniste a obstacolelor oferite de barierele protectoare.

Practica recomandă 20 de cazuri care trebuie să constituie motiv de investigare pentru responsabilul cu securitatea sistemului:

1. compromiterea sau suspiciunea de compromitere a informaţiilor speciale ale unităţii;
2. pierderea sau incapacitatea de a evidenţia corect orice valoare patrimonială;
3. intervenţia inexplicabilă a operatorului în execuţia lucrărilor;
4. prezenţa sau suspiciunea prezenţei în sistem a unui intrus;
5. absenţa inexplicabilă a persoanelor cu drept de acces la informaţiile speciale;
6. apariţia unor nume-capcană într-o listă de persoane;
7. creşterea inexplicabilă a gradului de utilizare a sistemului, îndeosebi după program sau în regimul normal de lucru, de către utilizatori sporadici sau de la terminale inactive o lungă perioadă de timp;
8. tentative de accesare sau solicitare a înregistrărilor, fişierelor capcană sau de folosire a parolelor expirate;
9. pierderea sau folosirea neautorizată a identificatorilor utilizatorilor, a sistemului de control al accesului sau a elementelor de recunoaştere de către sistem;
10. plângeri repetate ale beneficiarilor referitoare la încărcarea nejustificată a facturilor de plată a serviciilor de prelucrare automată a datelor, de folosire greşită a adreselor, de apariţie a unor solduri eronate, de numeroase solduri zero sau de omisiuni în listele de plată a drepturilor salariale;
11. imposibilitatea stabilirii soldului final al unui cont;
12. imposibilitatea onorării la plată a cecurilor, facturilor ş.a.;
13. diminuarea inexplicabilă a nivelului stocurilor;
14. creşterea inexplicabilă a frecvenţei tentativelor eronate de obţinere a permisului de acces în sistem sau de violare a protocoalelor de securitate;
15. cererea excesivă a serviciilor de introducere sau extragere a datelor;
16. schimbarea inexplicabilă a căilor traficului de comunicare a datelor;
17. apariţia surprinzătoare a unor coduri noi în sistemul de operare sau în alte programe, a noi nume în listele de control al accesului, în statele de plată a salariilor, a furnizorilor de plătit sau în lista beneficiarilor;
18. schimbări inexplicabile în profilurile lucrărilor sau utilizatorilor;
19. accesul inexplicabil la fişierele speciale sau creşterea surprinzătoare a gradului de utilizare a unor fişiere sau conturi inactive o lungă perioadă de timp;
20. creşterea surprinzătoare a incidentelor produse de defectarea echipamentelor, softului sau de terminarea anormală a lucrărilor, a reluărilor exagerate de execuţii de programe, a restaurărilor multiple ş.a.

În plus, responsabilul cu securitatea sistemului poată să ceară informaţii suplimentare de la operatorii calculatoarelor, de genul:

- numele fişierelor şi subrutinelor accesate de un program dat;
- lista numelor de constante şi variabile ale programelor;
- datele ce ocupă spaţiul memoriei primare selectate;
- listele utilizatorilor de programe şi a fişierelor de date;
- exemplarele ce conţin mesaje de eroare;
- imaginea înregistrărilor bazelor de date înainte şi după actualizarea lor;
- lista suspendărilor din prelucrare (erori) a unor operaţiuni ce nu pot fi prelucrate pentru efectuarea actualizărilor fişierelor nomenclator;
- modificări ale bazelor de date declanşate de la un terminal conversaţional;
- schimbarea locului adresei utilizatorului după ce s-au încălcat regulile de securitate;
- lista de control a comenzilor folosite în timpul execuţiei unei lucrări.

#### 6.5.3.4 Aspecte generale privind controlul şi auditarea sistemelor informatice

Responsabilul cu securitatea sistemului trebuie să prevadă şi să construiască probe pentru auditarea sistemului pentru fiecare incident încadrat în una din următoarele categorii:

1. evidenţa tuturor vizitelor centrului de prelucrare automată a datelor de către persoane din afara sistemului;
2. istoricul tuturor elementelor privind controlul accesului în sistem;
3. evidenţa tuturor persoanelor ce activează în centrul de prelucrare automată a datelor, de la angajare până în prezent, cu drepturile avute, retrase ş.a.;
4. cronologia experienţelor deosebite ale personalului în ultimul an, îndeosebi pe linia a ceea ce a putut vedea, mânui sau a supravegheat activitatea de contabilizare a operaţiunilor informatice;
5. descrierea cronologică a tuturor incidentelor privind actele contabile;
6. păstrarea tranzacţiilor pe ultimii cinci ani despre orice persoană care a participat la derularea lor;
7. istoricul operaţiunilor privind negocierile, din faza anterioară şi următoare acestora, dacă valoarea este mai mare decât o valoare dată (100 dolari);
8. istoricul evoluţiei oricărui program al sistemului de operare, de la implementarea lui până în prezent, cu consemnarea tuturor modificărilor prin care a trecut;
9. verificarea concordanţei tuturor tranzacţiilor cu orice înregistrare dintr-o serie de trei generaţii de fişiere (bunic, tată, fiu), în format intern;
10. istoricul evoluţiei oricărui program de aplicaţii cu rol special în sistem, de la implementare până în prezent, dar consemnând şi modificările, modul de utilizare, de întreţinere;
11. o listă cronologică a tuturor incidentelor în ceea ce priveşte violarea protecţiei sistemului;
12. o listă cronologică a tuturor dificultăţilor întâmpinate în timpul investigării oricărui atac al securităţii sistemului.

#### 6.5.3.5 Acţiunile de răspuns

Toate sistemele trebuie să se bazeze pe existenţa unei persoane cu autorizare specială care să poată declanşa acţiuni reparatorii sau de anihilare a tentativelor de violare a sistemului. De regulă, astfel de acţiuni se numesc acţiuni de răspuns şi pot fi încadrate în două categorii: acţiuni imediate şi acţiuni retroactive.

*Acţiunile imediate*. Îndată ce responsabilul cu securitatea sistemului sau o persoană autorizată să presteze o astfel de activitate constată apariţia unui atac al securităţii, trebuie să stopeze imediat componentele supuse acţiunii frauduloase şi să reţină operaţiunile ce au putut fi afectate, pentru o cercetare minuţioasă ulterioară. Imediat vor fi informate persoanele autorizate cu responsabilităţi pe linia securităţii.

*Acţiunile retroactive*. În cazul în care au intervenit situaţii clare sau numai suspiciuni de compromitere a informaţiilor secrete, de pierdere a valorilor patrimoniale deosebite, de modificare a informaţiilor, de folosire neautorizată a resurselor, probele reviziei şi alte elemente edificatoare vor fi puse laolaltă şi aduse la cunoştinţa celor ce răspund de securitate. Aceştia, pe baza informaţiilor obţinute, vor stabili amploarea pierderilor reale la nivelul firmei, persoanele cărora să li se impute valoarea pierderilor, să determine cu exactitate eficienţa măsurilor de securitate, să înveţe cum să fie prevenite pierderile asemănătoare în viitor, acoperirea pierderilor dacă este posibil.

Deseori se vorbeşte şi despre efectuarea unor acţiuni speciale, care trebuie să fie declanşate când se întâlneşte unul din următoarele patru tipuri de violare a securităţii:

1. orice îndepărtare de la regulile prescrise de deschidere a sesiunii de lucru;

2. o a treia tentativă, consecutivă, eşuată, de deschidere a sesiunii;
3. tentativa eşuată de a da răspunsul corect la acţiunea de reautentificare declanşată de sistem;
4. orice intenţie a utilizatorilor de a obţine accesul neautorizat la fişiere sau de a folosi instrucţiuni sau secvenţe de instrucţiuni nepermise.

### 6.5.3.6 Infractorii tipici ai sistemelor informatice

De la început trebuie menţionat că o mare parte a delincvenţilor îşi încetează misiunea prin utilizarea unor mijloace convenţionale: intimidarea, anchetarea şi apelarea la informatori. Cele mai importante metode de informare privind suspecţii se bazează pe supravegherea lor discretă, lucrul în comun sau asocierea. De multe ori persoanele ce se despart oferă informaţii preţioase despre partenerul lor de viaţă. Nu trebuie neglijate categoriile dintr-o unitate cărora la prima vedere nu prea li se dă prea multă importanţă (curieri, personalul care se ocupă de curăţenie, paznici), care, de multe ori, văd şi ştiu foarte multe.

Deşi în capitolele anterioare au fost prezentate categoriile de atacatori, în cele ce urmează se va face o scurtă descriere a patru tipuri reprezentative de delincvenţi: delapidatorii, detractorii sau seducătorii, hackerii şi trişorii.

*Delapidatorii* au devenit hoţi informatizaţi printr-o explicaţie foarte simplă: înregistrările la care trebuie să ajungă şi modalităţile de acoperire a faptei sunt realizabile cu ajutorul calculatorului.

De regulă, delapidatorii sunt de vârstă mijlocie, cu destulă credibilitate în firmă, câştigată, îndeosebi, printr-o prezenţă îndelungată în aceeaşi unitate. Ei sunt buni cunoscători ai măsurilor antifurt şi de controlare a fraudelor, iar locul lor de muncă le permite să aibă acces legal în sistem sau la valorile patrimoniale publice. De cele mai multe ori ei se cred neglijaţi, mai ales pentru că nu ocupă o funcţie mai bună în sistem.

Totul începe de la existenţa unor probleme personale de natură financiară, prin îmbolnăvirea unor membri ai familiei, ca urmare a unor mofturi pe care nu şi le permit să şi le satisfacă sau dorinţei de a trăi pe picior mare. Totuşi, pe ultima sută, operează bunul simţ. După ce „şterpelesc” o jumătate de milion de dolari, pentru o foarte lungă perioadă de timp, se opresc.

*Detractorul* este un adevărat hoţ informatizat şi lucrează în domeniul prelucrării automate a datelor. În majoritatea cazurilor, detractorul este un bărbat în jurul vârstei de 35 de ani. Salariul său se situează, ca mărime, în prima jumătate a salariilor din firmă. Vechimea la unitatea actuală nu este mai mare de trei ani, locuieşte într-un cartier respectabil, este căsătorit şi are doi copii. S-a ocupat de „şterpeliri” timp de aproximativ 18 luni şi a obţinut venituri din această activitate ce reprezintă cam 120 procente din venitul său anual. El este capabil să conducă un centru de calcul sau să fie şeful echipei de programare sau de exploatare a sistemului. Motivaţia faptei sale poate fi una de natură egocentrică sau, în virtutea poziţiei pe care o ocupă, consideră că este normal să execute lucrări personale în sistem, să vândă soft sau orice altceva.

*Hackerul* este tot bărbat, între 14 şi 25 de ani, deşi s-au descoperit şi cazuri de 8 ani sau de peste 40 de ani. Este fie student, fie şomer. Are o minte sclipitoare şi are soarta lupilor singuratici, fiind obsedat numai de tehnologiile de vârf, de ultimă oră. Deseori se consideră neglijat de societate, care nu-şi dă seama cât de isteţ este. Astfel de cazuri sunt uşor de întâlnit în mediile universitare, persoanele în cauză petrecându-şi zilnic 16-18 ore în faţa calculatorului sau a unui terminal, fără să mai facă nimic altceva. De cele mai multe ori sunt căzuţi la examenele de matematică şi limbă maternă, dar la calculatoare sunt mai buni decât directorii centrelor de calcul sau profesorii care le predau limbaje de programare sau sisteme de operare. Nici nu le pasă ce se întâmplă în jurul lor. După ani, dacă mediul le permite, pot deveni unii dintre cei mai buni specialişti în domenii cheie de activitate: şefii firmelor de contabilitate, specialişti în securitatea sistemelor, ofiţeri ai serviciilor secrete, oameni de afaceri cu mult succes.

*Trişorul*, de regulă, este femeie. De cele mai multe ori este singurul părinte al unuia sau doi copii şi poate să aparţină, în mod vizibil, unor grupuri minoritare. Vârsta este între 25 şi 35 de ani. Profesia este cea de responsabil introducere-date şi, prin prisma acesteia, are posibilitatea să-şi adauge drepturi băneşti suplimentare, pe care de multe ori le împarte unor societăţi caritabile. Poate să aibă şi o motivaţie ideologică sau să acţioneze sub un sindrom invers celuia sub care acţiona Robin Hood, luând de la bogaţi, dar păstrând totul pentru ea. În cele mai multe cazuri au operat pe un anumit scenariu cam doi ani şi au agonisit sume ce depăşesc 50000 de dolari.

Cauzele succesului unor astfel de furturi se datorează, în majoritatea lor, ineficienţei controlului exercitat de către sistem, ineficienţei controlului propriului personal şi a unui control managerial slab.

## 6.5.4 Integritatea sistemelor

Integritatea sistemelor se referă, de fapt, la programe şi date. Integritatea datelor este protejată prin controlul erorilor, iar a programelor, printr-un control riguros asupra tuturor activităţilor de programare. Un caz aparte îl poate constitui protecţia programelor şi funcţiilor pe linia securităţii.

### 6.5.4.1 Securitatea programelor

Controlul în detaliu al conceperii, realizării şi implementării programelor calculatoarelor reprezintă problema-cheie a securităţii sistemului.

*Conceperea programelor*. Activităţile de programare trebuie să se organizeze în jurul echipelor de programare. Într-un astfel de concept, programele se scriu de o întreagă echipă, sub coordonarea directă a unui şef, care are rolul de arhitect al întregii lucrări, stabilind interfeţele dintre modulele programatorilor din subordine. Fiecare dintre ei răspunde de o componentă bine definită din program. Toţi programatorii, inclusiv şeful, transmit ceea ce au făcut unui secretar de proiect, care colectează documentaţia şi urmăreşte dacă numele variabilelor sau subrutinelor sunt uniforme.

Activitatea de programare trebuie să urmeze metoda top-down (descentralizată, de sus în jos), pornind de la un proiect general şi continuând cu descompunerile în jos.

Pentru un control asupra întregului program trebuie să se folosească diverse tehnici de descriere a algoritmilor de prelucrare (diagrame, scheme logice, tabele de decizie ş.a.).

Înaintea compilării programului trebuie să se verifice dacă există erori de logică, operaţiune executată de două persoane foarte pricepute în programare. Se poate apela şi la folosirea calculatoarelor pentru efectuarea acestor activităţi.

*Realizarea programelor* se înfăptuieşte prin apelarea la compilatoare adecvate, în ultimul timp folosindu-se compilatoare conversaţionale sau inteligente. Pentru adevăraţii programatori ele nu sunt de un mare ajutor.

*Datele de test* au rolul de a verifica multitudinea ipostazelor de prelucrare prin care poate să treacă sistemul. Datele de test se introduc în documentaţia programului.

*Implementarea programului*. În cazul îmbunătăţirii unor programe deja existente, se recomandă implementarea prin funcţionarea paralelă a celor două versiuni.

### 6.5.4.2 Protecţia funcţiilor securităţii

Funcţiile principale de control al centrului de prelucrare automată a datelor trebuie să fie asigurate prin mecanismul de protecţie. Ele, în mare parte, se referă la:

1. controlul direct al resurselor fizice (benzi, pachete de discuri, alte suporturi de date şi echipamente periferice);
2. procedurile de pornire şi oprire a sistemului;

3. mecanismele de supraveghere a utilizatorilor;
4. detectarea şi corectarea erorilor, precum şi reluarea lucrului în condiţii normale;
5. generarea, coordonarea şi trimiterea secvenţelor de instrucţiuni (sau prelucrări);
6. cuplarea cazurilor, în vederea prelucrării lor într-o anumită ordine;
7. identificarea şi verificarea utilizatorilor;
8. controlul fluxurilor de date;
9. ştergerea datelor remanente în memoria calculatorului de la un utilizator la altul sau înaintea efectuării operaţiunilor de întreţinere;
10. proceduri de criptare şi decriptare.

Este foarte important ca securitatea să fie întreţinută tot timpul şi în toate condiţiile, inclusiv când apar mari încărcături de date, ceea ce ar trebui să se concretizeze într-o securitate sporită. La fel trebuie pusă problema şi în cazul diminuării cantităţii de date prelucrate sau când apar defecţiuni la echipamente sau programe, sau când se asigură întreţinerea şi repararea sistemului. Măsuri speciale trebuie prevăzute şi pentru cazurile provocate de intervenţia voită a omului asupra securităţii sistemului.

Un rol deosebit revine programelor de asigurare a securităţii, despre care s-a discutat într-un paragraf anterior.

### 6.5.5 Înregistrarea activităţilor efectuate şi a măsurilor de securitate

Este foarte important să se ţină evidenţa înregistrărilor astfel încât principiile securităţii prelucrării automate a datelor să poată fi puse în practică. Jurnalele asigură o înregistrare cronologică a cazurilor pe linie de securitate. Fişierele de siguranţă fac posibilă reconstituirea datelor după catastrofe sau funcţionări proaste ale sistemului.

Jurnalele de bord trebuie să fie ţinute la zi pentru toate activităţile ce au loc sub controlul operatorului, al ofiţerului cu securitatea sistemului (dacă există), al bibliotecii de suporturi şi de la punctele de prelucrare.

*Controlul operatorului*. În jurnalul operatorului trebuie să fie înregistrate următoarele evenimente:

1. pornirea calculatorului;
2. configuraţia cu care s-a început lucrul;
3. iniţializarea şi reiniţializarea sistemului;
4. execuţia testelor de rutină şi a programelor de întreţinere;
5. momentul de început-execuţie programe sau de serie de programe înlănţuite;
6. finalizarea normală sau anormală a lucrărilor;
7. disfuncţionalităţi ale softului de sistem sau proasta funcţionare a echipamentului;
8. oprirea normală sau anormală a calculatorului;
9. timpii de prelucrare pierduţi;
10. mesajele de eroare afişate de calculator;
11. interogări anormale ale fişierelor cu date secrete;
12. montarea suporturilor detaşabile;
13. intervenţia operatorului în programele utilizatorilor sau suprascrierea de către operator a unor funcţii de protecţie;
14. responsabilităţile operatorului în regim activ sau inactiv;
15. prezenţa vizitatorilor în sala calculatorului.

*Jurnalele punctelor de prelucrare şi ale operaţiunilor de intrare-ieşire*. În continuare se va prezenta o listă a activităţilor de consemnat în jurnalul punctelor de prelucrare sau al locurilor unde se înregistrează prestările de servicii. Multe dintre ele pot fi consemnate de calculator, în mod automat. Dacă nu există această posibilitate se vor consemna manual. Evenimentele care se vor înregistra sunt:

1. identificarea utilizatorului;
2. procedurile deschiderii sesiunii de lucru;
3. procedurile închiderii sesiunii, cu contabilizarea datelor privind funcţionarea sistemului;
4. momentul de lansare în execuţie a lucrărilor;
5. momentul opririi execuţiei lucrărilor;
6. linia-destinaţie;
7. terminalul-destinaţie;
8. rutinele de comunicaţie;
9. calculatoarele şi sistemele de operare folosite pentru execuţia lucrărilor;
10. programele şi subrutinele apelate şi condiţiile de securitate pe care le solicită;
11. fişierele de date accesate şi nivelurile lor de securitate;
12. identificarea unică a lucrărilor din noianul de lucrări ale zilei sau din sistemul de clasificare pe linia securităţii;
13. identificarea fişierelor de date sau a programelor create sau distruse în cursul execuţiei unei lucrări, condiţiile de securitate şi mărimea lor.

*Jurnalele bibliotecilor de suporturi*. Bibliotecarul de suporturi trebuie să vadă data, timpul şi circumstanţele în care a apărut unul din următoarele evenimente:

1. achiziţia de materiale în bibliotecă;
2. ştergerea sau distrugerea suporturilor de prelucrare automată a datelor şi a documentaţiei;
3. înlocuirea documentaţiei sau a suporturilor de date;
4. scoaterea din locul de păstrare sau arhivare a suporturilor sau documentaţiilor;
5. scoaterea din bibliotecă a unor obiecte şi data aducerii lor înapoi;
6. schimbări ale proprietăţii asupra elementelor de prelucrare automată a datelor sau documentaţiei;
7. schimbarea încadrărilor pe linia securităţii suporturilor din bibliotecă sau a documentaţiei.

*Jurnalele ofiţerului cu securitatea*. Ofiţerul cu securitatea sistemului sau un soft specializat trebuie să fie în măsură să înregistreze evenimente de natura celor de mai jos:

1. identificarea utilizatorilor care săvârşesc erori;
2. identificarea terminalului la care s-a înregistrat infracţiunea;
3. tipul de violare a securităţii;
4. data şi timpul incidentului;
5. identificarea şi încadrarea în nivelul de securitate adecvat a tuturor programelor speciale sau fişierelor de date expuse pericolelor externe.

Pentru a asigura securitatea sistemelor de prelucrare automată a datelor, echipamentele şi programele de control trebuie să se afle în deplină siguranţă, numai în acest mod putându-se continua serviciile, care sunt de cea mai mare importanţă în existenţa sistemului. Se ştie că şansele de reuşită ale furturilor sau compromiterii datelor sunt deosebit de favorabile atunci când personalul de prelucrare automată a datelor este preocupat de repunerea în funcţiune a echipamentelor şi programelor. Problema tinde să devină deosebit de gravă atunci când se referă la mecanismele de protecţie. Uneori rezolvarea cazurilor de defectare a echipamentelor sau programelor presupune apelarea la specialişti din afară, care nu au responsabilităţi pe această linie, ceea ce nu este un lucru bun. În fine, trebuie să existe copii de siguranţă care să fie folosite în momentul apariţiei unor defecţiuni la fişierele în lucru. Totul trebuie să se desfăşoare astfel încât să nu ducă la oprirea sistemului.

Aşadar, siguranţa întregului sistem se realizează prin asigurarea funcţionării normale a echipamentelor, softului şi existenţa copiilor de siguranţă. Despre toate s-a discutat în paragrafele anterioare.

- Extrageţi din subcapitolul de mai sus un set de factori pe baza cărora un sistem informatic să poată fi încadrat în una dintre clasele de evaluare propuse de Centrul de Apărare a Securităţii Calculatoarelor al Agenţiei Naţionale de Securitate. Aplicaţi factorii pe un sistem informatic dintr-o firmă cunoscută de dumneavoastră.
- Imaginaţi un alt profil de infractor al sistemelor informatice decât cele din subcapitolul 6.5.3.6.

# 6.6 Măsuri administrative pe linia securităţii sistemelor

Problemele referitoare la atribuirea responsabilităţilor pe linia prelucrării automate a datelor revin conducerii la vârf. Punerea în practică a principiilor securităţii sistemelor este diferită pentru sectorul public faţă de cel privat.

## 6.6.1 Securitatea sectorului public

În Departamentul Apărării din S.U.A., sistemele de prelucrare automată a datelor trebuie să aibă autorizat acceptul de prelucrare pentru asigurarea securităţii datelor, operaţiune realizată de ofiţerul responsabil cu informaţiile, situat deasupra nivelului la care se efectuează prelucrarea. El are responsabilitatea securităţii întregului sistem de prelucrare automată a datelor, care, de cele mai multe ori, înseamnă mai multe centre de calcul. Alteori, el este format din mai multe sisteme informaţionale. Pentru fiecare dintre acestea trebuie să existe câte un responsabil cu securitatea datelor, iar la nivelul întregului centru va fi numit alt responsabil, pentru ceea ce ţine de componentele acestuia. Pentru reţele există un alt responsabil cu interconectarea datelor de la terminale la calculatorul central. La rândul lor, terminalele sunt supravegheate de un alt ofiţer. De asemenea, pot fi unul sau mai mulţi ofiţeri responsabili cu aplicaţiile bazate pe procesare de texte şi alte tipuri de aplicaţii.

Actele normative pe linia securităţii sistemelor de prelucrare automată a datelor sunt promulgate de către Departamentul Apărării şi de alte trei componente:

- Centrul de Securitate a Sistemelor de Prelucrare Automată a Datelor ale Apărării din Agenţia Securităţii Naţionale;
- Biroul Management şi Bugete stabileşte regulamentele departamentelor civile, în special pe linia analizei riscurilor;
- Biroul Naţional de Standarde emite o serie de standarde federale ale prelucrării informaţiilor.

În mod normal, fiecare departament dispune de un responsabil cu securitatea sistemelor informaţionale, excepţie făcând locurile în care se pune problema gestionării fondurilor federale, situaţie în care intervine Serviciul Secret al Statelor Unite.

Norme privind prelucrarea datelor cu caracter financiar sunt emise de Trezoreria Statului. Ele afectează nu numai departamentele guvernamentale, ci şi băncile şi alte instituţii care intră în relaţii cu Trezoreria.

În Canada, de asemenea, de securitatea sistemelor de prelucrare automată a datelor pe linia apărării se ocupă Securitatea Apărării şi Agenţia de Informaţii Secrete. În sectorul civil, standardele sunt promulgate de către Consiliul Trezoreriei, cu avizul de specialitate al Comitetului de Avizare a Securităţii din cadrul Comitetului Interdepartamental pentru Probleme de Securitate şi Informaţii Secrete. Urmărirea şi rezolvarea problemelor securităţii datelor revine Poliţiei Călare Regale Canadiene.

În România,[1] securitatea informaţiilor din domeniul public revine ca responsabilitate conducătorilor autorităţilor şi instituţiilor publice. Coordonarea generală a activităţii şi

[1] *** – *Protecţia informaţiilor clasificate. Ghid practic*, www.sri.ro/biblioteca_art_infclas.html

controlului măsurilor privind protecţia informaţiilor secrete de stat se realizează de către Serviciul Român de Informaţii. De asemenea, Ministerul Apărării Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul Român de Informaţii Externe, Serviciul de Protecţie şi Pază şi Serviciul de Telecomunicaţii Speciale stabilesc, pentru domeniile lor de activitate şi responsabilitate, structuri şi măsuri proprii pentru coordonarea şi controlul activităţilor legate de protecţia informaţiilor secrete de stat. Alături de aceste organisme, Parlamentul, Administraţia Prezidenţială şi Consiliul Suprem de Apărare a Ţării stabilesc măsuri proprii privind protecţia informaţiilor secrete de stat, fiind asistate de către Serviciul Român de Informaţii.

Pentru implementarea măsurilor de securitate şi organizarea activităţilor specifice protecţiei informaţiilor clasificate, la fiecare autoritate sau instituţie publică, agent economic sau orice altă organizaţie care, prin natura activităţii, gestionează informaţii clasificate, se va înfiinţa o structură de securitate sau se vor desemna funcţionari de securitate.

Implementarea unitară, la nivel naţional, a măsurilor de securitate naţională clasificate, precum şi a celor echivalente care fac obiectul tratatelor, înţelegerilor şi acordurilor bilaterale sau multilaterale la care România este parte, este asigurată de către *Oficiul Registrului Naţional al Informaţiilor Secrete de Stat*, înfiinţat prin Ordonanţa de Urgenţă nr. 153/7 noiembrie 2002. Acest organism îşi desfăşoară activitatea de reglementare, autorizare, evidenţă şi control în conformitate cu prevederile Legii 182/2002 privind protecţia informaţiilor clasificate, ale *Standardelor naţionale de protecţie a informaţiilor clasificate* în România (Hotărârea de Guvern 585/2002) şi ale normelor privind protecţia informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România (Hotărârea de Guvern 353/2002).[2]

## 6.6.2 Securitatea sistemelor informaţionale din domeniul privat

În acest sector nu este o situaţie similară sectorului public, întrucât misiunea asigurării securităţii informaţiilor revine contabilului şef şi administratorului firmei. În cazul firmelor mai mici, de problema amintită se ocupă directorul general. Obiectivul, în toate cazurile, îl constituie reducerea pierderilor şi îmbunătăţirea mediului de lucru al firmei.

### 6.6.2.1 Obligaţiile contabilului şef

Contabilul şef, ca responsabil al sectorului financiar-contabil, are datoria să realizeze corect auditul intern şi trebuie să fie primul care să cunoască eventualele nereguli. Cât timp în multe cazuri el răspunde şi de sistemul de prelucrare automată a datelor, el are decizia financiară pe linia procurării de noi echipamente şi a organizării sistemelor de prelucrare automată a datelor.

### 6.6.2.2 Obligaţiile secretariatului şi oficiului juridic

În acest caz responsabilităţile nu sunt de aceeaşi importanţă ca şi cele enumerate anterior, dar ele se referă la:

- raporturile cu acţionarii;
- perfectarea de contracte;
- procurarea patentelor, copyrighturilor, mărcilor de fabrică;
- asigurarea cadrului legal al desfăşurării activităţilor comerciale;
- apărarea împotriva potenţialilor inamici ai sistemului;
- păstrarea secretului informaţiilor vehiculate în şedinţele consiliului de administraţie;
- plasarea poliţelor de asigurare ale firmei.

[2] *** – *Ordonanţa de Urgenţă nr. 153 din 7 noiembrie 2002 privind organizarea şi funcţionarea Oficiului Registrului Naţional al Informaţiilor Secrete de Stat*, Monitorul Oficial nr. 826, 15 noiembrie 2002

#### 6.6.2.3 Rolul vicepreşedintelui cu probleme administrative

Atunci când există această funcţie, responsabilul cu securitatea sistemului raportează către vicepreşedinte, prin intermediul unor manageri numiţi cu un astfel de obiectiv. Oricum, ideea de bază este că şi securitatea sistemului se realizează pe mai multe niveluri, ca şi conducerea firmelor.

#### 6.6.2.4 Organizarea securităţii firmelor

De regulă, de problemele securităţii unui organism economico-social se ocupă o persoană numită, fie în mod direct, fie prin delegarea altei persoane care să aibă o poziţie deosebit de bună în unitate, în primul rând să fie respectată.

Responsabilul cu securitatea va crea o adevărată infrastructură de asigurare a securităţii firmei, un rol important în îndeplinirea obiectivelor generale revenind nivelurilor inferioare, adică responsabililor de clădiri şi locuri de muncă. Aceste ultime persoane vor fi responsabile cu asigurarea sistemelor de închidere, a containerelor, birourilor sau a altor mijloace de protecţie a documentelor, asigurarea siguranţei funcţionării birourilor şi întregii organizaţii, controlul traficului auto, controlul cheilor, sistemului ecusoanelor, al permiselor de intrare, biletelor de voie ş.a.

### 6.6.3 Responsabilităţi intra-organizaţionale pe linia prelucrării automate a datelor

De problemele securităţii sistemului de prelucrare a datelor se ocupă responsabilul cu securitatea firmei sau a celorlalte componente organizatorice ale acesteia, responsabilul clădirii sau al locului de muncă, directorul centrului de prelucrare automată a datelor şi coordonatorul activităţilor de asigurare a securităţii. Ultimul este cel mai puternic implicat în problema de faţă.

*În centrele mici*, coordonarea tuturor activităţilor pe linia securităţii poate să-i revină directorului centrului, oficiului sau staţiei de calcul respective. *În cele puţin mai mari*, activitatea poate să-i revină unei persoane delegate de director. *Centrele mari* vor avea un administrator numit special pentru a exercita această funcţie. *În centrele foarte mari*, coordonatorul securităţii poate fi ajutat de un administrator cu securitatea pentru controlarea activităţilor care presupun lucrul cu informaţii şi un programator al securităţii sistemului pentru controlarea aspectelor tehnice ale locurilor de muncă.

#### 6.6.3.1 Responsabilităţile directorului sistemului de prelucrare automată a datelor

Directorul centrului de prelucrare automată a datelor trebuie să observe dacă evaluarea pericolelor se efectuează periodic şi dacă ele sunt realiste. Tot el va fi responsabil cu implementarea măsurilor de prevenire a pierderilor. De asemenea, directorul centrului va crea un sistem de urmărire continuă a comportamentului personalului pe linia securităţii sistemelor. El va numi coordonatorul sistemului de securitate, care trebuie să fie un specialist în prelucrarea automată a datelor, cu suficiente cunoştinţe despre securitatea sistemelor sau o persoană cu ample cunoştinţe privind securitatea şi suficient instruită în domeniul prelucrării automate a datelor. O altă preocupare a sa constă în întreţinerea unor legături permanente cu alte unităţi ale căror date se prelucrează în sistemul lui.

În vederea asigurării securităţii la nivel de componente, directorul centrului numeşte responsabili pe domenii astfel:

- bibliotecarul, care are răspunderea păstrării suporturilor de prelucrare automată a datelor;
- administratorul bazei de date, care gestionează întreaga bază de date a organizaţiei;

- responsabilul cu integrarea sistemului, care răspunde de integrarea echipamentelor şi softului;
- şeful echipei de programare a sistemului, responsabil pentru funcţionarea sistemului, cu sarcini cum ar fi achiziţia de noi programe pentru asigurarea funcţionării corecte a acestuia;
- şeful exploatării răspunde de activitatea propriu-zisă de prelucrare automată a datelor;
- şeful controlului de calitate răspunde de calitatea prelucrării automate a datelor şi a rezultatelor prelucrării;
- şeful echipei de pregătire date răspunde de pregătirea şi verificarea datelor de intrare.

Fiecare responsabil, dintre cei enunţaţi anterior, va trebui să-şi actualizeze documentaţia prin care consemnează procedurile necesare atingerii obiectivelor securităţii. Ei trebuie să-şi întemeieze activităţile pe următoarele lucrări:

- consemnarea cu rol statistic a tuturor activităţilor de prelucrare automată a datelor, pentru detectarea excepţiilor de la regulă;
- registre/jurnale care să consemneze toate acţiunile de întreprins pentru asigurarea securităţii;
- descrierea tuturor evenimentelor deosebite privind securitatea;
- rezultatele la care s-a ajuns prin cercetarea cazurilor de violare a securităţii.

### 6.6.3.2 Obligaţiile responsabilului cu securitatea

Coordonatorul securităţii este persoana de bază în domeniul securităţii prelucrării automate a datelor şi are cel puţin şase responsabilităţi:

- evaluarea ameninţărilor potenţiale ale sistemului;
- procedurile de realizare a securităţii;
- contramăsuri la eventualele pericole;
- planificarea realizării copiilor de siguranţă şi a reconstituirii datelor pierdute;
- prevenirea incidentelor;
- instruire de specialitate.

La baza oricărei evaluări a ameninţărilor care planează asupra sistemului stau identificarea şi evaluarea elementelor patrimoniale, subiecte ale ameninţărilor (echipamente, programe, date, documentaţie, furnituri de birou ş.a.).

Problema-cheie pentru asigurarea eficienţei măsurilor de precauţie pe linia securităţii constă în identificarea, prin nume, a persoanelor responsabile direct pentru fiecare element patrimonial. Ele se numesc şi *persoane responsabile*, obligaţiile lor fiind de a evidenţia absolut toate operaţiunile efectuate asupra elementelor de care răspund.

### 6.6.3.3 Controlul accesului la elementele patrimoniale

Pasul următor în programul de asigurare a securităţii constă în exercitarea controlului accesului la fiecare element patrimonial. Coordonatorul securităţii sistemului trebuie să-şi ţină la zi evidenţa privind:

- lista persoanelor ce deţin permise de intrare, legitimaţii sau ecusoane speciale;
- listele de control al cheilor, cartelelor şi altor elemente de acces în unitate;
- lista parolelor, cifrurilor de intrare, codurilor secrete şi a cunoscătorilor acestora;
- numele uzual, de lucru, al echipamentelor sistemului;
- numele unice ale fişierelor şi ale persoanelor care le pot accesa şi modifica;
- numele unice ale programelor şi ale persoanelor care le pot lansa în execuţie şi modifica;
- profilurile utilizatorilor sistemului, cum ar fi: ce i se permite utilizatorului să facă cu fişierele şi programele la care are acces;

- numele proiectului şi al programatorilor lui;
- urmărirea continuă a documentelor de control al locurilor în care sunt păstrate informaţiile confidenţiale sau speciale ale unităţii;
- regulile interne referitoare la modul în care sunt păzite toate elementele patrimoniale importante.

### 6.6.3.4 Urmărirea respectării măsurilor de securitate

*Cel puţin o dată pe săptămână, coordonatorul securităţii* trebuie *să viziteze centrul de prelucrare automată a datelor*, pentru a verifica în ce mod se achită de obligaţii persoanele responsabile.

*Cel puţin o dată pe lună, coordonatorul securităţii* sistemului va *face revizia documentaţiei* întocmite de persoanele responsabile cu asigurarea securităţii elementelor patrimoniale pe care le au în grijă.

*Cel puţin o dată pe an,* tot el, *va solicita efectuarea reviziei interne a eficienţei procedurilor şi practicilor de securitate*.

*Oricând*, coordonatorul securităţii sistemului *poate propune directorului centrului să ia măsuri de prevenire a ameninţărilor securităţii*, iar acesta va include o apreciere a eficienţei măsurilor pe timpul funcţionării normale a sistemului, în perioadele de pauză, la iniţializarea lui, la căderea lui, precum şi în timpul întreţinerii echipamentelor şi programelor.

O atenţie deosebită va fi acordată copiilor de siguranţă şi acţiunilor de reconstituire în caz de avarie, în toate variantele posibile ale ivirii ei. *Cel puţin o dată la trei luni*, coordonatorul securităţii *va inspecta locurile în care sunt păstrate suporturile de memorie externă*. De *cel puţin două ori pe an, va inspecta orice componentă a centrului de prelucrare automată a datelor*.

*O dată pe an, va supune personalul unui test* pentru a-l verifica în ce măsură poate *să reconstituie sistemul* folosind numai copiile de siguranţă, fără să pericliteze securitatea sistemului.

La rândul lui, *coordonatorul securităţii raportează*, în detaliu, *cel puţin o dată pe lună sau ori de câte ori este nevoie*, către directorul centrului de prelucrare automată a datelor, absolut *toate problemele pe linia securităţii sistemului*. Raportul poate să conţină şi propuneri de luare a unor măsuri suplimentare de prevenire a incidentelor.

De asemenea, *coordonatorul securităţii* sistemului este *responsabil şi de realizarea unor programe speciale de instruire*, preocupându-se de procurarea materialelor din reviste sau alte publicaţii care abordează astfel de probleme. El va participa şi la întâlniri cu alţi specialişti din domeniu.

### 6.6.3.5 Principii administrative privind responsabilităţile de securitate

Pe linia securităţii sistemelor de prelucrare automată a datelor, în ceea ce priveşte componenta administrativă a personalului, există trei principii:

- principiul „niciodată singur”
- principiul exercitării limitate a unei funcţii
- principiul delimitării obligaţiilor de serviciu.

**Principiul „niciodată singur”**

În măsura în care resursele de personal ale centrului o permit şi sunt în total acord cu studiile de evaluare a ameninţărilor elaborate de director, două sau mai multe persoane, desemnate de directorul centrului de prelucrare automată a datelor, recunoscute a fi bine pregătite profesional, vor participa la exercitarea acţiunilor-cheie pe linia securităţii şi vor consemna, prin semnătură, într-un registru special, tot ceea ce se referă la:

1. eliberarea şi restituirea elementelor de control al accesului sau o împuternicire a exercitării acestei activităţi;
2. eliberarea şi restituirea suporturilor de prelucrare automată a datelor;
3. iniţializarea şi oprirea sistemului;
4. prelucrarea informaţiilor deosebit de importante;
5. întreţinerea echipamentelor şi programelor;
6. testarea şi acceptarea hardului;
7. modificarea hardului;
8. reconfigurarea permanentă a sistemului;
9. proiectarea şi implementarea bazelor de date;
10. proiectarea, implementarea şi modificarea sistemului de operare;
11. proiectarea, implementarea şi modificarea programelor de aplicaţii;
12. proiectarea, implementarea şi modificarea softului de securitate;
13. modificarea documentaţiei;
14. modificarea planurilor privind cazurile de avarie;
15. declararea stărilor de avarie;
16. distrugerea sau ştergerea programelor sau a datelor importante;
17. reproducerea informaţiilor foarte importante;
18. schimbarea procedurilor de exploatare a sistemelor de prelucrare automată a datelor;
19. recepţia, eliberarea şi transportul materialelor deosebit de importante.

**Principiul exercitării limitate a funcţiei**

Acest principiu prevede ca nici o persoană să nu fie lăsată în poziţiile cheie pe linia securităţii datelor un timp prea îndelungat, astfel încât să înceapă a crede că sarcina ce-i revine îi aparţine în exclusivitate sau că puterile sale sunt veşnice.

**Principiul separării obligaţiilor de serviciu**

Principiul de faţă este cel mai important. El constă în respectarea cu stricteţe a regulii ca nici o persoană să nu aibă cunoştinţă despre funcţiile privind securitatea sistemului, să nu fie expusă la astfel de probleme şi nici să nu participe la acţiuni pe această temă dacă acestea nu intră în responsabilitatea ei.

*Există zece perechi de funcţii* pe linia prelucrării automate a datelor, care, din considerente de securitate, *trebuie să fie exercitate de persoane sau grupuri diferite*. Acestea sunt:

1. operarea la calculator şi programarea calculatorului;
2. pregătirea datelor şi prelucrarea lor;
3. prelucrarea datelor şi controlul calităţii prelucrării;
4. operarea la calculator şi gestiunea suporturilor de memorare;
5. recepţia materialelor importante şi transmiterea lor;
6. reproducerea, eliberarea sau distrugerea informaţiilor importante şi autorizarea înfăptuirii acestora;
7. scrierea programelor de aplicaţii şi a programelor de sistem;
8. scrierea programelor de aplicaţii şi administrarea bazei de date;
9. proiectarea, implementarea şi modificarea softului privind securitatea sistemului şi exercitarea oricărei alte funcţii;
10. controlul împuternicirilor de acces şi exercitarea oricărei alte funcţii.

Principiul separării obligaţiilor de serviciu poate fi realizat pe două căi:

- prin ridicarea unor bariere fizice;
- prin instituirea unui sistem de norme interne.

Există şase *bariere fizice* principale:

1. biblioteca suporturilor fizice ale datelor trebuie să fie amplasată într-un singur loc, dar separat de sala calculatorului;

2. pregătirea datelor trebuie să se efectueze într-o sală apropiată, dar diferită de cea a calculatorului;
3. birourile programatorilor trebuie să fie amplasate în alte locuri decât sala calculatorului;
4. biroul personalului responsabil cu securitatea trebuie să fie inaccesibil altor categorii de persoane;
5. sala calculatorului trebuie să fie o zonă de acces cu restricţii, chiar şi pentru operatorii de serviciu şi personalul cu întreţinerea, şi se impune supravegherea activităţii lor;
6. materialele aruncate, care conţin informaţii importante, trebuie să fie depozitate într-un loc aflat în siguranţă, departe de sala calculatorului.

*Normele interne* au caracter administrativ şi se referă la:

- interdicţia operatorilor calculatoarelor de a lucra şi cu alte echipamente de prelucrare automată a datelor;
- operatorii nu trebuie să întocmească şi nici să modifice programe;
- implementarea şi păstrarea rezultatelor pe linia securităţii trebuie să fie activităţi distincte;
- controlul calităţii şi auditarea trebuie să fie funcţii separate şi distincte de cele de prelucrare propriu-zisă.

- Extrageţi din două fişe ale posturilor dintr-o organizaţie atribuţiile de securitate informaţională.
- Arătaţi cum se aplică într-o organizaţie principiile administrative privind responsabilităţile de securitate.

## Rezumat

Securitatea sistemelor are ca obiectiv împiedicarea pătrunderii intruşilor în sistem, transmiţându-le mesaje de avertizare. Dacă împiedicarea pătrunderii nu este posibil de realizat, atunci barierele trebuie să le stopeze temporar sau să le întârzie atacul, situaţie când se impune să opereze, în primul rând, detectarea intenţiei de atac sau atacul propriu-zis.

Principalele aspecte vizate de securitatea sistemelor informaţionale publice şi private sunt: securitatea locului de amplasare a centrelor de prelucrare a datelor, securitatea echipamentelor, securitatea softului, securitatea personalului, securitatea la nivelul întregului sistem informatic.

Măsurile şi responsabilităţile aplicabile în privinţa securităţii sistemelor sunt diferite, într-o anumită măsură, în sectorul public faţă de cel privat.

CAPITOLUL VII

# Securitatea telecomunicaţiilor

În pofida căderii *dot com*-urilor, adică a companiilor ce se ocupă îndeosebi cu comerţul electronic, viitorul nu poate fi schimbat, în sensul că o astfel de formă de comerţ, bazată pe tehnologii de ultimă oră, orientate spre informaţii şi comunicaţii, va avea un curs firesc. Politica statelor a fost una foarte agresivă. Investiţiile în tehnologii orientate spre reţele au explodat în toată lumea. Capitolul de faţă îşi propune să treacă în revistă principalele elemente legate de interceptarea comunicaţiilor, de securitatea transmisiilor, radiaţiilor, securitatea tehnică şi a tehnologiilor mobile, dorind ca, la finalul său, să se atingă următoarele obiective:

- stăpînirea de către cititor a principalelor concepte din domeniile menţionate;
- cunoaşterea principalelor pericole care afcetează mediile de transmisie a datelor;
- posibilitatea de a lua măsuri care să asigure securitatea transmisiilor.

## 7.1 Interceptarea conversaţiilor

De la începutul lor, sistemele de comunicaţie au fost vulnerabile în faţa celor puşi pe furt sau distrugeri. Furtul însemna pe atunci să vorbeşti fără să plăteşti şi astfel a apărut o categorie, a *phreak*-erilor, definită mult mai târziu de la apariţie, într-un mod similar hackerilor, ocupaţi îndeosebi de „hăcuirea" calculatoarelor. O a doua etapă a fost cea declanşată de pungaşi, în dorinţa lor de a comunica între ei fără ca poliţia să le intercepteze convorbirile. Într-o nouă fază, când piaţa telecomunicaţiilor s-a liberalizat, au început atacurile companiilor împotriva clienţilor altor companii sau acestea au început să se lupte între ele. Aproape întotdeauna măsurile de apărare luate erau tardive, căci apărea pe piaţă alt sistem de atac. Ceva similar se întâmplă acum cu Internetul, numai că vitezele actuale sunt mult mai mari.

Se desprinde concluzia că majoritatea comunicaţiilor sunt vulnerabile în faţa intenţiilor de interceptare. Facem doar menţiunea că unele interceptări sunt înfăptuite cu multă uşurinţă, iar altele numai cu instrumente speciale şi cu resurse considerabile.

Când atacul nu afectează conţinutul comunicaţiei, iar persoanele care comunică între ele nu sesizează că sunt ascultate, se spune că este un *atac pasiv*. La polul opus se află atacurile care distrug sau distorsionează semnalele, numite *atacuri active*. Interceptarea se poate realiza cu microfoane receptoare („bugs"), prin înregistrarea pe casetă sau bandă magnetică, prin scannere de celulare radio-receptoare, receptoare de microunde şi de sateliţi, prin pătrunderea în reţelele de calculatoare, precum şi prin utilizarea altor filtre de informaţii. Microfoanele parabolice pot detecta conversaţiile de la o distanţă de peste un kilometru, iar variantele laser interceptează discuţiile purtate chiar în spatele geamurilor închise.

De regulă, este foarte greu să ştii în ce loc se efectuează supravegherea comunicaţiei. De aceea, trebuie pornit de la premiza că orice conversaţie care conţine informaţii valoroase este posibil să fie urmărită de cei interesaţi. Pentru contracarare pot fi luate două măsuri preventive:

a) de evitat subiectele sensibile în discuţiile telefonice sau în transmisiile fax;
b) dacă telefonul sau faxul trebuie să fie folosite, atunci pentru informaţiile speciale se recomandă criptarea.

Pentru a se evita includerea numelui organizaţiei unde lucrăm sau chiar al nostru pe lista neagră a căutătorilor de informaţii speciale, se recomandă ca în fazele discuţiilor telefonice sau ale textelor transmise prin fax să nu figureze anumite tipuri de informaţii, cum ar fi numele organizaţiei, numele codurilor proiectelor, denumirea produselor, numele persoanelor-cheie din organizaţie ş.a. Pentru a-şi atinge obiectivele, agenţiile specializate în căutarea informaţiilor speciale apelează la căutări automate, prin cuvinte-cheie aflate într-o bază de date predefinită.

Criptarea convorbirilor telefonice se realizează cu o aparatură specială. Guvernul şi industria de apărare ale SUA folosesc STU-III (*Secure Telephone Unit*) pentru comunicarea informaţiilor clasificate prin telefon, sub formă criptată.

## 7.1.1 Telefoanele standard

Telefonul a devenit un obiect nelipsit din viaţa noastră. Formelor tradiţionale li s-au adăugat sistemele moderne, ale telefoniei mobile, care conturează un mediu cu totul nou pentru afaceri, diferit de comerţul sau afacerile electronice, numit comerţ sau afaceri mobile.

În paragraful de faţă ne propunem, însă, să discutăm despre telefoanele standard şi rolul lor într-un sistem de prelucrare automată a datelor. Referirea la ele o vom face prin două componente esenţiale:

a) moduri de transmisie;

b) aparatul telefonic standard.

Transmisia se poate efectua prin *cablu*, prin *satelit* sau prin *microunde terestre*.

### 7.1.1.1 Securitatea cablurilor de comunicaţie

Primele sisteme telefonice s-au bazat pe *perechea de fire neizolate*. Tendinţa este ca în configuraţia reţelelor locale (LAN) să se utilizeze *cablul coaxial*, deşi cea mai securizată şi mai performantă este *fibra optică*. În schimb, ea este mai scumpă şi mai pretenţioasă la instalare şi întreţinere.

Metoda securităţii liniilor se referă la tot ceea ce se întâmplă între centrala companiei telefonice şi calculatorul central al unităţii.

Când se pune problema liniilor telefonice, un aspect important îl constituie integritatea cablului. Oriunde este posibil, o linie de comunicaţie, care serveşte un centru de prelucrare automată a datelor, trebuie să fie una directă între acesta şi cea mai apropiată centrală telefonică. O astfel de legătură nu va permite amatorilor de interceptări ilegale de semnale să-şi atingă scopul.

Sunt, totuşi, companii telefonice în care se utilizează sistemul deschiderilor multiple, cablurile fiind orientate în mai multe casete de joncţiune, amplasate în locuri mai dosnice (subsolul clădirii, holuri necirculate ş.a.) de unde terminaţiile firelor disponibile pot fi folosite oricând de compania telefonică, dar, la fel de bine, ele pot fi destul de uşor deschise de cei rău intenţionaţi pentru a se lega la liniile la care au interes.

Când în unitate se impune utilizarea conductorilor multipli, pentru a satisface nevoile funcţionale ale unităţii de prelucrare automată a datelor, se recomandă cablurile cu cel mai mare număr de conductori pentru a face cât mai dificilă operaţiunea de selecţie a liniei care îi interesează pe atacatori.

Nu se admit liniile cu circuite cuplate, deşi deseori apar suprapuneri de transmisii, chiar dacă nu sunt folosite cuplajele, cauza fiind ori atingerea firelor, ori defectarea transformatoarelor sau a altor elemente din circuit, de cele mai multe ori factorii naturali având un rol determinant.

Pentru evitarea unor stări neplăcute, se recomandă ca firele de transmisie să fie ecranate şi să se realizeze şi aşa-zisele împământări. Ultima operaţiune se efectuează pentru eliminarea nedoritelor radiaţii. În acest scop, un cablu care efectuează legătura dintre două calculatoare trebuie să aibă împământări la fiecare 10 metri.

Există şi posibilitatea apărării împotriva „ascultătorilor” de fire, prin apelarea la aşa-zisul *fir-capcană*, neizolat, răsucit pe firul ecranat, iar, când ecranajul este distrus, firul-capcană produce un semnal de alarmă. Ca forme de utilizare, sistemele de punere în funcţiune a firului-capcană sunt foarte diversificate.

### 7.1.1.2 Securitatea transmisiilor prin satelit

Atunci când se iniţiază o convorbire telefonică sau se intenţionează transmisia unui fax, nu avem idee pe ce canal de comunicaţie se va înfăptui acţiunea declanşată de noi, întrucât

echipamentele de comutare automată stabilesc ruta pe o linie terestră, pe una bazată pe microunde terestre sau prin satelit – depinzând de metoda folosită şi de eficienţa din acel moment.

Majoritatea apelurilor pe distanţe lungi sunt realizate, fie şi parţial, prin unde propagate în aer – fie prin satelit, fie între releele staţiilor terestre bazate pe microunde – iar tot ceea ce se deplasează în aer poate fi interceptat.

Tehnologiile folosite pentru monitorizarea sau interceptarea comunicaţiilor prin microunde şi satelit păreau complicate şi necesitau imense investiţii guvernamentale, însă în prezent grupurile sau persoanele ce dispun de resurse financiare rezonabile au la dispoziţie echipamente ce pot fi procurate din magazin în forma dorită de ei. Cele mai simple interceptări sunt efectuate prin căutări de cuvinte-cheie sau de numere de abonat, totul fiind efectuat cu ajutorul calculatoarelor.

Ca regulă generală, semnalele se transmit prin linii terestre sau prin microunde către o staţie de comutare de lungă distanţă. Calculatorul companiei telefonice va căuta cea mai eficientă cale pentru transmiterea semnalului. Să presupunem că s-a efectuat conexiunea prin satelit. Apelul nostru este dirijat spre o staţie terestră, de unde este transmis către un satelit şi apoi plasat pe o staţie terestră. De aici apelul merge printr-o linie terestră sau prin microunde terestre către o staţie de comutare, unde are loc desprinderea de alte semnale şi plasarea lui pe cablu până la telefonul receptor, unde are loc retransformarea lui în voce sau mesaj fax. Tot ce am descris în acest aliniat se derulează într-o fracţiune de secundă. Tot mai mulţi sateliţi sunt plasaţi pe orbită pentru a face faţă cererii crescânde de telecomunicaţii. Legătura satelitului cu pământul este uşor interceptată, căci nu se realizează printr-un fascicul îngust, ci printr-un semnal de microundă care se dispersează în mai multe direcţii. Cu cât este mai sus satelitul, cu atât este mai extinsă aria terestră pe care se poate recepţiona mesajul, deci şi interceptat. Din multitudinea de sateliţi, „urma" satelitului sau zona în care semnalele acestuia pot fi recepţionate pe pământ înseamnă câteva mii de mile diametru. „Urma" poate fi îngustată prin coborârea orbitei satelitului sau mărirea dimensiunilor antenei-satelit, deşi recepţia se va efectua încă pe o zonă destul de extinsă.

Oricine posedă o antenă-satelit şi ceva echipamente specializate, şi se plasează în zona în care se află „urma" unui satelit, poate intercepta mesajul, aşa cum recepţionezi posturi TV. Iată de ce este atât de simplă interceptarea comunicaţiilor derulate prin satelit, operaţiune ce se poate înfăptui din clădirile ambasadelor, din clădirile deţinute de persoane străine, de pe vapoarele ce poposesc în porturile mărilor de coastă sau de la baze străine.

În pofida legislaţiei destul de clare privind interceptările, se înregistrează numeroase abateri. De exemplu, în SUA, legea federală interzice producerea, vânzarea, posesia şi promovarea echipamentelor folosite pentru interceptări. Şi, totuşi, o firmă, *The Spy Factory*, cu un lanţ de 12 magazine, a fost descoperită de FBI că deţinea mii de microfoane minuscule, inclusiv transmiţătoare ascunse în bilele minelor de pix, în calculatoare, în ştechere, în transformatoare, în casete minuscule ascunse în birouri, pe sub mese. Firma vindea echipamente de înregistrat ce se ataşau direct la o linie telefonică şi transmiteau comunicaţiile într-un loc aflat la distanţă, precum şi echipamente pentru interceptarea apelurilor telefoanelor celulare. Cumpărătorii erau partenerii de afaceri suspicioşi, concurenţii şi îndrăgostiţii geloşi.

### 7.1.1.3 Securitatea microundelor terestre

La început se credea că microundele terestre vor constitui mijlocul principal de transmitere a comunicaţiilor pe distanţe lungi, ele traversând întreg teritoriul Statelor Unite ale Americii şi, de aici, oriunde altundeva în lume. N-a fost să fie aşa, căci majoritatea comunicaţiilor pe distanţe lungi se efectuează prin satelit sau prin linii terestre de fibră optică, iar microundele terestre sunt folosite pentru traficul pe distanţe scurte sau între un oficiu telefonic şi cea mai apropiată legătură cu un satelit sau linie terestră.

Transmisiile de microunde terestre se înfăptuiesc la nivelul releelor plasate la 15-20 km unele de altele, căci semnalele se transmit în linie dreaptă şi nu urmează denivelările terestre. Cu cât frecvenţa este mai înaltă, cu atât distanţa dintre relee este mai mică.

Ca şi comunicaţiile prin satelit, cele prin microunde terestre sunt foarte uşor de interceptat de către oricine dispune de un echipament adecvat, pentru că ele au un punct slab, exploatat de către cei rău intenţionaţi, şi anume fasciculul este puternic răsfirat între releele participante la transmisie. Cu o antenă parabolică bine focalizată este posibil de interceptat semnalul respectiv.

#### 7.1.1.4 Securitatea aparatelor telefonice standard

Pentru evitarea posibilelor pierderi de informaţii, se recomandă numai aparatura capabilă să le preîntâmpine sau să anihileze eventualele atacuri.

Sunt trei elemente cărora trebuie să li se acorde o importanţă deosebită:

- soneria;
- piesele falsificate;
- piesele străine.

*Soneria*. Bobinele soneriilor din telefoanele obişnuite pot acţiona ca dispozitive de captare şi transmitere în linie, chiar şi atunci când receptorul este pus în furcă. Pentru a ne asigura împotriva unei astfel de surse compromiţătoare, se deconectează bobina în întregime şi se înlocuieşte cu o lampă ce se va cupla la un curent de 85 volţi (de activare a soneriei clasice), transmis prin semnal la receptor. Dacă se doreşte şi un semnal sonor, se poate apela la o alarmă electronică acţionată prin celulă fotoelectrică.

*Piesele falsificate*. Literatura de specialitate consemnează numeroase cazuri de falsificare a unor componente ale telefonului, introducând în piesele foarte cunoscute anumite elemente capcană. Există tehnici de depistare şi distrugere a lor, prin pulsuri de curenţi distructivi.

Cele mai cunoscute sunt metodele de adăugare la *piesele* existente a unora *cu rol special, de captare şi emisie***.** Ele se pot descoperi printr-o analiză atentă a componentelor telefonului.

Tot în cazul telefoanelor se discută şi despre aşa-zisul *sistem muzicuţă*, numit astfel deoarece se apelează la componente speciale, sub variate forme, care servesc drept aparate de ascultat în clandestinitate, în timp ce aparatul este aşezat în furcă, dar operaţiunea are loc nu în sistem continuu, ci sub controlul de la distanţă al interceptorului neautorizat de semnale. O astfel de „muzicuţă" va „cânta" doar la comandă, ceea ce ar însemna că, în momentul când pe linie se transmite un anumit semnal, se dă comanda de activare a unor microfoane speciale, ocolindu-se sistemul care activează soneria telefonului. „Muzicuţa" poate să dispună şi de un comutator de autodecuplare, activat de zgomote speciale, cel mai important fiind cel produs de ridicarea receptorului din furcă, moment în care s-ar putea descoperi ascultările ilegale.

Cum o „muzicuţă" este realizată din mai multe componente electronice, pentru cei avizaţi este relativ simplu de sesizat prezenţa lor în aparatul telefonic, dar pentru marea majoritate a utilizatorilor de telefoane ele rămân piese „veritabile" ale telefonului. Analiştii de linii, la rândul lor, dispun de tehnici speciale de depistare a unor astfel de intruşi.

Un principiu vital de apărare constă în evitarea instalării telefoanelor în zonele foarte importante ale centrului de prelucrare a datelor. Dacă acest lucru nu este posibil, se va trece la deconectarea aparatului atunci când se consideră că dialogul din camera respectivă este deosebit de important şi ar putea prezenta interes şi pentru alţii.

Pentru asigurarea unui control riguros asupra propriului personal, se recomandă apelarea la aparatură care să înregistreze data, ora şi destinaţia apelului telefonic pornit din centrul de prelucrare automată a datelor. Nu este considerată exagerată măsura ţinerii sub lacăt a aparaturii telefonice, mai ales acum, când prin e-mail se poate ieşi cu uşurinţă ... în lume.

De asemenea, se poate ţine legătura sistematic cu personalul specializat în telefonie pentru a afla cât de sigur este sistemul utilizat pentru prelucrarea datelor, dar şi cât de vulnerabil este în faţa potenţialilor atacatori.

Pentru un plus de precauţie, în cazul sistemelor foarte importante, se poate apela la „identificarea automată a numerelor” care au contactat sistemul nostru.

În afara rolului avut în prevenirea ascultărilor neautorizate, înregistrarea convorbirilor telefonice de pe liniile unei firme este susţinută şi de alte cinci argumente, după cum urmează:

1. asigurarea înregistrării complete a activităţilor prilejuite de stingerea incendiilor sau de alte dezastre ale naturii;
2. înregistrarea potenţialelor ameninţări cu bombe sau alte forme de atacare în forţă a sistemului;
3. ţinerea evidenţei sesiunilor de teleprelucrare pentru a înlesni obţinerea copiilor de siguranţă şi restaurarea fişierelor în cazul pierderii formei lor originale;
4. constituirea de probe în cazul utilizării neautorizate a componentelor de teleprelucrare;
5. obţinerea probelor împotriva angajaţilor care săvârşesc acte de fraudă la adresa unităţii.

Pentru realizarea acestor obiective, ca element tehnic de ajutor, intervine tot calculatorul, numai că el este unul special, realizat relativ recent, cu scopul de a înregistra cine a făcut apelul din unitate, data, ora, unde a sunat, cât timp a durat convorbirea.

Se pune, totuşi, întrebarea: cum aflăm că suntem „ascultaţi”? Un bun „ascultător” nu face zgomot în timpul misiunii şi transmite curenţi foarte slabi sau, uneori, aceştia nici nu există. În concluzie, ascultarea liniei, cu scop de verificare, este fără prea mari şanse de reuşită. Chiar şi voltmetrele, cât ar fi ele de sensibile, nu constituie o aparatură de detectare deosebit de puternică.

Ca o măsură eficientă, se recomandă înregistrarea pe bandă a zgomotelor din linie, metodă ce duce şi la înregistrarea sunetelor foarte fine produse de aparatele ce efectuează înregistrări ilegale, fie şi pentru perioade foarte scurte de timp. Înregistrarea pe banda de control se va lansa prin intermediul unui comutator automat, declanşat de zgomotele sesizate în linie.

Absenţa tonului din aparatul telefonic este un semn de ascultare, dar profesioniştii în furturi evită o astfel de tehnică deconspiratoare. Un alt semn al interceptărilor neautorizate îl constituie sesizările repetate ale prietenilor că telefonul nostru este cam tot timpul ocupat, deşi se ştie că în realitate n-a fost aşa.

O măsură de apărare împotriva ascultătorilor neautorizaţi, chiar şi când telefonul este în furcă, o constituie crearea unor sunete electrice înalte în locurile în care bănuim că intruşii ar fi interesaţi să asculte.

O altă cale, ce duce la diminuarea pericolului ascultării, o constituie folosirea modemurilor sau apelarea la servicii telefonice cu viteze mari, chiar dacă presupun un cost ceva mai mare. Şi multiplexoarele diminuează şansele intruşilor din liniile de comunicaţii.

Nu trebuie să încheiem succinta abordare a problemei de faţă fără să amintim de particularităţile reţelelor de transmisie a datelor şi de multitudinea aspectelor specifice transmiterii de date prin radio.

## 7.1.2 Securitatea celularelor

Un telefon celular are trei vulnerabilităţi majore pe linia securităţii:

- vulnerabilitatea la monitorizarea conversaţiei în timpul folosirii telefonului;
- vulnerabilitatea telefonului de a fi pe post de microfon pentru monitorizarea conversaţiilor din preajma sa în timp ce telefonul este inactiv;
- vulnerabilitatea de a fi „clonat” sau de a se folosi numărul nostru de telefon de către alţii, înregistrând convorbirile în contul nostru.

Pentru a înţelege slăbiciunile telefoanelor celulare este bine să cunoaştem câteva detalii privind modul lor de funcţionare. Ele se bazează pe frecvenţe radio prin aer pe două canale distincte, unul pentru comunicaţiile vocale, iar celălalt este folosit pentru semnalele de control. Când un celular este activat pentru prima dată, el emite un semnal de control, prin care se identifică faţă de un „site de celulă”, transmiţându-i numărul de identificare al mobilului (*MIN, Mobile Identification Number*) şi numărul de serie electronic (*ESN, Electronic Serial Number*),

cunoscute sub numele generic de pereche (*pair*). Când site-ul celulei primeşte semnalul pereche, determină dacă solicitantul este înregistrat oficial, prin compararea perechii solicitantului cu lista abonaţilor la telefonia celulară. Îndată ce perechea de numere este recunoscută, site-ul celulei emite un semnal de control, prin care îi permite abonatului să facă apeluri. Un astfel de proces, cunoscut sub numele de înregistrare anonimă, se realizează de fiecare dată când telefonul este activat sau este recepţionat de un nou site-celulă, aflându-se în raza lui de acţiune.

Un telefon celular este, de fapt, un aparat radio cu emisie-recepţie. Vocea noastră este transmisă prin aer ca unde radio, iar acestea nu sunt direcţionale, ci dispersate în toate direcţiile, astfel încât oricine posedă un anumit tip de radio receptor poate să le intercepteze. Sunt foarte mulţi radio-amatori care au site-uri web prin care se schimbă numere de telefon ale unor ţinte „interesante". Uneori persoanele oportuniste cu un astfel de hobby îşi vând „colecţiile".

Dacă sistemul celular foloseşte tehnologia analogică, cineva poate programa un număr de telefon sau o listă de numere de telefon supravegheate într-un echipament de monitorizare a celulelor care activează automat un înregistrator de voce, oricând un număr de telefon, aflat pe lista supravegheaţilor, este în folosinţă. Urmărirea automată, asistată de calculator, permite monitorizarea unui telefon anume 24 de ore din 24, după cum ţinta se deplasează de la o celulă la alta, fără un alt efort uman.

Dacă sistemul de telefonie celulară foloseşte tehnologia mai nouă, digitală, supravegherea este mult mai dificilă, dar, la preţuri rezonabile, este posibil ca majoritatea radio-hobbiştilor să cumpere un interpretor de date digitale care se conectează între un scanner radio şi un calculator personal. Interpretorul datelor digitale citeşte toate datele digitale transmise între site-ul celulei şi telefonul celular şi oferă calculatorului aceste informaţii.

Este destul de simplu pentru un „ascultător" să fixeze numărul de telefon celular al ţintei pentru că transmisiile sunt în dublu sens către site-ul celulei, atât timp cât telefonul este alimentat de la baterie şi este pregătit să primească apeluri.

Pe pieţele occidentale există un echipament numit *Celltracker* (urmăritor de celulă), cu care un „ascultător" se poate orienta spre conversaţiile ce apar la un anumit telefon celular prin intermediul celui mai apropiat site-celulă. Numărul telefonului urmărit se introduce în echipament prin tastatură. Agenţiile secrete, precum şi cele ce supraveghează modul de respectare şi punere în aplicare a legii, au la dispoziţie echipamente şi mai performante. De exemplu, *Law Enforcement Corp* face publicitate unui sistem care monitorizează 19 canale şi urmăreşte trei conversaţii simultan.

Aşa se explică uşurinţa cu care convorbirea dintre prinţesa Diana şi prietenul ei, James Gilbey, a fost înregistrată pe bandă, timp de 23 de minute. Ulterior a fost publicată, aflându-se că prietenul prinţesei o alinta cu „draga mea sepie". Nici prinţul Charles n-a scăpat. El a fost înregistrat în timp ce discuta cu Camilla despre viaţa lor sexuală. La fel s-a întâmplat cu purtătorul de cuvânt al Casei Albe, Newt Gingrich. România nu este mai prejos. Vă amintiţi de discuţia dintre un membru al guvernului din perioada 1992-1996 şi un senator, nu prea academică, prin care se negociau nişte spaţii „mai umane". Sau, în 2002, scandalul interceptării convorbirilor telefonice ale ziariştilor ieşeni. Ca o concluzie, nu trebuie să fii la S.R.I. pentru a intercepta astfel de telefoane. După ce în SUA s-au interzis importurile, producerea şi vânzarea scannerelor de celulare, specialiştii au demonstrat cum, într-un minut, cu două fire scurte de sârmă şi un ciocan de lipit, un scanner legal radio se transformă într-un colector impecabil de convorbiri de pe celulare. S-a făcut chiar afirmaţia că, din 10 milioane de scannere vândute legal în SUA, câteva sute de mii au fost modificate pentru a intercepta celulare.

*Vulnerabilitatea celularului de a fi folosit drept microfon* este o „performanţă" pe care o ştiu foarte puţini dintre beneficiarii telefoniei mobile. Se pare că astfel şi-a găsit sfârşitul un lider rebel al unui fost stat sovietic sau aşa ne explicăm de ce teroriştii nu prea apelează la telefonia celulară. Ei ştiu că un telefon celular poate fi transformat într-un microfon şi emiţător cu scopul de a asculta conversaţiile din preajma lui. Noua funcţie se realizează prin transmiterea către telefonul celular a unei comenzi de întreţinere pe canalul de control, operaţiune care aduce

telefonul mobil în „modul diagnostic", după care orice conversaţie din preajma telefonului mobil poate fi monitorizată prin canalul de voce. Interesant este că utilizatorul nu-şi să seama că este în modul diagnostic şi că se recepţionează toate sunetele din jurul lui, până când va încerca să sune pe cineva şi-şi va da seama că ceva nu merge. În astfel de situaţii, înainte ca telefonul să fie folosit pentru noi apeluri, aparatul trebuie să fie închis şi apoi deschis. Iată de ce nu trebuie să fie permis accesul cu telefoane mobile în sălile sau zonele în care se discută lucruri sensibile sau se face trimitere la informaţii clasificate.

*Vulnerabilitatea la clonare* este cea mai „elegantă" formă de a fura pe cineva, prin telefonia mobilă, fără să-i furi aparatul. Este de ajuns ca noii hoţi să monitorizeze spectrul frecvenţelor radio şi să-şi însuşească perechea de numere a telefonului celular, atunci când se face înregistrarea anonimă la un site de celulă. Clonarea este procesul prin care un hoţ interceptează numărul de serie electronic, *ESN*, şi numărul de identificare mobil, *MIN*, apoi programează aceste numere într-un alt telefon şi-l face identic cu cel al posesorului de drept, utilizându-l exact ca abonatul serviciului telefonic mobil.

Numai în SUA, la nivelul unui an, s-au înregistrat furturi care se apropie de miliardul de dolari, iar arestările au fost de ordinul miilor. Cel mai cunoscut este cazul lansării a 1500 de apeluri telefonice într-o singură zi de către hoţii perechii de numere a unui abonat.

*ESN*-ul şi *MIN*-ul se pot obţine foarte uşor cu un cititor de *ESN*-uri, care arată ca şi un telefon celular receptor, conceput să monitorizeze canalele de control. El captează perechile de numere în momentul în care acestea sunt transmise de la un telefon celular la un site de celulă şi memorează informaţiile respective în propria-i memorie. Operaţiunea este uşor de realizat căci, de fiecare dată când activăm celularul sau intrăm în raza altui site de celulă, de la aparatul nostru se transmite perechea de numere către site-ul celulă, pentru fixarea canalului de voce.

Deşi pare cam defetistă afirmaţia noastră, în concluzie, putem spune că nici un abonat nu poate fi ferit de clonarea telefonului său mobil. Ea se efectuează cel mai mult în locurile aglomerate: parcări mari, aeroporturi, supermagazine, săli de concerte, stadioane şi în toate zonele foarte aglomerate ale oraşelor. De puteţi evita folosirea celularului în astfel de locuri, aţi făcut deja un pas mare spre evitarea clonării.

În final, vă prezentăm câteva măsuri pe care statele civilizate le recomandă utilizatorilor de celulare pentru a le asigura propria lor securitate. Se spune că cea mai bună apărare împotriva celor trei vulnerabilităţi majore ale celularelor ar fi una foarte simplă: nefolosirea lor. Şi, totuşi, dacă le folosiţi încercaţi să reduceţi riscurile, respectând următoarele sfaturi:

- pentru că celularul se poate transforma oricând într-un microfon, fără să ştim când, nu trebuie să-l purtăm cu noi în locurile în care se discută lucruri sensibile sau se face referire la informaţii clasificate;
- activaţi-vă telefonul doar în anumite momente, îndeosebi atunci când vreţi să apelaţi pe cineva. În alte condiţii, închideţi-l!
- nu oferiţi oricui numărul dumneavoastră de mobil. Este o mare greşeală. Ca atare, nu-l puneţi pe cărţi de vizită, pe pagina web, pe corespondenţa zilnică!;
- dacă puteţi, nu folosiţi mobilul pentru a fi apelaţi de alţii, căci aceasta înseamnă activarea lui continuă şi, firesc, posibilitatea urmăririi continue a dumneavoastră. În acest scop se recomandă folosirea de pager pe care să primiţi semnalele de la cei ce vă interesează. După primirea lor, puteţi activa şi folosi mobilul pentru o scurtă perioadă de timp;
- nu discutaţi lucruri importante prin telefonul mobil. Când sunaţi pe cineva, puneţi-l în gardă că vorbiţi de pe mobil şi atenţionaţi-l, dacă e cazul, că mobilul e vulnerabil şi că trebuie să se poarte doar discuţii generale, fără detalii;
- nu lăsaţi mobilul nesupravegheat;
- evitaţi folosirea telefonului mobil în locuri foarte aglomerate şi în imediata lor apropiere. Aici este terenul propice pentru radio-amatorii ce folosesc scannere pentru

monitorizări aleatoare. Dacă v-au identificat şi „le place" discuţia, vă vor reţine pentru monitorizarea permanentă;

- dacă vi se oferă de către compania telefonică un PIN (Personal Identification Number), folosiţi-l o dată şi nu la fiecare activare, că şansele de a fi clonat aparatul sunt mai reduse.

Există o zicere înţeleaptă care spune: Doamne, spune-mi duşmanul care mi-e prieten, căci pe ceilalţi îi ştiu eu! Unde plasaţi celularul!?!

- Adaptaţi formele de manifestare a pericolelor în sistemele informaţionale prezentate în subcapitolul 1.2.3. la tehnologiile mobile, identificând factori naturali, incidente şi atacuri care afectează datele şi informaţiile transmise în mediul mobil .
- Câte vulnerabilităţi asociate Bluetooth cunoaşteţi? Noi începem lista cu *bluejacking*...

## 7.1.3 Securitatea telefoanelor portabile

Telefoanele portabile au constituit, la vremea lansării lor pe piaţă, o realizare deosebită, prin dispariţia unicului loc de unde se putea vorbi în sistemul telefoniei fixe. Iată că şi numele îşi pierde sensul odată cu inventarea telefonului portabil. S-au înregistrat multe satisfacţii în lumea utilizatorilor fără ca ei să-şi dea seama că totul se plăteşte. În cazul de faţă, comoditatea purtării unei convorbiri telefonice era eclipsată de creşterea insecurităţii, cât timp transmisiile pot fi recepţionate de la mai mult de un kilometru distanţă. Cu un telefon analogic foarte ieftin, oricine posedă un scanner radio şi se află în vecinătatea unui telefon portabil poate să-şi regleze scannerul pe conversaţia respectivă şi să o asculte. De asemenea, interceptarea se poate efectua printr-un aparat similar portabil sau printr-un *baby monitor*, utilizat pentru supravegherea copiilor.

O soartă similară o au microfoanele portabile folosite la şedinţele de lucru sau la conferinţe. Ele transmit semnale foarte clare în exterior, de unde pot fi interceptate chiar de la câteva sute de metri. Din această cauză folosirea lor trebuie să fie condiţionată de categoria informaţiilor comunicate, evitându-se cele clasificate şi/sau neclasificate speciale.

Din această categorie, telefoanele digitale sunt mai sigure, întrucât interceptarea pe canalul de voce a unor semnale digitale înseamnă recepţionarea unui simplu zgomot. Totuşi, radio-amatorii mai pretenţioşi pot să apeleze la tehnologii care să transforme semnalele digitale în voce. Cele mai securizate sunt aparatele portabile care operează în spectrul de 900 MHz şi 2,4 GHz. Acestea au o lăţime a benzii foarte mare şi nu pot fi urmărite cu aparatura obişnuită de scannare a frecvenţelor radio. Doar aparatura foarte performantă poate fi folosită pentru interceptare.

Oricum, un posesor de aparat portabil poate fi duşmanul principal al altui posesor de aparat identic, prin furtul tonului şi folosirea lui pentru conversaţii facturate titularului aparatului.

Procedura este foarte simplă. Cineva, cu un aparat portabil activat, urcă în propriul autoturism şi începe să se plimbe pe o stradă unde ştie că sunt mai multe portabile sau bănuieşte acest lucru. Când telefonul lui primeşte semnalul de ton înseamnă că aparatul este compatibil cu cel din zona în care se află şi astfel poate să înceapă convorbirile în contul altuia. Şi dacă cineva ridică telefonul interceptat nu-şi dă seama de ceea ce se întâmplă, ci doar dacă, accidental, priveşte pe geam, vede că într-un autoturism cineva vorbeşte la telefon.

Dacă producătorul atribuie un cod de securitate aparatului, scenariul de mai sus încă este valabil căci persoana se va plimba până va găsi un alt aparat cu codul fabricii identic cu al ei.

## 7.1.4 Securitatea poştei vocale (Voice Mail, V-Mail)

Una dintre performanţele deosebite ale poştei vocale constă în posibilitatea accesării de la distanţă a acesteia. Nu este necesară deplasarea la birou pentru a-ţi consulta poşta vocală, ci de la distanţă. După lansarea apelului telefonic, prin introducerea unei parole, se pot asculta mesajele înregistrate. Din păcate aceeaşi operaţiune poate fi efectuată şi de o terţă persoană.

Ghicirea parolei nu este o mare problemă, pentru că sunt prea puţine persoanele care se preocupă de utilizarea unei parole unice, diferită de cea implicită care vine odată cu sistemul instalat. Ea este, de regulă, formată din ultimele patru cifre ale telefonului sau numărul interior al angajaţilor. Alteori, când se schimbă parola, greşelile sunt comune, apelându-se la nume sau persoane sau data naşterii.

Cele mai mari ameninţări vin de la foştii angajaţi care cunosc numărul de telefon al poştei vocale şi pot intui parolele cu uşurinţă.

Cu câţiva ani în urmă, preşedintele unei companii de valori imobiliare a anunţat Serviciile Secrete ale S.U.A. că hackerii i-au atacat calculatorul care gestiona mesajele vocale. Ancheta a condus la Leslie Lynne Doucette, cunoscută şi sub numele Kyrie, care era capul unei reţele ce se ocupa de fraudele prin calculatoarele ce administrau poşta vocală din S.U.A. Asupra ei s-au găsit 481 coduri de acces, folosite de 152 hackeri.

De regulă, puştii de 13-15 ani dau lovituri mari, fie folosind sistemul pentru convorbiri la distanţe mari, fie pentru a intra în posesia unor informaţii importante despre firme. Au fost puternic mediatizate nelegiuirile înfăptuite de „Domnul Nimeni” (*Mr. Nobody*) sau „Fantoma Celularelor” (*Cellular Phantom*).

Dintr-un studiu efectuat în Anglia a reieşit că jumătate dintre hackeri – mai degrabă i-am numi *phreackeri* – sunt elevi sau studenţi, între 14 şi 22 de ani. Cam o treime nu erau angajaţi, iar vârsta lor se situa între 18 şi 35 de ani. Restul aveau vârste între 18 şi 31 de ani. Media generală de vârstă a tuturor era de 21 de ani.

### 7.1.5 Securitatea robotului telefonic

Robotul telefonic (*answering machine*) este o invenţie destul de comodă pentru persoanele foarte ocupate sau pentru cele ce vor să răspundă selectiv la apelurile telefonice primite. Nu întotdeauna putem să răspundem la telefon, aşa că se va apela la robotul telefonic. Deseori mesajele înregistrate pe casetă, adresate persoanelor care ne apelează, sunt total neinspirate. Un exemplu este cel ce spune că lipsim din localitate două săptămâni, dar putem citi mesajul telefonic. Cei ce recepţionează un astfel de mesaj ştiu foarte bine ce au de făcut, casa fiind nelocuită o bună perioadă de timp. Dar insecuritatea provine şi din alte cauze. Vulnerabilitatea este aproape similară celei descrise la poşta vocală. Accesul de la distanţă este o înlesnire bine venită pentru posesorul telefonului cu robot dar, în acelaşi timp, el oferă impostorilor şansa să-l utilizeze. Ei pot forma numărul nostru şi asculta mesajele. Singura protecţie constă într-un cod scurt, presetat de producător, şi care rareori este schimbat de cumpărător. Codul de folosire este cunoscut de cei ce se ocupă cu astfel de activităţi. Şi dacă este schimbat, codul poate fi uşor spart de „profesionişti”.

Roboţilor telefonici li s-a mai adăugat o a doua vulnerabilitate: lor li s-a introdus funcţia ce-i permite proprietarului să sune acasă şi să asculte ce se întâmplă acolo, telefonul acţionând ca un microfon ce va capta fondul sonor al locuinţelor. Totul este frumos, numai că realizatorii acestei performanţe tehnice nu s-au gândit că la fel poate proceda şi o terţă persoană care ar dori să intre în intimitatea casei noastre.

### 7.1.6 Interfonul casei şi supraveghetorii de copii (*Baby Monitors*)

În urmă cu vreo câţiva ani mă aflam în casa unui croitor şi am asistat la un dialog al acestuia cu fiul său aflat într-o altă parte a casei, prin intermediul unui mic aparat aflat într-o priză a camerei. M-am minunat cât de simplu puteau dialoga de oriunde se aflau membrii familiei. Firesc, dacă aveau într-o priză câte o astfel de minune. Ulterior am aflat cât de simplă este tehnologia, dar, mai ales, cât este de vulnerabilă.

Sistemul de comunicaţii din casă se bazează pe un set de transmiţătoare şi cu emiţătoare care apelează la energia electrică a firelor instalaţiei din casă în două moduri: transformă curentul alternativ în curent cărăuş şi, în acelaşi timp, foloseşte firele drept antenă pentru a

transmite mesajele de la emiţător la receptor. Tehnologia se numeşte *carrier curent*, adică ar fi curentul cărăuş. Ceea ce nu ştia croitorul este faptul că dialogurile lor, atât de uşor realizate, puteau fi interceptate şi de alţii aflaţi pe stradă, cu condiţia să aibă un aparat similar care să funcţioneze pe aceeaşi frecvenţă sau să deţină un scanner de frecvenţă pentru o astfel de emisie.

Procedeul este folosit în sistemul energetic, pentru a gestiona furnizarea energiei către grupurile de consumatori casnici.

Supraveghetorii copiilor (*Baby Monitors*) sunt tot echipamente independente care transmit semnale în exteriorul spaţiilor unde sunt amplasate. Majoritatea sunt puse în priza de curent alternativ şi folosesc un sistem identic celui descris anterior. Sunt şi sisteme care folosesc frecvenţele radio. Scopul unor astfel de aparate este acela de a alerta părinţii când se întâmplă ceva în camera de joacă sau în dormitoarele copiilor, situate în diverse locuri ale casei.

Odată cu liniştea oferită părinţilor, ele constituie şi un atentat la intimitatea casei prin vulnerabilitatea în faţa celor interesaţi a le intercepta.

## 7.2 Securitatea transmisiilor

Problema securităţii transmisiei de date se pune în mod deosebit atunci când două sau mai multe calculatoare sau terminale conversaţionale sunt interconectate într-o reţea. Acolo unde funcţionează o astfel de reţea, responsabilul cu prelucrarea automată a datelor din partea unităţii, contabilul şef sau vicepreşedintele coordonator al activităţii sistemului informatic trebuie să desemneze pe unul din responsabilii activităţii de prelucrare automată a datelor sau pe o altă persoană să răspundă de reţea, în sensul supravegherii tuturor activităţilor care se referă la două sau mai multe posturi de lucru în reţea.

Terminalele aflate la distanţă trebuie să funcţioneze în aşa-zisul *mod prestabilit*. El constă în stabilirea unor reguli de folosire de către utilizatorii acestor terminale numai în limitele unui program special de aplicaţii, aflat sub controlul direct al sistemului de operare, şi trebuie să realizeze două funcţii principale: intermedierea şi autentificarea.

*Intermedirea*. Un echipament independent, cunoscut, de regulă, sub numele de front-end processor, trebuie să intermedieze orice intrare, ceea ce ar însemna validarea sintactică şi logică înaintea înlesnirii accesului la calculatorul central. Ea ar consta în controlul preventiv al erorilor la intrare, al încadrării datelor în limitele unor intervale prestabilite, precum şi controlul biţilor de paritate.

Cel mai important lucru realizat prin funcţia de intermediere constă în acceptarea doar a anumitor comenzi ce pot fi transmise calculatorului central.

*Autentificarea*. Rolul ei este de a ne asigura, în avans, că fiecare comandă sau secvenţă de comenzi are un răspuns sau un efect prestabilit, ceea ce ar însemna că ea nu afectează programul aplicaţiilor, nici sistemul de operare şi nici datele cu regim special. Accesul este autentificat la anumite puncte din aplicaţii, în caz contrar utilizatorul fiind dezafectat din reţea.

Controlorul de reţea trebuie să permită doar procedurile de funcţionare care se încadrează într-un scenariu predeterminat dintre punctele terminale şi calculatorul central. Operatorii trebuie să respecte cu stricteţe modurile de lucru respective.

Fiecare calculator trebuie să poată identifica, fără ambiguităţi, traseul pe care se realizează la transmisie sau recepţie traficul de date, cunoscându-se portul sau canalul de comunicaţie.

Comunicaţiile terminalelor trebuie să se declanşeze sub controlul calculatorului central în momente predeterminate pentru anumite categorii de lucrări. Controlorul de reţea va realiza şi va lua decizii pe linia ordinii de execuţie a acestora.

Comunicaţiile nu trebuie să aibă loc înainte de autentificare, componentă de bază a sistemului de securitate, apelându-se la parole, tabele de autentificare şi la celelalte tehnici de asigurare a securităţii.

O atenţie deosebită trebuie să se acorde sistemului de intrare în regim de comunicaţie cu calculatorul central şi cu terminalele, *prin remorcare* (*piggybacking*), intrusul dispunând de un

minicalculator cu care să efectueze o astfel de operaţiune ilegală, având acces la ceea ce şi-a propus să obţină.

*Tabelul de autentificare*. O formă a tabelului de autentificare este cea matriceală, de 26 x 26 elemente, completat cu caractere alfabetice generate aleator. Capetele de tabel şi de rânduri sunt litere ale alfabetului. Utilizatorul transmite de la un terminal o pereche de litere, iar calculatorul va căuta în propria-i memorie pentru a afla tabelul corespunzător şi a transmite caracterele aflate la intersecţia liniei cu coloana specificată de utilizator, realizându-se astfel autentificarea prin verificarea aceloraşi caractere dintr-un tabel similar al transmiţătorului.

*Mesajele test*. Comunicaţia efectivă nu trebuie să se declanşeze până când ambele capete ale liniei nu au transmis suficiente mesaje test, astfel încât controlerul să poată stabili că toate circuitele funcţionează corect. O secvenţă de mesaje test va include suficiente erori şi tentative de depăşire a sistemului de securitate pentru a verifica vigilenţa lui.

*Reautentificarea*. După ce comunicarea este înlesnită, reautentificarea punctelor terminale, a calculatorului central sau a ambelor se impune pentru a testa potenţialii „remorcaţi" ai dialogului. Operaţiunea va avea loc sistematic, la intervale aleatoare, imediat ce s-a înregistrat unul din cazurile următoare: tentativă de folosire de către un operator a unui cod-calculator interzis; încercarea de a adresa un operand interzis sau de depăşire a zonei autorizate de lucru; cererea de acces la programe şi date cu regim special; cererea de a se permite efectuarea unui serviciu special de la un echipament care nu are astfel de drepturi.

*Prevenirea intrării „printre linii"*. Pentru a preîntâmpina accesul neautorizat al unora în timp ce, pentru o scurtă perioadă de timp, adevăratul utilizator lipseşte de la terminal, se cere ca sistemul să testeze aceste prezenţe şi, în condiţii date, să se închidă singur.

*Securitatea comunicaţiei*. În caz de defecţiune, de cădere a sistemului din lipsă de alimentare cu energie sau de ocolire a mecanismului de securitate, traficul de linie trebuie să fie suspendat imediat.

*Înregistrarea comunicaţiilor şi asigurarea copiilor*. Rolul lor este de a facilita analizele de trafic şi de a permite reconstituirea datelor pierdute.

Alături de toate aceste mijloace şi metode, există şi altele cu un pronunţat caracter tehnic, cel mai important fiind sistemul verificării parităţii sau imparităţii codurilor transmise.

## 7.3 Securitatea radiaţiilor

Toate echipamentele care funcţionează pe bază de energie electrică, chiar şi maşinile de spălat, produc energie electrică, emisă prin semnale electromagnetice necontrolabile, transmisibile prin aer, ca undele radio, sau de-a lungul firelor şi metalelor conductibile, ca orice curent electric. Este în natura lucrurilor un astfel de fenomen şi nimic nu îl poate stopa. Astfel de radiaţii de la calculatoare sau de la cablurile de comunicaţii pot fi purtătoare de informaţii, ce pot fi extrase de către persoane din afară, după o analiză specială.

### 7.3.1 Cadrul general al radiaţiilor necontrolate

Protecţia echipamentelor de prelucrare automată a datelor utilizate pentru informaţiile speciale împotriva riscului generat de propriile lor radiaţii este una dintre cele mai dificile probleme puse în faţa agenţiilor specializate din orice parte a globului. Ele nu sunt de competenţa utilizatorilor finali şi nici a personalului din domeniul prelucrării automate a datelor, dar este foarte important să se cunoască efectele unui astfel de proces.

Oricine a pătruns într-o sală cu calculatoare mari, îndeosebi în centrele de prelucrare automată a datelor, unde se folosesc repetitiv cam aceleaşi programe, poate să-şi dea seama cu uşurinţă cam ce activităţi efectuează echipamentele, fără să fie nevoie să privească la consolă sau la operator. Urechea desluşeşte sunetele produse de diverse echipamente. Toate acestea sunt *radiaţii acustice*.

Echipamentele electronice şi cele electromagnetice au *radiaţii electrice*.

În general, complexitatea radiaţiilor echipamentelor depinde de felul lor şi de mediul în care se utilizează:

- echipamentele periferice, în special imprimantele şi aparatura video, emit semnale puternice, fără zgomote, ce pot fi „percepute" de la distanţă;
- semnalele produse de unitatea centrală de prelucrare sunt mai complexe şi mai greu de descifrat. De asemenea, zonele aglomerate cu multe echipamente video şi imprimante, cum sunt oficiile de calcul medii, produc semnale sesizabile mai greu, dar nu imposibil de descifrat, prin „citirea" numai a unora dintre ele, cele ce prezintă interes pentru atacatori;
- modul în care un echipament anume produce radiaţii depinde, în mare parte, de măsurile de protecţie încorporate în el în fazele de proiectare, fabricaţie, instalare şi utilizare;
- de regulă, radiaţiile de la un echipament de birou pot fi detectate de la o distanţă de până la 100 de metri, deşi sunt numeroase excepţii, după cum o să reiasă din prezentările ulterioare.

Pentru preîntâmpinarea sau diminuarea pericolelor radiaţiilor, s-au realizat echipamente speciale, despre care literatura de specialitate are următoarele păreri:

- există o prea mare preocupare pe linia promovării şi, firesc, a comercializării aparaturii de distrugere a radiaţiilor compromiţătoare, *TEMPEST* (*Transient ElectroMagnetic Pulse Emanation STandardizing*). Cu câţiva ani în urmă, un foarte popular program TV din Anglia a arătat cum este posibil ca dintr-un microbuz, dotat cu aparatură electronică specială, să se citească ceea ce se afişa pe un monitor dintr-un birou aflat în centrul Londrei, operaţiunea reuşind îndeosebi datorită utilizării calculatorului. De fapt, povestea este ceva mai veche, întrucât cu câţiva ani în urmă, un cercetător din Olanda a demonstrat că oricine dispune de un televizor, ce conţine mici modificări, ar putea citi ecranul unui calculator personal sau al unui terminal aflat la o distanţă de aproximativ ... 15 Km;
- dintre cei ce susţin aparatura *TEMPEST*, firesc, la loc de frunte se află producătorii ei;
- orice semnale interceptate sunt numai cele transmise în acel moment. Pentru detectarea datelor cu regim special, cum ar fi cazul parolelor, trebuie să fie urmărite toate radiaţiile, ceea ce presupune un mare consum de timp şi de resurse;
- pentru a obţine un semnal corect şi util, e nevoie ca răufăcătorii să se situeze la o distanţă optimă, care să le permită efectuarea cu succes a atacului. Ori, în cazul unui microbuz străin aflat foarte aproape de oficiul de calcul, practic în zona de securitate, oricine poate să-i sesizeze prezenţa şi să anunţe pe cei în drept pentru a lua măsurile necesare. Echipamentele cu gabarit redus sunt mai puţin eficiente, iar cele portabile au o utilitate foarte mică, întrucât purtătorul lor poate sesiza prin propriile organe de simţ ce îl interesează, fără să mai apeleze la astfel de echipamente;
- fenomenul captării radiaţiilor necontrolate nu este aşa de uşor de înfăptuit, cum se întâmplă cu metodele descrise anterior. El presupune cunoştinţe tehnice de înalt nivel, echipament scump, timp şi şansă, dar şi expunerea atacantului la un mare risc.

Totuşi, ar fi o mare greşeală să se desconsidere o astfel de tehnică de interceptare a informaţiilor. De regulă, calculatoarele situate în zone foarte aglomerate sunt şi cele mai vulnerabile la atac.

În cazul aplicaţiilor militare, în care se prelucrează multe date secrete, problema interceptării radiaţiilor trebuie pusă cu multă seriozitate, în toate fazele de realizare a sistemelor.

Oricum, aparatura anti-interceptare-radiaţii este mai mult o dorinţă a realizatorilor ei de a fi inclusă în echipamentele de prelucrare automată a datelor, dar numai în cazuri deosebite se recomandă utilizarea lor.

### 7.3.2 Măsuri elementare de precauţie împotriva captării radiaţiilor necontrolate

Există un număr substanţial de măsuri, relativ ieftine, de diminuare a pericolului răspândirii necontrolate a datelor prin radiaţii compromiţătoare. Dintre ele amintim:

1. *Zonele sterile*. Se recomandă crearea unor zone sterile în jurul echipamentelor de prelucrare automată a datelor, în special al monitoarelor şi imprimantelor, prin îndepărtarea tuturor corpurilor metalice din preajma lor. Nu se recomandă folosirea birourilor metalice, nici măcar cu picioare din metal şi nici coşuri de gunoi metalice.
2. *Telefoanele*. Monitoarele sunt veritabile surse de informaţii, iar, pentru bunul mers al operării, alături de ele se plasează telefonul, numai că în timp ce datele se afişează pe ecran, telefonul, chiar dacă este în repaos, poate să transmită datele oriunde în afara unităţii. De aceea, oricând este posibil, toate componentele telefonului, inclusiv cablurile, trebuie să fie ţinute la distanţă de echipamentele ce prelucrează date secrete.

   Dacă telefonul este, totuşi, necesar:
   - el trebuie amplasat la periferia zonei secrete, cu un filtru potrivit de distrugere a emanaţiilor compromiţătoare;
   - „securitatea în timpul nefolosirii" telefonului se realizează prin deconectarea aparatului de la linie.
3. *Curenţii filtranţi*. Radiaţiile compromiţătoare pot fi diminuate prin transmiterea în cablu a unor curenţi filtranţi.
4. *Accesul*. Un rol important va reveni controlării accesului în unitate al persoanelor sau al prezenţei vehiculelor în preajma centrului de prelucrare.
5. *Amplasarea echipamentelor în birouri*. Se va evita plasarea echipamentelor lângă ferestre, se vor poziţiona monitoarele cu ecranele spre interiorul camerei pentru prevenirea observării directe a ecranului din afara ei, deşi radiaţiile pot fi oricum compromiţătoare. Se recomandă plasarea tuturor componentelor fizice în centrul clădirii, pentru a beneficia de rolul protector al zidurilor şi al altor materiale cu rol asemănător. Atenţie mărită se va acorda locurilor în care se amplasează telefoanele.
6. *Echipamentele moderne*. Seturile actuale de echipamente electronice de calcul tind să dea mai puţine radiaţii în afară decât vechile modele. Preocupările au fost concentrate spre protejarea operatorilor de a nu mai fi „bombardaţi" cu radiaţii puternice, ceea ce a dus şi la diminuarea radiaţiilor compromiţătoare.
7. *Curăţirea ecranelor*. Scurgerile de date pot avea loc doar atunci când ele sunt afişate pe ecran sau în timpul procesului de imprimare. Personalul va fi instruit să şteargă ecranul după ce nu mai are nevoie de datele afişate şi, de asemenea, nu se recomandă listarea de probă de prea multe ori a documentelor ce conţin date secrete.
8. *Derutarea*. Datele importante pot fi protejate prin crearea unui val de scurgeri de informaţii nesemnificative, ceea ce se concretizează prin aglomerarea în jurul pieselor de bază ale centrului de prelucrare automată a datelor a unor echipamente care să prelucreze date lipsite de importanţă, dar care vor fi interceptate de inamicii sistemului. Mai mult chiar, li se va înlesni un acces foarte uşor la ele.

### 7.3.3 Echipamente de testare a existenţei radiaţiilor de date

Practica oferă echipamente speciale pentru testarea existenţei radiaţiilor compromiţătoare de date, dar decizia procurării lor este foarte îndrăzneaţă din cauza preţurilor foarte mari şi a dificultăţii procurării lor. Echipamentele veritabile funcţionează prin crearea unui mediu izolant din cupru în jurul întregii configuraţii de echipamente ale sistemului. Dacă instalarea şi exploatarea se desfăşoară conform proiectului, se poate pune problema anihilării radiaţiilor

compromiţătoare aproape în întregime. Sunt, totuşi, câteva aspecte de care trebuie să se ţină seama:

- nu sunt necesare echipamente protectoare pentru întregul sistem de prelucrare automată a datelor, ci numai pentru cele mai sensibile componente, cum ar fi cazul imprimantelor, monitoarelor, îndeosebi ale celor aflate la distanţă şi care nu au o protecţie fizică adecvată, mai ales când prelucrează date foarte importante;
- aparatura de protecţie trebuie tratată cu deosebită atenţie, fără să se intervină la structura sa fizică, deoarece defectarea ei poate fi foarte greu remediată;
- firmele care procură echipamente speciale protectoare nu au posibilitatea să-şi dea seama dacă ele funcţionează la cotele maxime, ci numai unităţile specializate pot da un astfel de verdict;
- calculatoarele mari sau întregul centru de calcul poate fi plasat într-un spaţiu de cupru protejat total – cuşca lui Faraday – , dar acesta costă foarte mult şi dă senzaţia unui mediu neplăcut de lucru.

## 7.4 Securitatea tehnică

Securitatea tehnică, ultimul domeniu din studiul securităţii comunicaţiilor, ar fi şi mai corect formulată sub titulatura „măsuri împotriva supravegherii tehnice". Oricum, ea tratează modul de apărare împotriva echipamentelor străine plasate deliberat în aparatura care ar trebui să fie protejată.

Supravegherea tehnică a devenit foarte studiată în ultimii ani, îndeosebi după ce s-au promulgat legi specifice în S.U.A. şi Canada. Ea se află în sfera de preocupare a agenţiilor naţionale de securitate, dar şi a unor grupări care se ocupă de diverse activităţi interzise de legile oricărui stat, ele urmărind, în mod indirect, fie să obţină anumite avantaje materiale, fie informaţionale.

Atacurile cu scop de supraveghere tehnică asupra centrelor de prelucrare automată a datelor nu au ca obiectiv primar aspectele tehnice ale activităţilor desfăşurate în aceste locuri, ci, mai de grabă, rolul lor în procesul decizional al firmei. Din această cauză, sălile în care se discută planurile de modificare a sistemelor informatice, birourile programatorilor, fiind martorele unor discuţii mult mai importante decât sălile de consiliu sau ale executivului, sunt mult mai interesante şi, deci, mai expuse pericolului de a fi supravegheate, în mod fraudulos.

Supravegherea tehnică a birourilor securităţii sistemului de prelucrare automată a datelor prezintă interes pentru a se afla anumite elemente de penetrare a sistemului, în primul rând parolele. De multe ori piese străine sunt plasate în echipamentele de prelucrare automată a datelor ale firmei.

### 7.4.1 Metode de apărare împotriva supravegherii tehnice

*Cercetarea fizică*. Cercetarea fizică este poate cea mai importantă din gama acţiunilor de curăţire a unei zone protejate. Se aplică adagiul clasic al investigării „*Caută ceva ce ar trebui să fie într-un loc dar nu este; caută ceva ce n-ar trebui să fie în acel loc dar este*". De regulă, echipa de cercetare intervine când probele sugerează că un aparat străin a fost instalat undeva. Se recomandă ca zonele deosebit de importante pe linia securităţii să fie inspectate periodic.

În prima fază a cercetării, echipa va trebui să aibă acces la planurile clădirii, din care să reiasă locurile de amplasare a grinzilor, conductelor de canalizare, ţevilor, uşilor, ferestrelor, conductorilor electrici ş.a. Se va continua cu stabilirea locurilor de amplasare a mobilierului, rafturilor, lămpilor, diverselor aparate, tablourilor, cablurilor mobile ş.a. Orice modificare a poziţiei acestora trebuie să fie anunţată din timp.

Se va continua cu fotografierea camerelor din diverse unghiuri. Examinarea fizică a zonei constă în repetarea activităţilor anterioare şi compararea lor. Vor fi urmărite îndeosebi locurile

ascunse: cărţile, dosul draperiilor, ramele tablourilor, birourile, stilourile, zona de dedesubt a meselor, scaunelor, deşi imaginaţia intruşilor poate fi mult mai bogată. La o ambasadă vestică dintr-o ţară a fostului bloc comunist s-au descoperit „corpuri străine" sub parchetul sălii.

*Cercetările electrice*. Partea electrică din acţiunea de cercetare se va concentra, în primul rând, asupra echipamentelor telefonice. Dacă nu există fotografii detaliate ale unor aparate identice, se vor efectua cu această ocazie, din mai multe poziţii. Piesele importante pot fi marcate pentru o recunoaştere ulterioară, iar bobina de inducţie va fi scoasă şi înlocuită conform discuţiilor de la „securitatea liniilor de comunicaţie".

Similar se va proceda cu întregul sistem de comunicaţie prin telefon, radio, televiziune, aparate de înregistrat ş.a. Se vor desface şi cerceta dozele electrice, de telefon, prizele şi comutatoarele electrice.

Există un aparat portabil, cunoscut sub numele de *detector de metale* sau *detector de arme electronice*. El arată ca un capsator, însă dispune de o lampă şi de un aparat de măsură. În structura lui se află un oscilator de frecvenţe radio şi o antenă pe bază de ferite. Lumina se aprinde dacă radiaţiile emise de detector întâlnesc chiar un ac sau un fir metalic, oricât de fin ar fi el.

Într-o primă fază, detectorul este folosit pentru confirmarea amplasării elementelor metalice care fac parte din configuraţia normală a sălii sau clădirii. Se efectuează câteva cercetări cu detectorul asupra pereţilor, podelei, tavanului şi se marchează punctele în care se aprinde lampa sau aparatul sesizează prezenţa corpurilor metalice. În pasul următor, se repetă cercetarea şi se marchează locurile unde lumina nu s-a aprins mai înainte.

Din arsenalul securităţii tehnice arma de apărare principală este *detectorul de „muzicuţe"*. El arată ca o perie de covoare, numai că în mijlocul palmei este o casetă mică în care este montat un galvanometru. Sursa de alimentare şi circuitele de control se află într-o geantă de umăr. Aparatul detectează prezenţa tuturor diodelor semiconductoare dintr-o cameră, bineînţeles şi a celor care fac parte din configuraţia normală a aparatelor întrebuinţate. Puterea lui trece de multe ori de limita fizică a zidurilor camerei.

*Detecţia radiaţiilor*. Detecţia radiaţiilor continuă seria căutărilor în locurile în care s-au constatat unele aspecte ciudate în urma cercetărilor fizice şi electrice. Echipamentele de transmisie în spaţiul liber sunt folosite de profesioniştii ascultărilor neautorizate şi pot fi activate sau dezactivate de la distanţă.

Detectorul de muzicuţe va sesiza pe cele ce nu sunt activate, iar detectorul de radiaţii va afla sursa de radiaţii.

O problemă importantă, în acest caz, se referă la *cunoaşterea modului în care pot fi activate microfoanele secrete sau emiţătoarele*.

Unele emiţătoare ale amatorilor acţionează doar atunci când sesizează un zgomot sau un ton deosebit emis de sursa supusă urmăririi, ele având nevoie de un detector de emisie pentru a funcţiona cu succes.

În acţiunea de cercetare, nu se recomandă provocarea activării microfoanelor secrete prin fluierături, astfel încât prezenţa lor să fie sesizată. Echipele însărcinate cu o astfel de misiune trebuie să lucreze în linişte, fără ca ascultătorii neautorizaţi să-şi dea seama că s-a făcut simţită prezenţa microfonului secret. Dimpotrivă, după localizarea microfonului intrus se pot întinde curse sau emite informaţii false.

Înregistrarea pe bandă a discuţiilor de afaceri poate fi declanşată tot prin elemente străine, care să stabilească momentul în care să înceapă să funcţioneze. În afara microfoanelor/emiţătoarelor străine introduse în aparatura din cameră sunt cunoscute şi activatoarele de înregistrări, aflate în preşurile de la uşi, în pernele fotoliilor sau în saltelele paturilor. În ultimul caz, reglajul este stabilit să declanşeze înregistrarea când în pat se constată greutatea medie a două persoane.

Instrumentul principal de detectare a radiaţiilor este *analizorul de spectru*, care este un radio receptor special, echipat cu capete de reglare în intervalul 8 kilohertzi - 3000 megahertzi.

Cu el se va cerceta camera în momente diferite, inclusiv în momentele de aglomeraţie maximă, cu comutatoarele aparatelor din cameră activate şi neactivate.

Există şi alte aparate pentru descoperirea microfoanelor/emiţătoarelor secrete, de regulă, create pentru liniştea utilizatorilor obişnuiţi, dar instituţiile şi locurile ce se ştiu urmărite cu orice preţ, nu apelează la ele, ci la altele mult mai performante, cum este cazul detectoarelor cu diode de cristal.

## 7.4.2 Tipuri de dispozitive intrus

*Mecanice*. Cel mai vechi dispozitiv mecanic intrus de captare acustică dintr-o cameră vecină l-a constituit paharul, plasat cu deschiderea sa pe zid, pe ţevi sau pe conducte, pe care se lipeşte urechea pentru a asculta discuţiile.

*Şarpele* este un tub gol în interior, plasat alături de ţevile instalaţiilor electrice care face legătura între camera ascultată şi locul de ascultare.

*Ţeapa* este o vergea lungă ce asigură cuplarea acustică între camera ascultată şi microfonul intrus. Literatura citează cazul ţepei de bambus la capătul căreia se află microfonul intrus, însă, datorită preluării a tot felul de sunete din clădire, care nu prezintă interes pentru ascultător, metoda nu prea mai este folosită.

*Urechea mărită* este o antenă parabolică folosită pentru captarea sunetelor; antena obişnuită de captare a sunetelor poate fi folosită şi la captarea electrică a emanaţiilor de date. În Vietnam grotele dealurilor erau folosite ca o ureche mărită.

*Puşca de vânătoare* este o variantă a antenei acustice, care foloseşte o serie de conuri concentrice de întărire reciprocă, montate de-a lungul unei vergele. Cea mai simplă formă constă în plasarea aparatelor de înregistrat în zonele de interes şi casetele se vor schimba de o persoană de serviciu, care este angajată la firmă, dar „cumpărată" de cei interesaţi. Altă formă se realizează prin purtarea aparatului de înregistrare de către vizitatori. De aceea, este nevoie să se facă un control riguros cu detectorul de „muzicuţă"

*Microfoane şi fire*. Cele mai obişnuite microfoane-intrus se plasează prin intermediul celor existente în mod normal (orice difuzor cu un amplificator în punctul final poate constitui un bun microfon). Microfoanele moderne sunt foarte mici. La unele ambasade s-au descoperit microfoane care arătau exact ca ţesătura covorului.

*Pioneza* este un cilindru de cauciuc cu capul având funcţia de microfon sau tranzistor de amplificare, de mici dimensiuni, plasat într-un suport special, care, la rândul său, este introdus în zid, într-un loc creat cu burghie mici. De cilindru se leagă firele aparatului de înregistrare.

*Tubul* are o lungime de aproximativ 10 cm şi un diametru de 3 mm, transparent, cu un minuscul microfon la un cap şi fire ce duc la un tranzistor de amplificare la celălalt. Tubul se introduce în orificiile create anterior în lemn sau plastic.

Sisteme speciale se folosesc pentru aparatele de înregistrat aflate în portbagajele maşinii. Microfoanele se plasează în interiorul portbagajului şi de la ele sunt fire mascate ce duc spre aparatul de înregistrat. Şoferul părăsea maşina în timpul discuţiilor, dar, fiind omul serviciilor secrete nu uita să-şi regleze sistemul de lucru.

*Emiţătoarele în spaţiul liber*. Emiţătoarele clandestine se vând la preţuri foarte mici, câteva zeci de dolari, şi sunt cunoscute sub numele de „doică electronică". Un emiţător foarte cunoscut, de dimensiunea unui timbru poştal, este cel numit „păianjenul Hong Kong".

De regulă, amatorii în „trasul cu urechea" folosesc emiţătoare de frecvenţă asemănătoare staţiilor radio sau TV. Rezultatul operaţiunii depinde şi de receptor, care, de regulă, nu poate fi plasat mai departe de câteva sute de metri.

Emiţătoarele funcţionează pe bază de baterii, deci misiunea lor încetează când bateriile se consumă, fiind nevoie de sprijinul oferit de „cineva" pentru a le înlocui. Emiţătoarele, de regulă, se amplasează în aparatura-gazdă, de unde îşi iau şi energia necesară.

Sunt preferate instalările de emiţătoare în locul aparaturii de înregistrare, întrucât atunci când persoana este prinsă nu se pot cunoaşte şi cele mai recente date captate. Emiţătorul funcţionează pe bază de cristale şi operează în frecvenţa de 30-50 megahertzi. Sunt şi excepţii de la regulă. Uneori numai aceste dispozitive asigură succesul sigur al intruşilor, celelalte fiind uşor detectabile.

*Intruşii echipamentelor*. În timp, cele mai multe tentative de implantare a dispozitivelor străine în echipamentele celor spionaţi s-au orientat spre dispozitivele de criptare. Într-un caz, dispozitivul de criptare s-a aflat în *bobina de inducţie* şi avea rolul de a stabili ce taste au fost apăsate pentru introducerea textului în clar de la tastatura maşinii de criptat.

În alt caz, după ce dispozitivul a fost luat pentru o „reparaţie" de o oră, s-a constat că avea instalat în el un emiţător radio. Acesta a fost introdus într-un condensator şi ocupa jumătate din volumul acestuia, cealaltă fiind folosită drept condensator propriu-zis.

Cum calculatoarele se folosesc din ce în ce mai mult ca dispozitive de criptare, ele vor constitui ţinta a cât mai multe acţiuni de implantare a dispozitivelor străine cu rol de spionaj.

Datele transmise de la diverse controllere spre unitatea centrală de prelucrare circulă paralel, ceea ce incumbă utilizarea a nouă (8 biţi + 1 de paritate) emiţătoare, făcându-le dificil de utilizat de către intruşi.

În afara elementelor descrise până acum mai sunt şi altele care au un pronunţat caracter tehnic, ele depăşind cadrul materialului de faţă.

## Rezumat

Pentru a demonstra vulnerabilitatea sistemelor de comunicaţie în faţa persoanelor rău-intenţionate, sunt prezentate posibilităţile de interceptare a comunicaţiilor şi alte vulnerabilităţi care apar în cazul telefoanelor standard, celularelor, telefoanelor portabile, poştei vocale, robotului telefonic, pagerelor, interfoanelor şi al baby monitors.

Transmisiile, radiaţiile şi supravegherea tehnică sunt analizate separat, în termenii vulnerabilităţilor şi măsurilor de asigurare a securităţii.

CAPITOLUL VIII

# Aspecte juridice privind protecţia şi securitatea sistemelor informaţionale[21]

Domeniul atât de sinuos al protecţiei şi securităţii informaţiilor, sistemelor informaţionale şi al tuturor componentelor specifice nu se limitează doar la politicile şi măsurile care pot fi stabilite la nivelul organizaţiilor, ci trebuie să abordeze şi problematica normelor juridice pentru a asigura, pe de o parte, legalitatea acestora, iar pe de altă parte, pentru a preîntâmpina sau elimina efectele eventualelor fraude ce ar putea fi comise în legătură cu informaţiile, prelucrarea şi transmiterea lor. Obiectivele capitolului sunt:

- cunoaşterea principalelor reglementări juridice privind protecţia şi securitatea informaţiilor existente în România;
- dobândirea de informaţii despre principalele aspecte ce caracterizează copyright-ul, mărcile înregistrare şi licenţele.

## 8.1 Legislaţia în România

La nivelul României, în ultimii ani, au început să apară din ce în ce mai multe reglementări legislative privind protecţia şi securitatea informaţiilor. Lucrurile s-au schimbat odată cu proliferarea şi pe teritoriul ţării a tehnologiilor informaţionale şi de comunicaţii, care au eliminat barierele de timp, spaţiu şi localizare a prelucrării, stocării şi transmiterii informaţiilor. Chiar dacă sunt încă multe lacune în această privinţă, se poate spune că este un început bun pentru trecerea României la societatea informaţională şi a cunoaşterii.

Printre cele mai importante legi care reglementează, direct sau indirect, protejarea informaţiilor, mecanismele de prelucrare, stocare şi transmitere, se pot enumera:

- Legea 51/1991 *privind siguranţa naţională a României*;
- Legea 182/2002 privind *protecţia informaţiilor clasificate*, însoţită de Hotărârea de Guvern 585/2002 pentru aprobarea *Standardelor naţionale de protecţie a informaţiilor clasificate în România*;
- Hotărârea de Guvern 781/2002 *privind protecţia informaţiilor secrete de serviciu*;
- Ordonanţa de Guvern 34/2002 privind *accesul la reţelele de telecomunicaţii electronice şi la infrastructura asociată, precum şi interconectarea acestora*;
- Legea 544/2001 *privind liberul acces la informaţia de interes public*;
- Legea 677/2001 *privind protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date*;
- Legea 682/2001 privind ratificarea *Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal*, adoptată la Strasbourg la 28 ianuarie 1981;
- Ordinul Avocatului Poporului 52/2002 privind *aprobarea cerinţelor minime de securitate a prelucrărilor de date cu caracter personal*;
- Ordinul Avocatului Poporului 75/2002 privind *stabilirea unor măsuri şi proceduri specifice* care să asigure un nivel satisfăcător *de protecţie a drepturilor persoanelor ale căror date cu caracter personal fac obiectul prelucrărilor*;

[21] Capitol realizat, în cea mai mare parte, de prof. dr. Gabriela Meşniţă de la Universitatea „Al. I. Cuza" Iaşi, Facultatea de Economie şi Administrarea Afacerilor şi revizuit pentru noua ediţie de lect. dr. Daniela Popescul

- Legea 506/2004 privind *prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice*;
- Legea 102/2005 privind *înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal*;
- Legea 161/2003 privind *unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei*, care conţine componenta de *prevenire şi combatere a criminalităţii informatice*, în Titlul III;
- Legea 64/2004 pentru *ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică*, adoptată la Budapesta la 23 noiembrie 2001;
- Ordonanţa 130/2000 privind *protecţia consumatorilor la încheierea şi executarea contractelor la distanţă*, aprobată cu modificări prin Legea 51/2003;
- Legea 365/2002 *privind comerţul electronic,* modificată şi completată prin Legea 121/2006;
- Legea 455/2001 *privind semnătura electronică*, împreună cu Norma tehnică şi metodologică din 13 decembrie 2001 pentru aplicarea ei;
- Legea 451/2004 *privind marca temporală*;
- Legea 589/2004 privind *regimul juridic al activităţii electronice notariale*, împreună cu Ordinul Ministrului Comunicaţiilor şi Tehnologiei Informaţiei pentru aprobarea normelor tehnice şi metodologice pentru aplicarea ei, nr. 221/2005;
- Hotărârea de Guvern 557/2006 *privind stabilirea datei de la care se pun în circulaţie paşapoartele electronice, precum şi a formei şi conţinutului acestora*;
- Ordinul Ministerului Finanţelor Publice 875/2001 pentru aprobarea *Regulamentului privind operaţiunile cu titluri de stat emise în formă dematerializată*;
- Ordonanţa de Guvern 24/2002 privind *încasarea prin mijloace electronice a impozitelor şi taxelor locale*;
- Ordinul Ministerului Comunicaţiilor şi Tehnologiei Informaţiei 218/2004 privind procedura de avizare a *instrumentelor de plată cu acces la distanţă, de tipul aplicaţiilor Internet-banking, home-banking sau mobile-banking*;
- Regulamentul Băncii Naţionale a României 6/octombrie 2006 privind *emiterea şi utilizarea instrumentelor de plată electronică şi relaţiile dintre participanţii la tranzacţiile cu aceste instrumente*;
- Legea 8/1996 privind dreptul de autor şi drepturile conexe, care conţine informaţii privind *drepturile autorilor programelor de calculator*;
- Ordonanţa de Urgenţă 123/2005 pentru modificarea şi completarea Legii 8/1996 *privind dreptul de autor şi drepturile conexe*, care aduce câteva precizări suplimentare privind *distribuirea pe Internet a bazelor de date şi a programelor de calculator*. Actele normative privind dreptul de autor sunt prezentate în paragraful 8.2.2.3.

**Legea 51/1991 privind siguranţa naţională a României**

Una dintre primele legi care face referire la securitatea informaţiilor pe teritoriul României a fost *Legea privind siguranţa naţională a României,* din 1991.

Printre principalele aspecte pe care le abordează sunt şi cele care se referă la organismele naţionale care au în atribuţii activitatea de informaţii privind realizarea siguranţei naţionale, şi anume:

- Serviciul Român de Informaţii, care este organul specializat în materie de informaţii din interiorul ţării;
- Serviciul de Informaţii Externe, care urmăreşte obţinerea informaţiilor din străinătate referitoare la siguranţa naţională;

- Serviciul de Protecţie şi Pază, organ specializat în asigurarea protecţiei demnitarilor români şi străini pe timpul prezenţei lor în România, precum şi în asigurarea pazei sediilor de lucru şi reşedinţelor acestora.

Legea stabileşte că *activităţile ce sunt legate de informaţii* necesare realizării siguranţei naţionale *au caracter secret,* stabilindu-se categoriile de persoane şi organisme cărora li se pot comunica aceste informaţii (preşedintele Senatului, al Camerei Deputaţilor, comisiile permanente pentru apărare publică, miniştrii şi şefii departamentelor ministeriale, prefecţii, primarul general al Capitalei, conducătorii consiliilor judeţene, organele de urmărire penală).

Divulgarea, prin orice mijloace, a datelor şi informaţiilor secrete care pot aduce prejudicii intereselor naţionale, indiferent de modul în care au fost obţinute, este interzisă şi se pedepseşte potrivit prevederilor legale.

Pentru obţinerea unor informaţii din această categorie este necesară autorizarea efectuării unor astfel de acţiuni de către procurorul general al României. În categoria actelor ce pot fi autorizate intră:

- interceptarea comunicaţiilor;
- căutarea unor informaţii, documente sau înscrisuri pentru obţinerea cărora este necesar accesul într-un loc, la un obiect sau deschiderea unui obiect;
- ridicarea şi repunerea la loc a unui obiect sau document, examinarea lui, extragerea informaţiilor pe care acesta le conţine, cât şi înregistrarea, copierea sau obţinerea de extrase prin orice procedee;
- instalarea de obiecte, întreţinerea şi ridicarea acestora din locurile în care au fost depuse.

Cererea de autorizare trebuie să fie formulată în scris şi să conţină următoarele informaţii:

- date sau indicii din care să rezulte existenţa unei ameninţări la adresa siguranţei naţionale, prevăzute în lege, pentru a cărei prevenire, descoperire sau contracarare este necesară emiterea mandatului;
- categoriile de activităţi pentru care trebuie emis mandatul;
- identitatea persoanei ale cărei comunicaţii trebuie interceptate, dacă este cunoscută, sau a persoanei care deţine informaţiile, documentele sau obiectele ce trebuie obţinute;
- descrierea generală, dacă şi când este posibil, a locului în care urmează a fi executate activităţile autorizate;
- durata de valabilitate a mandatului solicitat.

Dacă cererea de eliberare a mandatului a fost aprobată, acesta trebuie să conţină:

- aprobarea pentru categoriile de comunicaţii care pot fi interceptate, categoriile de informaţii, documente sau obiecte care pot fi obţinute;
- identitatea persoanei, dacă este cunoscută, ale cărei comunicaţii trebuie interceptate sau care se află în posesia datelor, informaţiilor, documentelor sau obiectelor ce trebuie obţinute;
- organul împuternicit cu executarea;
- descrierea generală a locului în care urmează a fi executat mandatul;
- durata de valabilitate a mandatului, care nu poate depăşi 6 luni.

În lege se specifică faptul că mijloacele de obţinere a informaţiilor necesare siguranţei naţionale nu trebuie să lezeze drepturile sau libertăţile cetăţenilor, viaţa particulară, onoarea sau reputaţia lor, ori să îi supună la îngrădiri ilegale. Iniţierea, organizarea sau constituirea pe teritoriul României a unor structuri informative care pot atinge siguranţa naţională, sprijinirea acestora sau aderarea la ele, deţinerea, confecţionarea sau folosirea ilegală de mijloace specifice de interceptare a comunicaţiilor, precum şi culegerea şi transmiterea de informaţii cu caracter secret ori confidenţial, prin orice mijloace, în afara cadrului legal, se pedepsesc potrivit prevederilor în vigoare.Informaţiile privind viaţa particulară, onoarea sau reputaţia persoanelor,

cunoscute incidental în cadrul obţinerii datelor necesare siguranţei naţionale, nu pot fi făcute publice.

Legea prevede că documentele organelor de informaţii şi ale celor cu atribuţii în domeniul siguranţei naţionale se păstrează în arhivele acestora şi nu pot fi consultate decât în condiţiile legii.

**Legea 182/2002 privind protecţia informaţiilor clasificate**

*Scopul* legii îl reprezintă protecţia informaţiilor clasificate şi a surselor confidenţiale ce asigură acest tip de informaţii. Protejarea lor se face prin instituirea sistemului naţional de protecţie a informaţiilor.

*Principalele obiective* ale protecţiei informaţiilor clasificate sunt:

- protejarea informaţiilor clasificate împotriva acţiunilor de spionaj, compromitere sau acces neautorizat, alterării sau modificării conţinutului acestora, precum şi împotriva sabotajelor ori distrugerilor neautorizate;
- realizarea securităţii sistemelor informatice şi de transmitere a informaţiilor clasificate.

Protecţia informaţiilor clasificate vizează:

- protecţia juridică;
- protecţia prin măsuri procedurale;
- protecţia fizică;
- protecţia personalului care are acces la informaţiile clasificate ori este desemnat să asigure securitatea acestora;
- protecţia surselor generatoare de informaţii.

În lege sunt abordate definiţiile principalilor termeni care operează în domeniul protejării informaţiilor clasificate, şi anume:

- *informaţii* – orice documente, date, obiecte sau activităţi, indiferent de suport, formă, mod de exprimare sau de punere în circulaţie;
- *informaţii clasificate* – informaţiile, datele, documentele de interes pentru securitatea naţională, care, datorită nivelurilor de importanţă şi consecinţelor care s-ar produce ca urmare a dezvăluirii sau diseminării neautorizate, trebuie să fie protejate;
- *clasele de secretizare* sunt secrete de stat şi secrete de serviciu;
- *informaţii secrete de stat* – informaţiile care privesc securitatea naţională, prin a căror divulgare se pot prejudicia siguranţa naţională şi apărarea ţării;
- *informaţii secrete de serviciu* – informaţiile a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat;
- *nivelurile de secretizare* se atribuie informaţiilor clasificate din clasa secrete de stat şi sunt:
  - *strict secret de importanţă deosebită* – informaţiile a căror divulgare neautorizată este de natură să producă daune de o gravitate excepţională securităţii naţionale;
  - *strict secrete* – informaţiile a căror divulgare neautorizată este de natură să producă daune grave securităţii naţionale;
  - *secrete* – informaţiile a căror divulgare neautorizată este de natură să producă daune securităţii naţionale;
- *protecţie juridică* – ansamblul normelor constituţionale şi al celorlalte dispoziţii legale în vigoare, care reglementează protejarea informaţiilor clasificate;
- *protecţie prin măsuri procedurale* – ansamblul reglementărilor prin care emitenţii şi deţinătorii de informaţii clasificate stabilesc măsurile interne de lucru şi de ordine interioară destinate realizării protecţiei informaţiilor;
- *protecţie fizică* – ansamblul activităţilor de pază, securitate şi apărare, prin măsuri şi dispozitive de control fizic şi prin mijloace tehnice, a informaţiilor clasificate;

- *protecţia personalului* – ansamblul verificărilor şi măsurilor destinate persoanelor cu atribuţii de serviciu în legătură cu informaţiile clasificate, pentru a preveni şi înlătura riscurile de securitate pentru protecţia informaţiilor clasificate;
- *certificate de securitate* – documentele care atestă verificarea şi acreditarea persoanei de a deţine, de a avea acces şi de a lucra cu informaţii clasificate.

În lege, la art. 17 este prezentată lista informaţiilor secrete de stat, iar în art. 19 cine sunt cei împuterniciţi să atribuie unul dintre nivelurile de secretizare a informaţiilor cu prilejul elaborării lor.

Legat de *informaţiile secrete de stat*, în lege sunt stipulate următoarele reglementări:

- *instituţiile deţinătoare de informaţii secrete de stat* poartă răspunderea *elaborării şi aplicării măsurilor procedurale de protecţie fizică şi protecţie* a personalului care are acces la informaţiile din această categorie;
- *documentele* cuprinzând informaţii secrete de stat *vor purta pe fiecare pagină nivelul de secretizare*, precum şi *menţiunea „personal”*, când sunt destinate unor persoane determinate;
- *autorităţile publice* care elaborează ori lucrează cu informaţii secrete vor întocmi *un ghid pe baza căruia se va realiza o clasificare corectă şi uniformă a informaţiilor secrete de stat*, în strictă conformitate cu legea;
- *persoanele autorizate* care copiază, extrag sau reproduc în rezumat conţinutul unor documente secrete vor aplica pe noul document rezultat menţiunile aflate pe documentul original;
- *declasificarea ori trecerea la un nivel inferior* de clasificare este realizată de *persoanele sau autorităţile publice competente* să aprobe clasificarea şi nivelul de secretizare a informaţiilor respective;
- protecţia informaţiilor nedestinate publicităţii transmise României de alte state sau de organizaţii internaţionale, precum şi accesul la informaţiile acestora *se realizează în condiţiile stabilite prin tratatele internaţionale sau înţelegerile la care România este parte*;
- *accesul la informaţii secrete de stat* este permis numai în baza unei autorizaţii scrise, eliberate de conducătorul persoanei juridice care deţine astfel de informaţii, după notificarea prealabilă la Oficiul Registrului Naţional al Informaţiilor Secrete de Stat.

În ceea ce privește *informaţiile secrete de serviciu*, legea prevede:

- informaţiile secrete de serviciu *se stabilesc de conducătorul persoanei juridice*, pe baza normelor prevăzute prin hotărâre a Guvernului;
- informaţiile secrete de serviciu *vor purta pe fiecare pagină* şi *menţiunea „personal”*, când sunt destinate strict unor persoane anume determinate;
- *dispoziţiile privind accesul* la informaţiile secrete de stat se aplică în mod corespunzător şi în domeniul informaţiilor secrete de serviciu;
- *neglijenţa în păstrarea informaţiilor secrete de serviciu* atrage, potrivit legii penale, răspunderea persoanelor vinovate;
- *se interzice clasificarea ca secrete de serviciu* a *informaţiilor* care, prin natura sau conţinutul lor, sunt *destinate să asigure informarea cetăţenilor asupra unor probleme de interes public sau personal*, pentru favorizarea ori acoperirea eludării legii sau obstrucţionarea justiţiei.

Legea stabileşte următoarele *obligaţii şi răspunderi* privind încălcarea prevederilor asupra informaţiilor secrete de stat:

- persoanele fizice cărora le-au fost încredinţate informaţii clasificate sunt obligate să asigure protecţia acestora, potrivit legii, şi să respecte prevederile programelor de prevenire a scurgerii de informaţii clasificate;

- obligaţiile persoanelor fizice se menţin şi după încetarea raporturilor de muncă, de serviciu sau profesionale, pe întreaga perioadă a menţinerii clasificării informaţiei;
- persoana care urmează să desfăşoare o activitate sau să fie încadrată într-un loc de muncă ce presupune accesul la informaţii clasificate va prezenta conducătorului unităţii un angajament scris de păstrare a secretului;
- autorităţile publice, precum şi celelalte persoane juridice care deţin sau cărora le-au fost încredinţate informaţii secrete de stat sau informaţii secrete de serviciu vor asigura fondurile necesare în vederea îndeplinirii obligaţiilor care le revin, precum şi luării măsurilor necesare privitoare la protecţia acestor informaţii;
- răspunderea privind protecţia informaţiilor clasificate revine conducătorului autorităţii sau instituţiei publice ori altei persoane juridice deţinătoare de informaţii, după caz;
- informaţiile secrete de stat se transmit, se transportă şi se stochează în condiţiile stabilite de lege;
- este interzisă transmiterea informaţiilor secrete de stat prin cablu sau eter, fără a se folosi mijloace specifice cifrului de stat sau alte elemente criptografice stabilite de autorităţile publice competente;
- încălcarea normelor privind protecţia informaţiilor clasificate atrage răspunderea disciplinară, contravenţională, civilă sau penală, după caz;
- persoanele încadrate în serviciile de informaţii şi siguranţă sau ale armatei, aflate în serviciul relaţiilor externe, precum şi cele special însărcinate cu protecţia informaţiilor secrete de stat, vinovate de deconspirări voluntare ori de acte de neglijenţă care au favorizat divulgarea ori scurgerea informaţiilor secrete, îşi pierd irevocabil calitatea.

Legea trebuie să fie aplicată având în vedere şi reglementările stabilite prin *Standardele naţionale de protecţie a informaţiilor clasificate*, aprobate prin *Hotărârea de Guvern 585/2002*. Standardele oferă garanţii de securitate pentru informaţiile naţionale clasificate şi pentru cele echivalente care fac obiectul acordurilor internaţionale la care România este parte.

**Hotărârea de Guvern 781/2002 privind protecţia informaţiilor secrete de serviciu**

Aplicarea Hotărârii se face pe baza *Standardele naţionale de protecţie a informaţiilor clasificate*, aprobate prin *Hotărârea de Guvern 585/2002.* Prin prevederile hotărârii, protecţia informaţiilor secrete de serviciu se aplică în ceea ce priveşte:

- clasificarea, declasificarea şi măsurile minime de protecţie;
- regulile generale de evidenţă, întocmire, păstrare, procesare, multiplicare, manipulare, transport, transmitere şi distrugere;
- obligaţiile şi răspunderile ce revin conducătorilor autorităţilor şi instituţiilor publice, agenţilor economici şi altor persoane juridice;
- accesul cetăţenilor străini, al cetăţenilor români care au şi cetăţenia altui stat, precum şi al persoanelor apatride la informaţii clasificate şi în locurile în care se desfăşoară activităţi, se expun obiecte sau se execută lucrări din această categorie;
- exercitarea controlului asupra măsurilor de protecţie

În Hotărâre sunt prezentate *regulile de marcare, utilizare* şi *accesare a informaţiilor secrete de serviciu*, după cum urmează:

- pentru identificarea documentelor cu caracter secret de serviciu numărul de înregistrare al acestora va fi precedat de litera S, iar pe fiecare pagină se va înscrie „secret de serviciu”;
- informaţiile secrete de serviciu constituite în dosare, precum şi cele legate în volume distincte se marchează pe copertă şi pe pagina de titlu;
- evidenţa documentelor secrete de serviciu se ţine separat de cea a documentelor secrete de stat şi nesecrete, în registrul special destinat acestui scop;

- se interzice scoaterea din incinta unităţii deţinătoare a informaţiilor secrete de serviciu fără aprobarea conducătorului acesteia;
- funcţiile care presupun accesul la informaţii secrete de serviciu se stabilesc de către conducătorii unităţilor deţinătoare;
- accesul personalului la informaţiile secrete de serviciu este permis numai în baza autorizaţiei scrise (pentru care este stabilit un model cadru de formulare), emisă de conducătorul unităţii;
- evidenţa autorizaţiilor de acces la informaţii secrete de serviciu se ţine centralizat de structura/funcţionarul de securitate în Registrul pentru evidenţa autorizaţiilor de acces la informaţii secrete de serviciu;
- sancţiunile contravenţionale prevăzute în Hotărârea Guvernului nr. 585/2002 se aplică şi în cazul nerespectării normelor ce privesc protecţia informaţiilor secrete de serviciu.

**Legea 544/2001 privind liberul acces la informaţia de interes public**

Potrivit legii, *informaţia de interes public* reprezintă orice informaţie care priveşte activităţile sau care rezultă din activităţile unei autorităţi publice sau instituţii publice, indiferent de suportul, forma sau modul de exprimare a acesteia. Accesul la informaţie se realizează cu ajutorul compartimentelor specializate sau de informare şi relaţii cu publicul sau prin persoanele desemnate cu atribuţii în acest domeniu.

Prin *autoritate sau instituţie publică* se înţelege orice autoritate sau instituţie publică, precum şi orice regie autonomă care utilizează resurse financiare publice şi care îşi desfăşoară activitatea pe teritoriul României, potrivit Constituţiei.

În conformitate cu prevederile legii, *sunt considerate informaţii publice*:

- actele normative privind organizarea şi funcţionarea autorităţilor sau instituţiilor publice;
- structura organizatorică, atribuţiile departamentelor, programul de funcţionare şi audienţe al instituţiilor;
- numele persoanelor din conducerea autorităţii sau instituţiei publice;
- coordonatele de contact;
- sursele financiare, bugetul şi bilanţul contabil;
- programele şi strategiile proprii;
- lista documentelor de interes public;
- lista categoriilor de documente obţinute şi/sau gestionate potrivit legii;
- modalităţile de contestare a deciziei autorităţii sau instituţiei publice, dacă persoana se consideră vătămată în privinţa dreptului de acces la informaţiile de interes public;
- informaţiile care favorizează sau ascund încălcarea legii de către o autoritate sau instituţie publică nu pot fi incluse în categoria informaţiilor clasificate şi se constituie în informaţii de interes public;
- informaţiile privind datele personale ale cetăţeanului dacă afectează capacitatea de exercitare a unei funcţii publice.

*Nu intră în categoria informaţiilor la care să aibă acces liber cetăţenii* următoarele:

- informaţiile din domeniul apărării naţionale, siguranţei şi ordinei publice, dacă fac parte din categoria informaţiilor clasificate;
- informaţiile privind deliberările autorităţilor sau cele care privesc interesele economice sau politice ale României, dacă fac parte din categoria informaţiilor clasificate;
- informaţiile privind activităţile comerciale sau financiare dacă publicitatea lor aduce atingere principiului concurenţei loiale;
- informaţiile cu privire la datele personale, potrivit legii;
- informaţiile privind procedurile din timpul anchetelor penale sau disciplinare, dacă se periclitează rezultatul anchetei;

- informaţiile privind procedurile judiciare, dacă aduce atingere asigurării unui proces echitabil ori interesului legitim al oricărei părţi implicate în proces;
- informaţiile a căror publicare prejudiciază măsurile de protecţie a tinerilor.

*Accesul la informaţiile publice* se realizează prin:

- afişare la sediul autorităţii sau al instituţiei publice;
- publicare în Monitorul Oficial al României;
- mijlocele de informare în masă;
- publicaţii proprii sau pe pagina de Internet a autorităţii sau instituţiei publice;
- consultare la sediul autorităţii sau instituţiei publice, în spaţii special amenajate.

**Legea 677/ 2001 privind protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date**

Legea are ca *scop* garantarea şi protejarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţa intimă, familială şi privată, cu privire la prelucrarea datelor cu caracter personal şi se aplică prelucrărilor de date cu caracter personal efectuate prin mijloace automate, precum şi prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă sau sunt destinate să fie incluse în astfel de sisteme.

Legea se aplică:

- prelucrărilor de date efectuate în cadrul activităţilor desfăşurate de operatori stabiliţi în România;
- prelucrărilor de date efectuate în cadrul activităţilor desfăşurate de misiunile diplomatice sau de oficiile consulare ale României;
- prelucrărilor de date efectuate în cadrul activităţilor desfăşurate de operatori care nu sunt stabiliţi în România, prin utilizarea de mijloace de orice natură situate pe teritoriul României, cu excepţia cazului în care aceste mijloace nu sunt utilizate decât în scopul tranzitării pe teritoriul României a datelor cu caracter personal care fac obiectul prelucrărilor respective.

*Datele cu caracter personal* pot fi *folosite cu acceptul persoanei* sau, în situaţii de excepţie, *fără acordul ei* cu respectarea următoarelor reguli:

- datele personale sunt prelucrate cu bună-credinţă şi în conformitate cu dispoziţiile legale;
- datele personale sunt colectate în scopuri determinate, explicite şi legitime;
- prelucrarea ulterioară a datelor personale se face în scopuri statistice, de cercetare istorică sau ştiinţifică, inclusiv a celor ce privesc efectuarea de notificări către autoritatea de supraveghere, precum şi cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute în normele ce reglementează activitatea statistică, cercetarea istorică sau ştiinţifică;
- datele sunt adecvate, pertinente şi neexcesive prin raportare la scopul pentru care sunt colectate şi prelucrate;
- datele sunt exacte, eventual actualizate. În situaţia datelor inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate, ele trebuie să fie şterse sau rectificate;
- datele sunt stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor pentru care sunt colectate;
- stocarea datelor pe o durată mai mare decât cea menţionată se face cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute în normele care reglementează aceste domenii.

*Legea interzice prelucrarea datelor cu caracter personal* legate de:

- originea rasială, etnică;

- convingerile politice, religioase, filosofice sau de natură similară;
- apartenenţa sindicală;
- starea de sănătate sau viaţa sexuală.

Sunt supuse unor *reguli speciale de prelucrare* o serie de date cu caracter personal care au o semnificaţie deosebită pentru persoanele la care fac referire, respectiv:

- prelucrarea datelor cu caracter personal având funcţie de identificare (cod numeric personal);
- prelucrarea datelor cu caracter personal privind starea de sănătate;
- prelucrarea datelor cu caracter personal referitoare la fapte penale sau contravenţii (cele care fac referire la săvârşirea de infracţiuni ori la condamnări penale, măsuri de siguranţă sau sancţiuni administrative ori contravenţionale aplicate persoanei vizate).

Persoana vizată de prelucrarea datelor cu caracter personal trebuie să-şi cunoască drepturile pe care le poate exercita, şi anume:

- *dreptul de a fi informată* cu privire la identitatea operatorului, scopul prelucrării datelor, destinatarii sau categoriile de destinatari ai datelor şi alte informaţii a căror furnizare este impusă prin dispoziţia autorităţii de supraveghere, ţinând cont de specificul prelucrării;
- *dreptul de acces la date*, prin care se poate solicita operatorului confirmarea faptului că datele care privesc persoana vizată sunt sau nu prelucrate de acesta. Operatorul este obligat să comunice persoanei, împreună cu confirmarea, informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele. De asemenea, legea stipulează obligativitatea comunicării într-o formă inteligibilă a datelor care fac obiectul prelucrării, precum şi a oricărei informaţii disponibile cu privire la originea datelor, a informaţiilor privind principiile de funcţionare a mecanismului prin care se efectuează prelucrarea automată a datelor ş.a.;
- *dreptul de intervenţie asupra datelor*, adică rectificarea, actualizarea, blocarea, ştergerea sau transformarea în date anonime a celor a căror prelucrare nu este conformă cu legea, în special a datelor incomplete sau inexacte;
- *dreptul de opoziţie*, prin care persoana vizată are dreptul de a se opune, din motive întemeiate şi legitime legate de situaţia sa particulară, ca datele care o vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care există dispoziţii legale contrare. De asemenea, persoana vizată are dreptul de a se opune, în mod gratuit şi fără nici o justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, în numele operatorului sau al unui terţ, sau să fie dezvăluite unor terţi într-un asemenea scop;
- *dreptul de a nu fi supus unei decizii individuale*, ceea ce presupune retragerea sau anularea oricărei decizii care produce efecte juridice în privinţa persoanei, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalităţii sale, cum ar fi competenţa profesională, credibilitatea, comportamentul sau alte asemenea aspecte. De asemenea, persoana poate solicita reevaluarea oricărei alte decizii luate în privinţa sa, care o afectează în mod semnificativ, dacă decizia a fost adoptată exclusiv pe baza unei prelucrări de date care întruneşte condiţiile enumerate anterior;
- *dreptul de a se adresa justiţiei*, prin care orice persoană care a suferit un prejudiciu în urma prelucrării unei date cu caracter personal, efectuată ilegal, se poate adresa instanţei competente.

Legea are prevederi exprese privind *confidenţialitatea* şi *securitatea prelucrărilor*. Astfel, orice persoană care acţionează sub autoritatea operatorului sau a persoanei împuternicite, inclusiv persoana împuternicită, care are acces la date cu caracter personal, nu poate să le

prelucreze decât pe baza instrucţiunilor operatorului, cu excepţia cazului în care acţionează în temeiul unei obligaţii legale.

De asemenea, operatorul este obligat să aplice măsurile tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală.

Pe lângă asigurarea confidenţialităţii şi securităţii prelucrărilor, legea stabileşte *condiţiile şi categoriile de date cu caracter personal care pot fi transferate peste graniţele ţării*.

**Legea 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei**

Legea face parte din pachetul legislativ anticorupţie aprobat de Guvern în anul 2003. Una din componentele importante pe linia securităţii sistemelor informaţionale o constituie cea cuprinsă în *Titlul III al legii* cu privire la *prevenirea şi combaterea criminalităţii informatice*, prin măsuri specifice de prevenire, descoperire şi sancţionare a infracţiunilor săvârşite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului şi protecţia datelor personale.

Potrivit legii, *autorităţile şi instituţiile publice cu competenţe în domeniu, în cooperare cu furnizorii de servicii, organizaţiile neguvernamentale şi alţi reprezentanţi ai societăţii civile* desfăşoară următoarele activităţi:

- promovează politici, practici, măsuri, proceduri şi standarde minime de securitate a sistemelor informatice;
- organizează campanii de informare privind criminalitatea informatică şi riscurile la care sunt expuşi utilizatorii sistemelor informatice.

De asemenea, *Ministerul Justiţiei, Ministerul de Interne, Ministerul Comunicaţiilor şi Tehnologiilor Informaţiei, Serviciul Român de Informaţii şi Serviciul de Informaţii Externe* au ca responsabilităţi:

- organizarea şi actualizarea continuă a bazei de date privind criminalitatea informatică;
- efectuarea de studii periodice în scopul identificării cauzelor care determină şi a condiţiilor ce favorizează criminalitatea informatică;
- desfăşurarea de programe speciale de pregătire şi perfecţionare a personalului cu atribuţii în prevenirea şi combaterea criminalităţii informatice.

În condiţiile legii, sunt considerate *infracţiuni împotriva confidenţialităţii şi integrităţii datelor şi sistemelor informatice* următoarele fapte:

- accesul, fără drept, la un sistem informatic;
- interceptarea neautorizată a unei transmisii de date care nu este publică şi care este destinată unui sistem informatic, provine dintr-un astfel de sistem sau se efectuează în cadrul unui astfel de sistem informatic;
- interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic ce conţine date care nu sunt publice;
- modificarea, ştergerea sau deteriorarea datelor sau restricţionarea accesului la aceste date, fără a avea autorizarea necesară;
- transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare;
- perturbarea gravă, fără autorizare, a funcţionării unui sistem informatic prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor sau prin restricţionarea accesului la aceste date;
- producerea, vinderea, importarea, distribuirea sau punerea la dispoziţie, sub orice altă formă, fără autorizare, a unui dispozitiv sau program informatic conceput sau adaptat în scopul săvârşirii de infracţiuni prezentate la punctele anterioare;

- producerea, vinderea, importarea, distribuirea sau punerea la dispoziţie, sub orice altă formă, în mod neautorizat, a unei parole, cod de acces sau alte asemenea date care permit accesul total sau parţial la un sistem informatic, cu scopul săvârşirii de infracţiuni prezentate la punctele anterioare;
- tentativa producerii uneia din infracţiunile anterioare.

În ceea ce priveşte *infracţiunile informatice*, legea face referire la următoarele fapte:

- introducerea, modificarea sau ştergerea fără autorizare a datelor ori restricţionarea accesului la aceste date, rezultând date necorespunzătoare adevărului, cu scopul producerii unei consecinţe juridice;
- cauzarea unui prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ştergerea de date, prin restricţionarea accesului la aceste date sau prin împiedicarea în orice mod a funcţionării unui sistem informatic cu scopul obţinerii unui beneficiu material pentru sine sau pentru altul;
- tentativa uneia din infracţiunile informatice precedente.

**Legea 455/2001 privind semnătura electronică**

Legea stabileşte regimul juridic al semnăturii electronice şi al înscrisurilor în formă electronică, precum şi condiţiile furnizării de servicii de certificare a semnăturilor electronice.

Într-o primă parte, legea oferă toate definiţiile necesare înţelegerii şi aplicării prevederilor legale privind:

- *datele în formă electronică* – reprezentări ale informaţiei într-o formă convenţională adecvată creării, prelucrării, trimiterii, primirii sau stocării acesteia prin mijloace electronice;
- *înscrisurile în formă electronică* – o colecţie de date în formă electronică între care există relaţii logice şi funcţionale şi care redau litere, cifre sau orice alte caractere cu semnificaţie inteligibilă, destinate a fi citite prin intermediul unui program informatic sau al altui procedeu similar;
- *semnătura electronică* – date în formă electronică, care sunt ataşate sau logic asociate cu alte date în formă electronică şi care servesc ca metodă de identificare;
- *semnatarul* – o persoană care deţine un dispozitiv de creare a semnăturii electronice şi care acţionează fie în nume propriu, fie ca reprezentant al unui terţ;
- *date de creare a semnăturii electronice* – orice date în formă electronică cu caracter de unicitate, cum ar fi coduri sau chei criptografice private, care sunt folosite de semnatar pentru crearea unei semnături electronice;
- *dispozitivele de creare a semnăturii* – software şi/sau hardware configurate pentru a implementa datele de creare a semnăturii electronice;
- *dispozitiv securizat de creare a semnăturii electronice* – dispozitiv de creare a semnăturii electronice;
- *date de verificare a semnăturii electronice* – date în formă electronică, cum ar fi coduri sau chei criptografice publice, care sunt utilizate în scopul verificării unei semnături electronice;
- *dispozitiv de verificare a semnăturii electronice* – software şi/sau hardware configurate pentru a implementa datele de verificare a semnăturii electronice;
- *certificat* – o colecţie de date în formă electronică ce atestă legătura dintre datele de verificare a semnăturii electronice şi o persoană, confirmând identitatea acelei persoane;
- *furnizorii de servicii de certificare* – orice persoană, română sau străină, care eliberează certificate sau care prestează alte servicii legate de semnătura electronică;
- *produsul asociat semnăturii electronice* – un produs hardware sau software utilizat de furnizorul de servicii pentru prestarea serviciilor legate de semnătura electronică sau pentru crearea/verificarea acesteia.

Potrivit art. 5 şi 6, înscrisul în formă electronică este asimilat, în ceea ce priveşte condiţiile şi efectele sale, cu înscrisul sub semnătură privată, având acelaşi efect ca actul autentic între cei care l-au subscris şi între cei care le reprezintă drepturile. De asemenea, conform art. 7, în situaţia în care forma scrisă este cerută ca o condiţie de probă sau de validitate a unui act juridic, un înscris în formă electronică îndeplineşte această cerinţă dacă i s-a încorporat, ataşat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat şi generată prin intermediul unui dispozitiv securizat de creare a semnăturii.

Legea stabileşte condiţiile de furnizare a serviciilor de certificare, obligaţia furnizorilor de a comunica autorităţii de reglementare şi supraveghere specializată în domeniu toate informaţiile referitoare la procedurile de securitate şi de certificare utilizate, precum şi orice intenţie de modificare a lor, cu precizarea datei şi orei la care modificarea intră în vigoare.

Furnizorul de servicii de certificare va asigura accesul la toate informaţiile necesare utilizării corecte şi în condiţii de siguranţă a serviciilor sale.

Persoanele fizice care prestează, conform legii, în nume propriu servicii de certificare, precum şi personalul angajat al furnizorului de servicii de certificare, persoană fizică sau juridică, sunt obligate să păstreze secretul informaţiilor încredinţate în cadrul activităţii lor profesionale, cu excepţia celor în legătură cu care titularul certificatului acceptă să fie publicate sau comunicate terţilor.

Autoritatea de reglementare şi supraveghere specializată în domeniu şi furnizorii de servicii de certificare au obligaţia să respecte dispoziţiile legale privitoare la prelucrarea datelor cu caracter personal.

Furnizorii de servicii de certificare au obligaţia de a crea şi de a menţine un registru electronic de evidenţă a certificatelor eliberate, care trebuie să fie disponibil permanent pentru consultare, inclusiv în regim on-line.

De asemenea, sunt stipulate:

- menţiunile pe care trebuie să le conţină certificatul la eliberare;
- condiţiile pe care trebuie să le îndeplinească furnizorii de servicii pentru eliberarea certificatelor;
- obligativitatea asigurării pentru acoperirea prejudiciilor pe care furnizorul le-ar putea cauza cu prilejul desfăşurării activităţilor legate de certificarea semnăturilor electronice;
- condiţiile în care poate fi suspendată şi încetează validitatea certificatelor eliberate;
- responsabilităţile autorităţii de reglementare şi supraveghere;
- omologarea dispozitivelor securizate de creare şi verificare a semnăturii electronice;
- modalitatea de recunoaştere a certificatelor eliberate de furnizorii de servicii de certificare străini;
- răspunderea furnizorilor de servicii;
- obligaţiile titularilor de certificate;
- contravenţiile şi sancţiunile.

**Legea 451/2004 privind marca temporală**

Prin legea sus-menţionată se stabilesc regimul juridic al mărcii temporale şi condiţiile de furnizare a serviciilor de marcare temporală.

În înţelesul legii, *marca temporală* este o *colecţie de date în formă electronică, ataşată în mod unic unui document electronic; ea certifică faptul că anumite date în formă electronică au fost prezentate la un moment de timp determinat furnizorului de servicii de marcare temporală.* Mai precis, ea este un set de tehnici care permite oricărei persoane să identifice în mod exact momentul emiterii şi semnării unui document electronic şi care asigură asupra faptului că nimeni, nici măcar autorul documentului, nu a intervenit cu modificări după marcarea temporală a acestuia.

Alţi termeni definiţi de lege sunt:

- *amprenta ataşată unui document electronic*, adică acea informaţie cu ajutorul căreia documentul poate fi identificat în mod unic, dar care nu permite deducerea conţinutului documentului respectiv;
- *certificatul asociat mărcii temporale*, adică informaţia cuprinsă în marca temporală prezentabilă în formă inteligibilă şi care conţine cel puţin numele furnizorului de servicii de marcare temporală, numărul de ordine din registrul furnizorului şi informaţia reprezentând momentul de timp;
- *baza de timp*, ca sistem unitar de referinţă temporală la care se raportează toţi furnizorii de servicii de marcare temporală.

Marca temporală este formată din cel puţin următoarele elemente:

- *amprenta* ataşată documentului electronic supus marcării;
- *data şi momentul de timp* aferente documentului supus marcării, exprimate în timp universal;
- *informaţii care identifică în mod unic furnizorul* de servicii de marcare temporală;
- *numărul de ordine din registrul furnizorului* de servicii de marcare temporală.

Informaţiile verificate la furnizorul de servicii de marcare temporală sunt:

- elementele de identificare ale certificatului relativ la cheia ce verifică marca;
- identificarea algoritmului utilizat pentru generarea amprentei.

Marca temporală poate să conţină şi elementele de identificare a solicitantului mărcii temporale.

Din punct de vedere tehnic, marcarea digitală este bazată pe semnături electronice şi funcţii hash. Cu ajutorul unei funcţii hash se obţine amprenta datelor originale, prin ataşarea unui şir de biţi individual fiecărui set de date în parte. Dacă datele sunt modificate, se modifică automat şi amprenta care le-a fost ataşată. Amprenta este trimisă furnizorului de servicii de marcare temporală, care îi ataşează o dată şi un moment din timp şi calculează o nouă funcţie hash. Rezultatul este criptat cu cheia privată a furnizorului de servicii şi trimis solicitantului mărcii temporale. Cum datele originale nu pot fi extrase din amprenta trimisă autorităţii de marcare, ca urmare a modului de lucru într-o singură direcţie a funcţiei hash, metoda asigură confidenţialitatea lor.

Marca temporală garantează asupra faptului că documentul nu a fost creat sau modificat după data şi ora cuprinse în amprenta digitală. Cel care doreşte să verifice aplică din nou funcţia hash datelor originale, ataşează rezultatului marca temporală primită de la furnizorul de servicii de marcare şi calculează un nou hash al şirului concatenat. Obţine astfel un prim hash (A). Apoi, este decriptată, cu cheia publică a furnizorului, marca temporală emisă de acesta. Rezultatul obţinut (hash B) trebuie să fie egal cu hash A, altfel înseamnă că în document au intervenit modificări după momentul furnizat de autoritate.

Potrivit legii, marca temporală trebuie generată de un sistem informatic sigur, care va îndeplini următoarele *cerinţe de securitate*:

- asigură că este imposibil să fie emisă o marcă corectă pentru un alt timp decât momentul când a fost primit documentul sau să se schimbe ordinea în care mărcile de timp sunt emise;
- asigură continuitatea furnizării serviciului.

Furnizorii de servicii de marcare temporală au obligaţia de a crea şi de a menţine un registru electronic operativ de evidenţă cuprinzând momentul de timp la care au fost emise mărcile temporale. Ei trebuie să dispună de instrumente financiare asiguratorii pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfăşurării activităţilor legate de marcarea temporală. Pe lângă acestea, furnizorii de servicii de marcare temporală mai au următoarele *obligaţii:*

- să menţină înregistrări ale mărcilor temporale emise pe o perioadă de 10 ani;

- să păstreze documentaţia aferentă algoritmilor şi procedurilor de generare a mărcilor temporale emise;
- să asigure posibilitatea obţinerii şi verificării on-line a mărcilor temporale (verificarea se face gratuit);
- să asigure accesarea permanentă a bazei de timp.

Furnizorul de servicii de marcare temporală răspunde pentru prejudiciul adus oricărei persoane care îşi întemeiază conduita pe efectele juridice ale respectivelor mărci temporale.

**Legea 589/2004 privind regimul juridic al activităţii electronice notariale**

Legea stabileşte *regimul juridic al actelor notariale în formă electronică*, venind în completarea legilor privind semnătura electronică şi marcarea temporală.

Potrivit articolului 2, actele notariale în formă electronică instrumentate de notarul public trebuie să îndeplinească, sub sancţiunea nulităţii absolute, următoarele *condiţii*:

- să fie efectuate în formă electronică;
- să fie semnate cu semnătura electronică extinsă a notarului public, bazată pe un certificat calificat, eliberat de un furnizor de servicii de certificare acreditat. Certificatele emise pentru notarii publici vor conţine informaţii privind biroul notarial, stabilite prin reglementări de către autoritatea de reglementare şi supraveghere specializată în domeniu;
- să îndeplinească toate condiţiile de fond prevăzute de lege privind operaţiunea juridică pe care o consemnează.

Actele notariale în formă electronică au acelaşi regim juridic ca şi actele notariale pe suport de hârtie. Valabilitatea în străinătate a actului notarial în formă electronică este stabilită prin convenţii internaţionale la care România este parte. Documentele în formă electronică provenind de la autorităţile sau notariatele altui stat pot fi luate în considerare de notarii publici în instrumentarea unui act notarial în formă electronică numai dacă semnăturile electronice străine sunt bazate pe un certificat calificat, eliberat de un furnizor de servicii de certificare acreditat.

Următoarele acte notariale pot fi îndeplinite în formă electronică:

- legalizarea copiilor electronice de pe documentele originale;
- darea de dată certă prin marcare temporală a documentelor ce îndeplinesc condiţiile prevăzute la articolul 2 şi atestarea locului unde s-au încheiat acestea;
- primirea şi păstrarea în arhiva electronică a documentelor ce îndeplinesc condiţiile prevăzute la articolul 2;
- legalizarea traducerilor în formă electronică;
- eliberarea de duplicate.

Pentru ca notarii publici să fie autorizaţi să efectueze acte notariale în formă electronică, ei trebuie să îndeplinească un set de condiţii, dintre care majoritatea se referă la necesitatea de a *garanta securitatea serviciilor oferite de ei*. Astfel, utilizarea unui sistem informatic omologat este obligatorie, ca şi emiterea de mărci temporale şi semnături electronice pentru documentele întocmite. Legea obligă şi la:

- angajarea, în cabinetul notarial, de personal cu cunoştinţe de specialitate în domeniul tehnologiei semnăturii electronice şi o practică suficientă în ceea ce priveşte procedurile de securitate corespunzătoare;
- adoptarea de măsuri de securitate împotriva falsificării actelor notariale în formă electronică;
- garantarea confidenţialităţii în cursul procesului de generare şi arhivare a acestora;
- păstrarea tuturor informaţiilor cu privire la un act notarial în formă electronică pe o perioadă stabilită în conformitate cu normele tehnice privind activitatea de păstrare a documentelor create şi primite de birourile notarilor publici, Camerele notarilor publici şi Uniunea Naţională a Notarilor Publici din România;
- utilizarea de sisteme omologate pentru arhivarea actelor notariale în formă electronică.

O autoritate de reglementare şi supraveghere specializată va urmări modul în care furnizorii de servicii electronice notariale respectă cerinţele de securitate stabilite prin lege.

În Ordinul ministrului privind normele tehnice şi metodologice de aplicare a legii activităţii electronice notariale, sunt precizate, în mod concret, condiţiile pe care trebuie să le îndeplinească notarul pentru a obţine autorizaţia privind activitatea electronică. Prezentăm, din întregul set de cerinţe, pe cele legate strict de sistemul informatic:

- asigurarea securităţii fizice;
- protecţia antivirus;
- asigurarea unui mecanism de autentificare a utilizatorilor;
- asigurarea confidenţialităţii şi integrităţii comunicaţiilor, a datelor recepţionate, transmise şi stocate,
- menţinerea unei arhive electronice locale;
- menţinerea unui registru automatizat de audit care va cuprinde evenimentele legate de utilizarea şi administrarea sistemului informatic - aceste informaţii vor fi păstrate pentru o perioada de cel puţin 10 ani şi în arhiva de siguranţă;
- accesul (eventual pe baze contractuale) la servicii calificate de arhivare electronică de siguranţă, unde va fi păstrată o copie a fiecărui act electronic notarial efectuat, o copie a registrului electronic al notarului, precum şi o copie a registrului de audit menţionat la punctul anterior.

**Hotărârea de Guvern 557/2006 privind stabilirea datei de la care se pun în circulaţie paşapoartele electronice, precum şi a formei şi conţinutului acestora**

Hotărârea de Guvern stabileşte ca dată de punere în circulaţie a paşapoartelor electronice *1 ianuarie 2007*. Paşaportul electronic este definit ca paşaportul diplomatic, paşaportul de serviciu sau paşaportul simplu, *în care se include un mediu de stocare electronică a datelor biometrice ale persoanei*. În înţelesul dat de Hotărâre, datele biometrice sunt *imaginea facială, impresiunea digitală, precum şi orice alte date ale persoanei care pot fi introduse în mediul de stocare electronică*.

Responsabilitatea alegerii, prin licitaţie publică, a unui furnizor care să asigure confecţionarea paşapoartelor electronice şi a întregii infrastructuri aferente este atribuită Regiei Autonome „Administraţia Patrimoniului Protocolului de Stat", în colaborare cu Ministerul Administraţiei şi Internelor şi cu Ministerul Afacerilor Externe.

În anexele la Hotărâre, sunt precizate forma şi conţinutul pentru paşaportul electronic diplomatic, paşaportul electronic de serviciu şi paşaportul electronic simplu. Acesta din urmă, de exemplu, pe lângă elementele fizice ale paşaportului „tradiţional", va conţine fotografia titularului engravată laser şi fotografia în umbră realizată prin perforaţie cu laser, ca şi datele informatizate citibile optic şi mediul de stocare electronică a datelor biometrice ale persoanei.

**Ordinul Ministerului Finanţelor Publice 875/2001**
**pentru aprobarea Regulamentului privind operaţiunile**
**cu titluri de stat emise în formă dematerializată**

Prin acest Ordin sunt specificate doar regulile specifice emisiunilor de titluri, fără să fie specificate obligaţiile de asigurare a securităţii şi protecţiei informaţiilor ce decurg din utilizarea mediilor electronice de emisiune şi decontare.

Singurele elemente la care se face trimitere în textul Ordinului şi care au legătura cu dematerializarea emisiunii de titluri de stat sunt cele referitoare la condiţiile minime pe care trebuie să le îndeplinească intermediarii pe piaţa primară sau secundară, respectiv:

- *dotări tehnice specifice activităţilor de tranzacţionare*: echipamente informatice, echipament de suport informaţional (Reuters, Telerate etc.), echipamente de comunicaţii specifice (linii telefonice, fax, telex, SWIFT etc.);

- *dotări tehnice specifice activităţii de custodie*: sisteme informatizate de evidenţă, gestiune şi control, sisteme de baze de date securizate, sisteme de stocare şi arhivare a informaţiilor.

**Ordinul Ministerului Comunicaţiilor şi Tehnologiei Informaţiei 218/ 2004 privind procedura de avizare a instrumentelor de plată cu acces la distanţă, de tipul aplicaţiilor Internet-banking, home-banking sau mobile-banking**

Ordinul se aplică *băncilor*, persoane juridice române, precum şi sucursalelor din România ale băncilor, persoane juridice străine, şi are ca obiect stabilirea procedurii privind eliberarea avizului Ministerului Comunicaţiilor şi Tehnologiei Informaţiei asupra instrumentelor de plată cu acces la distanţă tip Internet-banking, home-banking sau mobile-banking.

În primă fază, sunt prezentate *definiţiile* pe care le dă Ordinul principalilor termeni din domeniu:

- *instrument de plată cu acces la distanţă* - soluţie informatică ce permite deţinătorului să aibă acces la distanţă la fondurile aflate în contul său, în scopul obţinerii de informaţii privind situaţia conturilor şi operaţiunilor efectuate, efectuării de plăţi sau transferuri de fonduri către un beneficiar, prin intermediul unei aplicaţii informatice, al unei metode de autentificare şi al unui mediu de comunicaţie;
- *emitent* - banca autorizată de Banca Naţională a României să emită instrumente de plată electronică şi care pune la dispoziţie deţinătorului un instrument de plată electronică cu acces la distanţă, pe baza unui contract încheiat cu acesta;
- *deţinător* - persoana fizică sau juridică care, în baza contractului încheiat cu emitentul, deţine un mecanism de autentificare în utilizarea instrumentului de plată cu acces la distanţă;
- *utilizator* - deţinătorul instrumentului de plată cu acces la distanţă sau o persoană fizică recunoscută şi acceptată de către deţinător ca având acces la drepturile sale conferite de către emitent;
- *instrument de plată la distanţă tip Internet-banking* - acel instrument de plată cu acces la distanţă care se bazează pe tehnologia Internet (world wide web) şi pe sistemele informatice ale emitentului;
- *instrument de plată la distanţă tip home-banking* - acel instrument de plată cu acces la distanţă care se bazează pe o aplicaţie software a emitentului instalată la sediul deţinătorului, pe o staţie de lucru individuală sau în reţea;
- *instrument de plată la distanţă tip mobile-banking* - acel instrument de plată cu acces la distanţă care presupune utilizarea unui echipament mobil (telefon, PDA - Personal Digital Assistant etc.) şi a unor servicii oferite de către operatorii de telecomunicaţii;
- *plan de securitate* - document ce descrie totalitatea măsurilor tehnice şi administrative care sunt luate de către emitent pentru utilizarea în condiţii de siguranţă a instrumentului de plată cu acces la distanţă.

În articolul 3, se precizează că vor fi avizate pentru oferirea de instrumente de plată cu acces la distanţă băncile al căror sistem informatic îndeplineşte unele *cerinţe minime de securitate*, referitoare la:

- confidenţialitatea şi integritatea comunicaţiilor;
- confidenţialitatea şi nonrepudierea tranzacţiilor;
- confidenţialitatea şi integritatea datelor;
- autenticitatea părţilor care participă la tranzacţii;
- protecţia datelor cu caracter personal;
- păstrarea secretului bancar;
- trasabilitatea tranzacţiilor;
- continuitatea serviciilor oferite clienţilor;
- împiedicarea, detectarea şi monitorizarea accesului neautorizat în sistem;

- restaurarea informaţiilor gestionate de sistem în cazul unor calamităţi naturale, evenimente imprevizibile;
- gestionarea şi administrarea sistemului informatic;
- orice alte activităţi sau măsuri tehnice întreprinse pentru exploatarea în siguranţă a sistemului.

Articolul 4 stipulează că măsurile tehnice şi organizatorice întreprinse pentru îndeplinirea cerinţelor enumerate la articolul 3 vor fi în concordanţă cu progresul tehnologic şi cu riscurile potenţiale.

Pe lângă alte documente necesare, pentru obţinerea avizului, banca va trebui să prezinte:

- planul de securitate al sistemului informatic, semnat de către emitent, cuprinzând totalitatea măsurilor tehnice şi organizatorice prevăzute pentru asigurarea cerinţelor cuprinse la articolul 3 – structura planului este descrisă ulterior în Ordin;
- certificări din punct de vedere al securităţii asupra soluţiei informatice sau produselor conţinute în aceasta, emise de organizaţii naţionale sau internaţionale recunoscute, acolo unde există;
- opinia de audit asupra planului de securitate şi a soluţiei informatice prin intermediul căreia este oferit instrumentul de plată cu acces la distanţă;
- o declaraţie în care este exprimată independenţa auditorului faţă de sistemul informatic auditat.

**Regulamentul Băncii Naţionale a României 6/2006 privind emiterea şi utilizarea instrumentelor de plată electronică şi relaţiile dintre participanţii la tranzacţiile cu aceste instrumente**

Regulamentul are ca *obiect* stabilirea principiilor privind emiterea şi utilizarea instrumentelor de plată electronică pe teritoriul României, monitorizarea activităţii cu aceste instrumente, şi a condiţiilor care trebuie îndeplinite de bănci şi de alţi participanţi la desfăşurarea activităţii de plăţi cu instrumente de plată electronică, indiferent de moneda în care sunt emise/denominate acestea.

După prezentarea principalilor termeni utilizaţi în decontările cu ajutorul instrumentelor electronice, a caracteristicilor generale ale cardurilor, condiţiilor de desfăşurare a tranzacţiilor, sunt prezentate toate drepturile, obligaţiile şi responsabilităţile emitentului instrumentului de plată şi a băncilor acceptate, precum şi ale deţinătorului. Dintre acestea au fost selectate cele considerate importante pe linia protecţiei şi securităţii tranzacţiilor şi informaţiilor implicate, după cum urmează:

- *emitentul* va *asigura* şi va *răspunde* pentru *elemente de siguranţă* şi *de personalizare ale instrumentului de plată electronică*, accesibile sau nu simţurilor ori cunoaşterii comune, care *să prevină falsificarea sau alterarea informaţiei necesare şi suficiente în efectuarea de plăţi prin intermediul instrumentului de plată electronică*, precum şi *limitarea efectelor cauzate de pierderea, furtul şi distrugerea acestora*, în scopul evitării producerii unor prejudicii şi afectării încrederii în sistemele de plăţi care operează cu instrumente de plată electronică;
- *emitentul* este *responsabil pentru confecţionarea materială a cardului* şi pentru *informaţia necesară şi suficientă pe care acesta trebuie să o conţină*;
- emitenţii şi instituţiile acceptante au obligaţia *să asigure liniile şi echipamentele de comunicaţii şi procesare*, dispozitivele prin intermediul cărora se iniţiază, se înregistrează, se controlează şi se transmit informaţii şi date aferente tranzacţiilor iniţiate, precum şi terminalele şi locaţiile unde acestea sunt amplasate, astfel încât acestea să prezinte *un grad adecvat de siguranţă operaţională, în vederea prevenirii accesului neautorizat la acestea şi protejării confidenţialităţii, autenticităţii şi integrităţii informaţiilor şi datelor în timpul procesării, stocării şi arhivării datelor*, inclusiv asigurarea unei utilizări facile a terminalelor;

- *amplasarea terminalelor* trebuie să se facă în locuri care să asigure *siguranţa* deţinătorilor/utilizatorilor cardului sau ai instrumentului de plată de tip monedă electronică, *confidenţialitatea* operaţiunilor efectuate la acestea şi *accesul tuturor deţinătorilor/utilizatorilor*;
- *informaţiile şi datele transmise* băncii acceptante şi, respectiv, emitentului în momentul plăţii *nu trebuie să prejudicieze* sub nici o formă *confidenţialitatea operaţiunii*;
- *informaţiile* trebuie să se *limiteze strict* la cele *conţinute*, de regulă, de *instrumentele de plată fără numerar pe suport hârtie*, respectiv cecurile şi ordinele de plată;
- dacă *emitentul solicită autorizarea pentru un instrument de plată cu acces la distanţă*, de tipul aplicaţiilor *Internet-banking* sau *home-banking*, cererea va fi însoţită de toate avizele/certificările primite de la producătorul programului informatic aflat la baza aplicaţiei, privind *nivelul de securitate al transmisiilor de date* şi *protocolul de răspuns utilizat* în cazul apariţiei unor disfuncţionalităţi în cadrul sistemului, precum şi de avizul Ministerului Comunicaţiilor şi Tehnologiei Informaţiei sau al altor entităţi indicate de acesta;
- prin organizarea activităţii lor de informare *emitentul* şi *banca acceptantă răspund* de *identificarea, evaluarea* şi *limitarea* producerii *efectelor fraudelor* şi activităţilor cu *potenţial de risc*;
- *emitentul* va face dovada că *informaţiile* şi *datele* obţinute pe parcursul desfăşurării *tranzacţiilor cu carduri nu sunt utilizate, schimbate, transmise* sau *vândute* decât în conformitate cu contractul încheiat între emitent şi deţinător sau comerciantul acceptant, pentru raportările către Banca Naţională a României şi către Oficiul Naţional de Prevenire şi Combatere a Spălării Banilor sau în alte scopuri, conform legislaţiei în vigoare.

Potrivit Regulamentului, este considerată *activitate frauduloasă* una din următoarele situaţii:

- utilizarea unui card pierdut;
- furtul cardului;
- emiterea şi nerecepţionarea cardului de către deţinător;
- completarea unei cereri de eliberare a cardului în mod eronat sau fraudulos;
- utilizarea în cadrul tranzacţiilor a unui card contrafăcut;
- folosirea frauduloasă a cardului de către o persoană neautorizată;
- folosirea frauduloasă a numărului de cont al cardului în cadrul unei tranzacţii;
- o altă fraudă identificată de banca acceptantă şi efectuată la comerciantul acceptant.

Imaginaţi un caz de încălcare al unei legi dintre cele de mai sus. Imaginaţi un proces pe marginea respectivului caz, prezentând succint argumentele apărării şi acuzării.

## 8.2 Protecţia prin patente, copyright şi mărci înregistrate

Alături de legislaţia ce se referă efectiv la protejarea datelor şi informaţiilor din sistemele de prelucrare automată a datelor, se va urmări şi cadrul legal prin care sunt asigurate drepturile pentru protecţia intelectuală.

Astfel, în majoritatea ţărilor, legile privind protejarea proprietăţii intelectuale (patentele, copyright-ul şi mărcile înregistrate), împreună cu legile privind secretul comercial, legea contractelor, sunt aplicate pentru a asigura şi protecţia software-ului, în general.

Patentele au rolul de a proteja conceptele industriale încorporate la realizarea soft-ului, în timp ce copyright-ul urmăreşte protejarea codului sursă sau a codului obiect care stă la baza produselor obţinute. Marca de înregistrare pentru produsele informatice protejează „numele" sub care este realizat produsul, iar înregistrarea mărcii va preveni utilizarea însemnului de către alţi producători pentru bunuri sau servicii similare.

S-a constatat că, în ultima perioadă, costul unui sistem este format, în proporţie de aproape 2/3, din preţul mediu de achiziţionare şi instalare a soft-ului. Situaţia a fost mult amplificată de invadarea pieţei calculatoarelor de către microcalculatoarele personale. Una din cele mai importante probleme ale pătrunderii soft-ului pe piaţă o constituie faptul că programele trebuie să fie accesibile cumpărătorilor diferitelor tipuri de echipamente şi cărora trebuie să li se asigure o întreţinere corespunzătoare. Din această cauză, dificultatea producătorului de soft, care realizează produse în serie mare şi care sunt lansate pe diferite pieţe, este imposibilitatea prevenirii copierii programelor livrate de către diferite persoane neautorizate. Acest lucru determină o frustrare a producătorului de la drepturile sale de vânzare. Este cunoscut faptul că aproape 25% dintre cele mai utilizate produse de pe piaţa soft-ului nu aduc nici un venit celor care le-au realizat.

Educarea publicului este necesară pentru a arăta că dacă copierea produselor soft devine un fenomen de masă, rezultatul va fi o scădere drastică a resurselor obţinute de firme din vânzarea acestora, cu efecte vizibile asupra capacităţii de finanţare a activităţilor de cercetare şi de investiţii. De asemenea, publicul trebuie să ştie faptul că preţul unui program informatic nu este reprezentat de costul suportului pe care este memorat acesta (disc, bandă, CD, DVD etc.).

### 8.2.1 Patentele la nivelul Oficiului European de Patente (EPO – European Patent Office)

Reglementările stabilite la nivelul EPO au intrat în vigoare pe 6 martie 1985. În timpul discuţiilor, s-a stabilit că pentru industria informatică, care se confruntă cu dificultăţi practice în includerea programelor informatice în categoria invenţiilor, nu se justifică o abordare restrictivă a subiectelor ce pot fi puse sub jurisdicţia patentelor.

Reglementările clarifică problemele legate de înscrierea sau nu cu drept de patent a combinaţiei calculator-programe. Astfel, un program informatic sau o înregistrare efectuată pe un suport nu sunt brevetabile prin conţinutul lor. Pe de altă parte, dacă subiectul revendicat aduce contribuţii noi, el nu poate fi exclus din categoria celor supuse patentului. De exemplu, noile programe de control al echipamentelor, al producţiei sau al proceselor ar putea fi privite ca potenţiale subiecte de patente. Dacă subiectul revendicat se referă numai la mediul intern de lucru al unui calculator el poate fi supus legii patentelor numai dacă oferă o serie de elemente tehnice noi.

Pentru stabilirea dreptului de patent subiectul trebuie supus unor teste de determinare a gradului de noutate pe care îl aduce, respectiv să se urmărească modul de încadrare în prevederile legii.

Una dintre recomandările EPO nu se referă la programele informatice în sine, ci la invenţiile care pot lua forma unui program specific unui calculator. Potrivit acestora, furnizarea şi încărcarea unor programe pentru care nu s-a obţinut dreptul de folosire şi care au dreptul de protecţie prin patent reprezintă o încălcare a legii.

Recomandările EPO specifică următoarele elemente: programele informatice care, atunci când au fost încărcate într-un sistem, au determinat ca acel sistem să capete noi funcţii sau să îi fie reînnoite cele existente pot fi protejate prin patent. Distribuirea soft-ului ca atare, pe o dischetă, pe memoria ROM etc. poate fi supusă controlului sub termenii încălcării legii patentelor dacă nu au fost respectate prevederile legale de distribuire a produselor brevetate. Este foarte probabil ca noile produse informatice, deşi probează un anumit grad de noutate, să nu facă faţă testelor de probare a conţinutului lor, atât timp cât pentru realizarea lor s-au folosit

algoritmi şi subrutine deja cunoscute, fiind doar adaptări inventive la produsele existente. Din acest punct de vedere, s-ar putea considera că, de exemplu, doar primele procesoare de texte şi primele programe de calcul tabelar au dreptul de a obţine patentul.

Dintr-un anumit punct de vedere se consideră că patentele pentru invenţii ce se bazează pe programe informatice sunt mai puţin valoroase decât în cazul altor produse. În cazul microprocesoarelor, acest lucru este în mod evident neadevărat, dacă invenţia se concretizează într-un microprocesor care poate să facă faţă tuturor testelor ce se aplică unei invenţii oarecare.

În cazul programelor este necesară dezvăluirea mai multor informaţii cu privire la scopul care este urmărit prin ele. Pentru aceasta trebuie să se facă cunoscut codul-sursă, care în mod normal nu este vizibil publicului, căruia îi este suficient doar codul-obiect pentru a putea utiliza programul.

S-a pus şi problema dificultăţii descoperirii încălcărilor legii privind programele informatice faţă de alte domenii de activitate, în care procesul realizării invenţiilor poate fi supus unui control riguros prin intermediul patentelor (procesele chimice, domeniul telecomunicaţiilor, alte domenii tehnologice complexe).

O modalitate mai sigură de protejare a programelor este cea realizată prin copyright, încălcat numai de persoanele care au folosit, fără a avea dreptul, un program protejat prin copyright. Spre deosebire de această situaţie, un patent poate fi încălcat de către o persoană care concepe, la o perioadă de timp mai îndelungată, o invenţie asemănătoare sau foloseşte idei şi/sau elemente ale invenţiei originale, revendicându-şi un drept de brevet pentru lucrarea sa.

De asemenea, programele mai pot fi protejate prin asigurarea distribuirii numai a codului-obiect şi păstrarea secretului comercial de către distribuitori.

La respingerea includerii programelor informatice în categoria subiectelor de patente, s-a adus ca argument şi perioada mare de timp care se scurge între momentul formulării cererii şi cel al obţinerii patentului, dacă se ţine seama de rapiditatea schimbărilor din acest domeniu. Critica nu a fost lansată sistemului de patente, ci modului de derulare a procedurilor de obţinere a acestora.

### 8.2.2 Copyright-ul

Copyright-ul îşi are originea în Anglia, încă din 1709, dar statutul său a fost definit prin Legea Copyright-ului din 1911. Legea în vigoare este însă cea adoptată în 1956. Prin publicarea, în aprilie 1986, a unei recomandări numite „Proprietatea intelectuală şi invenţia", guvernul britanic a propus câteva amendamente acestei legi.

Copyright-ul, ca nume, sugerează un drept de copiere, dar în mod normal el este înţeles ca fiind un drept de a împiedica copierea muncii altora, care este subiect al copyright-ului. În Marea Britanie, copyright-ul implică o anumită formalitate şi înregistrarea unor date pentru obţinerea sa, acordându-se automat persoanelor calificate pentru ceea ce ele au creat prin munca lor. O persoană calificată se consideră a fi o persoană britanică sau protejată prin legile în vigoare, o corporaţie înregistrată care îşi desfăşoară activitatea pe teritoriul britanic şi pe baza legilor engleze. Publicarea lucrării ce se constituie subiect de copyright nu este esenţială pentru obţinerea acestuia. Data publicării va afecta, totuşi, termenul de copyright, care, în mod normal, este de 50 de ani de la sfârşitul anului calendaristic în care autorul moare, în cazul publicării post-mortem, sau 50 de ani de la publicarea pentru prima dată a lucrării. Termenul copyright-ului diferă faţă de cel al patentelor, care se acordă pentru o perioadă de 20 de ani, sau de perioada nedeterminată a secretului comercial sau al confidenţialităţii datelor, care, în cele mai multe cazuri, se stinge când subiectul ce a stat la baza confidenţialităţii a fost făcut public.

Copyright-ul se aplică lucrărilor originale din domeniul literar, dramaturgiei, artei plastice. Drepturi speciale se acordă filmelor cinematografice, înregistrărilor audio şi reclamelor. De asemenea, lucrările din industria informatică sunt asimilate lucrărilor literare şi artistice. Astfel de lucrări sunt subiecte de copyright numai dacă îşi dovedesc originalitatea. Totuşi, gradul de

originalitate cerut este nesemnificativ şi este legat mai mult de creaţie decât de conceptul de noutate, cum este în cazul patentelor.

Protecţia în cazul copyright-ului este acordată pentru conţinutul formal sau expresia lucrării şi nu pentru ideile pe care se bazează. Acest lucru este în contrast cu Legea Patentelor, în care protecţia este acordată pentru conţinutul de fond al invenţiei şi nu pentru conţinutul formal.

**8.2.2.1 Copyright-ul şi software-ul**

La nivelul majorităţii ţărilor dezvoltate s-au constituit organizaţii şi instituţii speciale care se ocupă de respectarea legislaţiei privind copyright-ul. De exemplu, în Anglia de aplicarea prevederilor legale privind copyright-ul se ocupă Federaţia Împotriva Furtului de Soft (FAST – *Federation Against Software Theft*).

Cele mai cunoscute reguli privind copyright-ul sunt:

- numai proprietarul copyright-ului sau celui căruia i s-a derogat acest drept poate apela la justiţie în cazul în care se dovedeşte încălcarea lui. De aceea, este deosebit de important ca proprietarii soft-ului să se asigure că şi-au înregistrat produsele lor sub copyright;
- când soft-ul este realizat de către salariaţi ai firmei, care sunt şi acţionarii săi, ei pot obţine, în mod automat, dreptul de copyright. Această regulă nu poate fi aplicată şi simplilor salariaţi sau programatorilor angajaţi temporar;
- documentaţia originală, obţinută în timpul realizării programului, trebuie să fie datată pentru a putea demonstra perioada în care a fost elaborat programul şi pentru a proteja materialele literare legate de produs. Copyright-ul poate fi obţinut chiar şi pe baza acestei documentaţii, care poate să asigure posibilitatea de stabilire a unui drept de copyright firmei producătoare, cât şi posibilitatea de a scoate în evidenţă faptul că produsul a fost realizat fără a încălca dreptul de copyright al altor produse;
- aducerea la cunoştinţa distribuitorilor şi utilizatorilor programului că este un produs aflat în proprietatea cuiva. Acest lucru se poate realiza prin includerea unui marcaj nu numai pe documentaţie şi manuale, ci chiar în program. Una din cele mai folosite notaţii este formată din simbolul © însoţit de numele proprietarului şi anul primei publicări, în concordanţă cu cerinţele Convenţiei Universale a Copyright-ului (UCC - *Universal Copyright Convention*). Deoarece mai sunt sisteme de prelucrare automată a datelor care nu dispun de acest simbol se poate utiliza şi notaţia **(C)**, sau poate fi scris efectiv cuvântul **Copyright**;
- detectarea şi identificarea încălcărilor copyright-ului sunt destul de dificile, mai ales când sunt realizate cu scopul includerii anumitor elemente în alte produse care nu sunt înregistrate sub aceeaşi descriere. Pentru aceasta nu este suficient să se demonstreze doar similaritatea produselor, ci ar trebui identificate anumite elemente specifice doar programului original. Astfel, ar putea fi înglobate în produsele originale, în mod deliberat, erori sau algoritmi suplimentari, dar care să nu afecteze utilizarea programului, şi care cu greu să poată fi identificate;
- stabilirea în contractele încheiate cu salariaţii a unor clauze prin care aceştia se obligă să respecte confidenţialitatea informaţiilor faţă de alţi producători de produse similare sau faţă de clienţi.

**8.2.2.2 Marcarea copyright-ului**

Există două convenţii internaţionale privind copyright-ul, respectiv Convenţia BERNE şi Convenţia Universală a Copyright-ului, care au efecte în teritoriile ţărilor semnatare ale acestora.

Protecţia oferită în fiecare ţară depinde de legea proprie a copyright-ului, iar convenţiile stabilesc numai drepturile reciproce care se respectă între ţările semnatare.

Legat de modul de marcare a copyright-ului nu sunt cerinţe stricte, dar potrivit prevederilor UCC, drepturile reciproce pot fi respectate dacă se foloseşte notaţia standard:

*© Proprietarul lucrării, anul primei apariţii*

Simbolul poate să apară fie pe prima pagină a publicaţiei, fie la sfârşitul paginii de titlu.

Problema care apare la introducerea notaţiei nu se referă la publicaţii sau alte materiale, ci la includerea ei în cadrul software-ului. Se recomandă ca o notaţie să fie înregistrată astfel încât să fie vizibilă pentru utilizatori, iar o altă notaţie să fie citibilă numai pentru calculator. În acest sens, Oficiul Copyright din SUA a promulgat câteva recomandări pentru plasarea corespunzătoare a notaţiei copyright. Astfel, pentru lucrările reproduse prin copii pe diferite suporturi de memorare, de pe care notaţia nu poate fi vizualizată decât cu ajutorul echipamentului, pot fi folosite următoarele metode de poziţionare a simbolului:

- un simbol care să fie perceptibil la listare, fie în titlu, fie la sfârşitul lucrării;
- un simbol care să fie afişat pe monitorul utilizatorului la demararea lucrului cu programul;
- un simbol care să apară continuu pe ecranul terminalului;
- un simbol fixat pe o etichetă sigură a copiilor, pe o cutie, cartuş, casetă sau orice alt dispozitiv folosit ca un receptor permanent al copiilor.

Trebuie avut în vedere că simbolul care apare în codul sursă, în momentul generării codului-maşină, cu ajutorul translatoarelor (asambloare, compilatoare), fiind considerat un comentariu al programului ar putea fi omis de la translare. De aceea, este necesar ca notaţia copyright-ului să fie realizată într-un format recunoscut la transformarea codului sursă în cod obiect. Acest lucru poate fi realizat prin includerea unei linii duble a notaţiei copyright-ului, care să apară în format alfa-numeric ce va conţine cele trei elemente ale notaţiei (simbolul de copyright, numele autorului şi anul primei apariţii).

**8.2.2.3 Protecţia copyright-ului în România**

În România prima lege care reglementează drepturile de autor şi cele conexe a fost *Legea nr. 8/1996 privind dreptul de autor şi drepturile conexe,* completată ulterior cu *Legea nr. 329 din 14 iulie 2006 privind aprobarea Ordonanţei de Urgenţă 123 din 1 septembrie 2005 pentru modificarea şi completarea Legii nr. 8/1996 privind dreptul de autor şi drepturile conexe***.**

Conform legii modificate şi completate, în capitolul III *Obiectul dreptului de autor*, art. 7, pct. a), constituie obiect al dreptului de autor *programele pentru calculator*, oricare ar fi modalitatea de creaţie, modul sau forma concretă de exprimare şi independent de valoarea şi destinaţia lor. În articolul 8, în categoria operelor derivate create plecând de la una sau mai multe opere preexistente sunt menţionate şi bazele de date – „care, prin alegerea ori dispunerea materialului, constituie creaţii intelectuale".

Potrivit articolului 13 din Capitolul IV – *Conţinutul dreptului de autor*, utilizarea unei opere dă naştere la *drepturi patrimoniale*, distincte şi exclusive, ale autorului de a autoriza sau de a interzice:

a) reproducerea operei;

b) distribuirea operei;

c) importul în vederea comercializării pe piaţa internă a copiilor realizate, cu consimţământul autorului, după operă;

d) închirierea operei;

e) împrumutul operei;

f) comunicarea publică, direct sau indirect a operei, prin orice mijloace, inclusiv prin punerea operei la dispoziţia publicului, astfel încât să poată fi accesată în orice loc şi în orice moment ales, în mod individual, de către public;

g) radiodifuzarea operei;

h) retransmiterea prin cablu a operei;

i) realizarea de opere derivate.

Drepturile asupra programelor de calculator sunt valabile pe tot timpul vieţii autorului, iar după moartea sa se transmit prin moştenire, potrivit legislaţiei civile, pe o perioadă de 70 de ani.

În secţiunea IV *Contractul de închiriere*, articolul 63, se prevede că prin contractul de închiriere a unei opere, autorul se angajează să permită folosinţa, pe timp determinat, cel puţin a unui exemplar al operei sale, în original sau în copie, în special programe pentru calculator ori opere fixate în înregistrări sonore sau audiovizuale. Autorul păstrează dreptul de autor asupra operei închiriate, cu excepţia dreptului de difuzare, dacă nu s-a convenit altfel.

Legea are un capitol distinct privind programele de calculator, unde sunt reglementate aspectele legate de protecţia programelor, stabilind categoriile ce intră sub incidenţa legii, respectiv programele de aplicaţie şi sistemele de operare, exprimate în orice fel de limbaj, fie în cod-sursă sau cod-obiect, materialul de concepţie pregătitor, precum şi manualele.

Autorii programelor beneficiază de drepturile generale ale oricărui autor de opere, aşa cum sunt stabilite în partea I a legii şi enumerate mai sus, cu accentuare asupra dreptului exclusiv de a realiza şi autoriza reproducerea, traducerea, difuzarea originalului sau copiilor unui program. O atenţie specială trebuie acordată articolului 74, care spune că, în lipsa unei clauze contrare, drepturile patrimoniale de autor asupra programelor pentru calculator, create de unul sau de mai mulţi angajaţi în exercitarea atribuţiilor de serviciu ori după instrucţiunile celui care angajează, aparţin *angajatorului*.

Legea oferă şi detalii privind drepturile utilizatorilor programelor legate de realizarea arhivelor, copiilor de siguranţă, testarea funcţionării programului cu ocazia încărcării lui în sistem pentru care există autorizarea din partea autorului. Toate aceste acţiuni se pot face fără autorizarea expresă a autorului. Nu se aplică în cazul programelor pentru calculator prevederile Art. 10, lit. e), care reglementează dreptul de a retracta opera, despăgubind, dacă este cazul, pe titularii drepturilor de exploatare, prejudiciaţi prin exercitarea retractării.

În schimb, art. 78 prevede că autorizarea titularului dreptului de autor nu este obligatorie atunci când reproducerea codului sau traducerea formei acestui cod este indispensabilă pentru obţinerea informaţiilor necesare interoperabilităţii unui program pentru calculator cu alte programe, dacă sunt îndeplinite o serie de condiţii:

a) actele de reproducere şi de traducere sunt îndeplinite de o persoană care deţine dreptul de utilizare a unei copii a programului sau de o persoană care îndeplineşte aceste acţiuni în numele celei dintâi, fiind abilitată în acest scop;

b) informaţiile necesare interoperabilităţii nu sunt uşor şi rapid accesibile persoanelor prevăzute la litera a);

c) actele prevăzute la litera a) sunt limitate la părţile de program necesare interoperabilităţii.

Art. 79 specifică faptul că informaţiile obţinute prin aplicarea art. 78:

a) nu pot fi utilizate în alte scopuri decât la realizarea interoperabilităţii programului pentru calculator, creat independent;

b) nu pot fi comunicate altor persoane, în afara cazului în care comunicarea se dovedeşte necesară interoperabilităţii programului pentru calculator, creat independent;

c) nu pot fi utilizate pentru definitivarea, producerea ori comercializarea unui program pentru calculator, a cărui expresie este fundamental similară, sau pentru orice alt act ce aduce atingere drepturilor autorului.

În capitolul VI al Titlului II al legii, sunt prezentate *drepturile sui-generis ale fabricanţilor bazelor de date.*

Articolul 122 defineşte baza de date ca o culegere de opere, de date sau de alte elemente independente, protejate ori nu prin drept de autor sau conex, dispuse într-o modalitate sistematică ori metodică şi în mod individual accesibile prin mijloace electronice sau printr-o altă modalitate.

Prin fabricantul unei baze de date se înţelege persoana fizică sau juridică ce a făcut o investiţie substanţială cantitativă şi calitativă în vederea obţinerii, verificării sau prezentării conţinutului unei baze de date. Acestuia îi revine dreptul patrimonial exclusiv de a autoriza şi de a interzice extragerea şi/sau reutilizarea totalităţii bazei de date sau a unei părţi substanţiale din aceasta, evaluată calitativ sau cantitativ. Fabricantul nu mai poate împiedica extragerea şi/sau

reutilizarea normală, parţială sau totală a bazei de date dacă a pus-o, prin orice modalitate, la dispoziţia publicului.

În acelaşi timp, însă, utilizatorul legitim al unei baze de date, care este pusă la dispoziţia publicului, *nu poate* efectua acte care intră în conflict cu utilizarea normală a acestei baze de date sau care lezează în mod nejustificat interesele legitime ale fabricantului bazei de date. De asemenea, el nu poate să aducă prejudicii titularilor unui drept de autor sau conex care se referă la opere ori la prestaţii conţinute în această bază de date.

Utilizatorului legitim al unei baze de date, care este pusă la dispoziţia publicului prin orice modalitate, îi este permis, fără autorizarea fabricantului bazei de date, să extragă sau să reutilizeze o parte substanţială a conţinutului acesteia în cazul în care utilizarea este:

a) privată, iar baza de date neelectronică;

b) pentru învăţământ sau pentru cercetare ştiinţifică, cu condiţia indicării sursei şi în măsura justificată de scopul necomercial urmărit;

c) în scopul apărării ordinii publice şi a siguranţei naţionale ori în cadrul unor proceduri administrative sau jurisdicţionale.

Baza de date este protejată de lege pentru 15 ani, începând cu data de 1 ianuarie a anului imediat următor definitivării sale.

De asemenea, orice modificare substanţială, evaluată calitativ sau cantitativ, a conţinutului unei baze de date, constând, în special, în adăugări, suprimări sau schimbări succesive şi pentru care se poate considera că s-a efectuat o nouă investiţie substanţială, evaluată calitativ sau cantitativ, permite atribuirea unei durate de protecţie proprii bazei de date rezultate din această investiţie.

## 8.2.3 Protejarea mărcilor înregistrate

Un ajutor deosebit pentru piaţa calculatoarelor îl poate constitui alegerea unui nume edificator pentru produsul lansat. Un nume uşor de reţinut şi remarcabil poate fi mai mult decât o simplă receptare a produsului. El poate identifica programul cu un comerciant şi poate asigura cumpărătorul sau licenţiatul că i se oferă programul care să-i satisfacă cerinţele aşteptate. Din acest motiv, un nume poate determina obţinerea unei imense valori comerciale, iar cel care-l distribuie va căuta să-şi protejeze *good-will*-ul asociat acestui nume.

Cea mai eficientă metodă de protejare a unui nume ataşat unui program constă în înregistrarea lui ca o marcă. Aceasta asigură recunoaşterea statutară a mărcii ca proprietate atribuibilă şi transmisibilă.

Ca formă a proprietăţii industriale, mărcile înregistrate au un mare avantaj faţă de brevete şi copyright: pot fi obţinute pentru o perioadă nelimitată.

De exemplu, în Marea Britanie, înregistrarea mărcilor este controlată prin Legea Înregistrării Mărcilor, în categoriile clasei 42 fiind incluse programarea calculatoarelor, consultaţiile profesionale şi serviciile de cercetare tehnică. În octombrie 1986 a luat fiinţă Serviciul de Înregistrare a Mărcilor.

## 8.2.4 Licenţele

Deşi, adesea, nu suntem conştienţi de importanţa acestui fapt, licenţele sunt o parte a vieţii noastre de zi cu zi. Aproape toţi dintre noi avem o licenţă de conducere sau pentru TV. Fără îndoială că majoritatea produselor pe care le avem în casă (alimente, jocuri, maşini de uz casnic etc.) au o etichetă ce conţine următoarele cuvinte „produs sub licenţă" (Manufactured under Licence) sau o frază similară. Este clar că licenţa nu se aplică numai calculatoarelor şi soft-ului.

Licenţa are rolul de a asigura producătorul că nici o altă firmă nu va putea realiza produsele sale sub alt nume fără a obţine acordul său, printr-un contract specific acestui gen de operaţiuni.

Unele licenţe derivă din legislaţia specifică unor activităţi pe care guvernele doresc să le controleze şi/sau să-şi asigure un venit din ele. De exemplu, licenţa TV îşi are originea în prevederile Legii telegrafiei din 1949 (Wireless Telegraphy Act). Altele se bazează pe legislaţia privind drepturile de proprietate intelectuală (IPR - Intellectual Property Rights).

Industria informatică poate fi considerată o industrie internaţională; soft-ul poate fi transmis foarte uşor şi rapid în întreaga lume, fie prin intermediul suporturilor de memorare, fie prin liniile de comunicaţii existente.

Problemele comerciale privind protecţia unui program apar ori de câte ori este transferat peste graniţele ţării în care a fost realizat.

Legislaţia privind proprietatea intelectuală are un grad diferit de uniformitate în lume, dar care poate fi influenţat prin convenţiile internaţionale. Totuşi, uniformitatea legislativă în acest domeniu este mult mai mare faţă de legile specifice altor domenii.

Majoritatea ţărilor industrializate recunosc că persoanei care cheltuie timp şi bani pentru a realiza un program informatic trebuie să îi fie asigurată o anumită protecţie împotriva utilizării neautorizate a programului său. Deşi, aşa cum am menţionat anterior, legile nu oferă acelaşi nivel de protecţie, efectele lor asupra informaţiilor confidenţiale, secretelor comerciale, concurenţei neloiale sunt aproape aceleaşi.

De multe ori, se consideră mai eficientă asigurarea protecţiei prin licenţă a anumitor informaţii sau programe, decât prin păstrarea secretului lor de către o persoană sau un grup restrâns de persoane.

În general, prin legislaţia existentă, părţilor interesate într-un contract de licenţă li se oferă libertatea de a-şi stabili termenii contractelor în funcţie de necesităţile lor. Cu toate acestea, sistemul legal al ţărilor tinde să stabilească anumite limite care să permită încadrarea termenilor contractuali într-o serie de norme economice şi sociale.

Prevederile legislative privind tranzacţiile de bunuri şi servicii, inclusiv comercializarea produselor informatice, se referă la condiţiile de desfăşurare a acestora, la calitatea produselor şi la modul de etichetare a bunurilor, conform standardelor naţionale şi internaţionale. Cu toate aceste măsuri, se întâlnesc numeroase cazuri de contrafacere a programelor prin copierea ambalajului şi a etichetelor unui program original, astfel încât clientul este înclinat să creadă că a cumpărat un produs original.

În Marea Britanie, ca şi în alte ţări, există suficiente măsuri de contracarare a unor astfel de acţiuni, pe baza legilor comerciale.

#### 8.2.4.1 Tipuri de licenţe

Pot fi delimitate *cinci principale categorii de licenţe*:

1. transferul drepturilor de licenţă;
2. licenţa simplă;
3. sistemul de închiriere sau leasing al programelor;
4. licenţa pe locul de utilizare a produsului (site licences);
5. licenţa liberă (free licences).

*Transferul drepturilor de licenţă*

În acest caz, proprietarul soft-ului transferă toate drepturile de licenţă unor persoane sau unei firme. Adesea, transferul se extinde şi asupra proprietăţii asociate soft-ului, respectiv asupra copiilor, manualelor şi a dreptului de a continua dezvoltarea şi modificarea sa, prin includerea într-un alt program sau în alte materiale similare.

Exemplul cel mai des întâlnit este cel în care programatorul firmei cere să i se atribuie toate drepturile pentru soft-ul realizat prin termenii contractului de angajare. Aceleaşi cerinţe pot fi solicitate şi de către programatorii angajaţi doar temporar de firmă, sau de o firmă care s-a angajat să realizeze un soft în numele alteia.

Trebuie însă reţinut că în cazul în care prin contractul de transfer al licenţei nu a fost inclusă o clauză ce prevede expres dreptul producătorului de a utiliza programul în cauză şi în

realizarea altor aplicaţii, se poate considera că el a încălcat contractul. Utilizarea oricăror drepturi rezervate de către producător poate deveni subiect de plată a drepturilor de autor de către cel care a încălcat aceste clauze. De asemenea, prin clauzele contractuale pot fi restrânse şi domeniile de activitate în care soft-ul poate fi utilizat.

*Licenţa simplă*

În această categorie de licenţe, producătorul (sau agentul/distribuitorul său) vinde utilizatorului o copie a programului, dar îşi păstrează toate drepturile de proprietate.

Scopul licenţei în acest caz poate fi explicat prin două aspecte.

În primul rând, operaţiunile comerciale în industria informatică sunt mult mai rapide decât în alte domenii. De aceea, producătorul trebuie să se asigure că toate drepturile privind produsele sale sunt respectate, indiferent de noutatea acestora.

De asemenea, se urmăresc şi cazurile în care pot fi folosite copiile programelor. Astfel, unii consideră că ar fi normal ca pe baza unei copii cumpărate ei să-şi poată realiza atâtea copii de câte au nevoie, mai ales în cazurile în care dispun de un sistem bazat pe o reţea de calculatoare. Se pune problema dacă acest lucru ar putea fi un argument favorabil pentru cumpărătorul unei singure copii de a nu fi considerat că a încălcat prevederile contractuale. Acest punct de vedere nu poate fi pus în discuţie, însă, în ceea ce priveşte publicarea manualelor tehnice.

Unii furnizori practică o politică fermă în ceea ce priveşte sistemul copiilor. Astfel, cumpărătorul este obligat să nu folosească decât copia oferită de către furnizor, deci să nu realizeze nici o altă copie, decât cea necesară pentru instalarea programului. Dacă programul nu mai poate fi folosit datorită unor defecţiuni ale mediului de lucru, utilizatorul va trebui să solicite furnizorului înlocuirea programului cu o altă copie. Pentru a-şi asigura securitatea programului împotriva copierilor neautorizate, producătorii au inclus în programe unele sisteme anticopiere, deloc atractive pentru utilizatori.

Dezavantajul acestui tip de licenţă îl constituie faptul că utilizatorul s-ar putea trezi în situaţia de a nu-şi mai putea actualiza soft-ul sau să-l înlocuiască în cazul defecţiunilor, pentru că furnizorul ori a stopat producerea unor elemente necesare în sprijinirea derulării programului ori a încetat comercializarea produsului.

În al doilea rând, trebuie urmărită natura activă a programelor informatice, faţă de cea pasivă a altor produse, de exemplu a înregistrărilor audio.

Un utilizator urmăreşte să cumpere un program care să-i asigure o serie de facilităţi, care ar putea fi puse la dispoziţie de un procesor de texte, un program grafic sau un program de contabilitate. Aceste facilităţi pot fi folosite în trei contexte diferite:

- în scop personal;
- pentru a realiza o activitate care nu este legată în mod special de facilităţile oferite de programe;
- să ofere sprijinul pentru realizarea altor produse sau servicii.

Dacă utilizatorul avea o parte din programele ce îi puteau fi oferite de aceste servicii şi apelează la un furnizor pentru a-i pune la dispoziţie una din componentele necesare, şi acesta dispune de posibilitatea de a-i oferi servicii complexe, l-ar putea considera pe cumpărător un posibil competitor.

Problema de bază a acestei categorii de licenţe o constituie faptul că furnizorul unui produs nu poate avea o legătură directă cu ultimul cumpărător, care poate avea şi el o reţea de desfacere. De aici rezultă, în mod evident, necesitatea de a se stabili o legătură contractuală între producător şi utilizatorul final, care implicit este considerat un contract de licenţă.

Marcajul licenţei, care este mult mai detaliat decât notaţia copyright-ului, este inclus în ambalajul de plastic transparent al dischetelor, CD-urilor pe care programul este înregistrat. O etichetă exterioară atenţionează cumpărătorul să nu rupă învelişul de plastic până nu a citit cu atenţie şi a acceptat condiţiile de licenţă.

*Sistemul de închiriere sau leasing al programelor*

În cazul în care un program este închiriat, furnizorul trebuie să se asigure împotriva efectuării de copii, pe baza prevederilor privind drepturile de proprietate intelectuală.

Regimul de închirieri este practicat mai ales în cazul calculatoarelor mari (mainframe-uri), caz în care furnizorul trebuie să asigure asistenţa şi actualizarea permanentă a programelor. Condiţiile de licenţă sunt mult mai complexe decât în cazurile anterioare, deoarece furnizorul are nevoie de un control asupra mediului de lucru al utilizatorului. De exemplu, dacă are loc o actualizare a sistemului de operare ce a fost închiriat prin licenţă pot să apară modificări ale aplicaţiei şi diagnosticarea programelor care se execută sub acel sistem de operare. O altă problemă apare atunci când utilizatorul decide să păstreze programele sale în momentul adaptării sistemului de operare.

În mod convenţional, licenţa este specificată pentru un utilizator şi un calculator anume. Este necesar să fie stabilită perioada pentru care s-a încheiat contractul şi dacă la sfârşitul acestei perioade furnizorul doreşte să vândă produsul său. Uneori intervin dificultăţi ca urmare a faptului că utilizatorul nu doreşte să preia toate programele incluse în contractul de închiriere sau urmăreşte să-l descompună în mai multe subcomponente, care vor funcţiona cu funcţii bine stabilite.

Forma contractelor de licenţă nu este prestabilită, aplicându-se de la un caz la altul. În general, prin forma de contract sunt surprinse toate problemele, începând cu suma care va fi plătită pentru obţinerea licenţei, drepturile care se acordă utilizatorului produsului închiriat în ceea ce priveşte realizarea copiilor de siguranţă, modificarea programului, utilizarea lui pentru obţinerea unor produse similare din punct de vedere al funcţionării sau în cadrul unor sisteme care nu sunt supuse licenţei, în caz de urgenţă sau în cazurile în care pot fi necesare pentru derularea eficientă a diferitelor operaţiuni.

*Licenţa pe un loc de utilizare (site licences)*

Unii licenţiatori sunt dispuşi să ofere unui utilizator o licenţă în termeni deosebit de favorabili în ceea ce priveşte copiile ce pot fi realizate pe baza programului ce constituie obiectul contractului de licenţă. În alte cazuri, se acordă substanţiale reduceri de preţuri dacă utilizatorul acceptă o singură copie a programului, cu condiţia ca modificările sau actualizările ulterioare să fie suportate de el, astfel că pentru producător/distribuitor costurile administrative se reduc simţitor. Avantajul acestei licenţe pentru cel care o acceptă constă în posibilitatea de a stabili fără acordul proprietarului momentul în care poate să-şi modifice sistemul, pentru a-şi asigura compatibilitatea cu noile programe achiziţionate.

Licenţa acordată pentru mai multe copii ale unui program capătă noi semnificaţii în următoarele condiţii:

- folosirea unor calculatoare similare (PC-uri sau staţii de lucru) într-o singură unitate, în loc de un mainframe, care ar fi putut să ofere aceleaşi facilităţi de lucru;
- creşterea capacităţii şi complexităţii sistemelor distribuite şi a reţelelor.

Unii utilizatori sunt mai interesaţi în reducerea costului soft-ului, în timp ce alţii urmăresc să obţină libertate în utilizarea programelor, astfel încât să-şi asigure fără probleme continuitatea licenţei şi păstrarea înregistrării.

*Licenţa liberă (free licences)*

Sunt unele surse care asigură obţinerea programelor fără a mai apela la licenţe, cum sunt bibliotecile de programe, magazinele de calculatoare, grupurile de utilizatori, revistele şi unele firme distribuitoare. Aceste programe sunt considerate de interes public sau sunt unele care prin preţul lor asigură acoperirea oricărui tip de pierdere. Nici un program de acest tip nu-l scuteşte pe utilizator de vreun cost, dar este mult mai ieftin. Astfel, un program care va fi listat dintr-un magazin specializat va fi vândut la un preţ ce nu va include şi o valoare a licenţei, dar cumpărătorul va trebui să facă dovada existenţei unui mediu de lucru adecvat şi a timpului necesar introducerii instrucţiunilor de la tastatura sistemului său.

Programele sunt realizate, de cele mai multe ori, pe suporturi disponibile oricărui sistem de prelucrare a datelor, cu preţuri care acoperă şi eventualele pierderi datorate de copierea neautorizată, precum şi un drept de autor.

Acest tip de licenţă nu garantează şi faptul că programul va funcţiona pe orice tip de calculator sau că se vor obţine rezultatele care sunt aşteptate de utilizator.

**8.2.4.2 Aspecte generale ale licenţelor**

Toate componentele dreptului de proprietate intelectuală, mai ales cele referitoare la produsele din domeniul informatic, sunt influenţate de o serie de factori, dintre care mai importanţi sunt:

*Eterogenitatea utilizatorilor*

Pătrunderea explozivă a calculatoarelor personale a determinat modificarea, aproape peste „noapte", a grupurilor ce lucrează cu echipamente profesionale de prelucrare automată a datelor, acum putând fi considerat utilizator oricine poate folosi o tastatură, indiferent de scopul urmărit. Astfel, s-a extins dorinţa sau nevoia de utilizare a calculatoarelor de la copii de vârstă şcolară, până la bunicile lor, care-şi păstrează reţetele pe calculator. Este de presupus că nici nepoţii şi nici bunicile nu au vreo cunoştinţă despre drepturile de proprietate intelectuală şi ce presupun ele. În consecinţă, ei nu-şi vor da seama că folosind copii ale unor programe sau jocuri comit o ilegalitate privind încălcarea copyright-ului sau a altor forme de protecţie. Ca urmare, industria informatică a reacţionat în consecinţă, dar fiecare firmă în felul ei (unele dintre ele invadând piaţa calculatoarelor, altele încercând să-şi asigure un grad cât mai ridicat de protecţie a produselor lor).

La nivel general s-a căzut de acord că este necesară asigurarea securităţii privind sistemele informatice. Astfel, în Marea Britanie a fost introdus un amendament al Legii Copyright-ului şi s-a creat, în 1984, Federaţia Împotriva Furtului de Software (*FAST - Federation Against Software Theft*), cu rol în educarea publicului, în general, şi a utilizatorilor de calculatoare, în particular, în asigurarea protecţiei programelor prin lege şi încurajarea respectării drepturilor legale ale producătorilor de soft.

Se crede, totuşi, că prin activităţile unor astfel de organisme nu se vor rezolva marile probleme care apar în acest domeniu. Problema protejării împotriva realizării copiilor neautorizate este doar una din fatetele generale ale aspectelor proprietăţii intelectuale. Cum pot fi constrânşi studenţii să plătească drepturile de autor proprietarilor programelor, când profesorii lor folosesc sute de copii xerografiate din materiale cu drept de copyright, pentru uzul şcolar? În al doilea rând, este destul de puţin probabil ca prin educaţie să se elimine pirateria „profesională", deşi potenţialii cumpărători de produse de acest gen încep să devină mult mai circumspecţi.

*Mărimea pieţei*

Majoritatea piraţilor de soft şi a imitatorilor sunt interesaţi în obţinerea unui profit cât mai rapid şi mai mare, prin producerea de copii ale unui produs şi exploatarea altora. Extinderea pieţei, care trebuie să satisfacă cerinţele diferitelor tipuri de utilizatori, determină o creştere a cererii şi, în consecinţă, o sporire a ofertei de produse, astfel că a devenit un domeniu deosebit de atrăgător şi profitabil pentru producătorii-piraţi, care şi-au mutat domeniul de acţiune de la producerea de copii imitate ale casetelor audio la cel al produselor informatice.

În general, piratul nu doreşte să se implice în acordarea vreunui sprijin cumpărătorilor programelor sale. El nu are adesea nici o pregătire tehnică sau informatică, esenţială în oferirea unor astfel de servicii. Programele, de cele mai multe ori, nu sunt funcţionale din cauza conversiilor neglijente sau a tehnicilor neadecvate de copiere, ceea ce determină din partea utilizatorilor depunerea de plângeri către diferitele magazine care-şi oferă serviciile de întreţinere. Dacă programul este contrafăcut, plângerile pot ajunge şi la firmele producătoare, dar fără nici un rezultat.

Unii distribuitori de copii nelicenţiate ale programelor originale, care sunt capabili să schimbe pachete de hard/soft pentru a creşte rata profitului, pot să-şi stopeze activitatea imediat ce simt că furnizorii lor au descoperit ceva. Este greu de înţeles ce este în mintea lor – ori cred că furnizorii nu-i vor prinde, ori că nu vor întreprinde nimic împotriva lor în cazul în care sunt depistaţi.

Un alt exemplu de copiere cu „grijă" este cel în care utilizatorul obţine o copie licenţiată pentru un program general, cum este un procesor de texte sau un program de calcul tabelar, cu intenţia ascunsă de a-l folosi pe un alt calculator decât pe cel căruia i s-a acordat dreptul de utilizare. Un caz similar apare şi când el cumpără calculatoare similare cu cel pentru care i s-a acordat dreptul de utilizare a programului şi cade în tentaţia de folosi atâtea copii ale programului câte are nevoie. Problemele apar nu numai la nivelul PC-urilor, ci şi la nivelul mainframe-urilor, care necesită programe mai complexe. Deşi au fost prinşi de nenumărate ori în astfel de situaţii, utilizatorii refuză să accepte că ar fi făcut ceva ilegal.

*Costul echipamentelor*

Problema pachetelor de aplicaţii este legată de asigurarea continuităţii lor, de cele mai multe ori privind programele de salarii, de contabilitate etc. Programele achiziţionate asigură utilizatorului o bază substanţială de pornire, deoarece aproape toate programele rulate în cadrul firmelor sunt rezultatul unei improvizaţii, prin adăugarea de noi facilităţi şi prin simplificarea modului de utilizare a programelor existente.

Preţul programelor originale a fost determinat în cea mai mare măsură, în ultimul timp, în concordanţă cu preţul echipamentului pe care se intenţionează a se instala. Dar este puţin probabil că un utilizator va fi dispus să plătească un preţ pentru o aplicaţie standard care este comparabil cu costul echipamentului său, preferând, în schimb, să apeleze la copii ale programelor de care are nevoie, care însă, de cele mai multe ori, sunt şi copii pirat. Iată şi unul din motivele scăderii continue a costului echipamentelor în comparaţie cu creşterea gradului lor de performanţă, mai ales ca urmare a presiunii exercitate de furnizorii de soft.

*Sistemele distribuite şi reţelele de calculatoare*

Aşa cum se ştie, reţelele sunt definite, din punct de vedere al scopului lor, ca unităţi de prelucrare interconectate între ele, astfel încât să fie posibil transferul informaţiilor. Un program, în acest caz, poate fi considerat ca fiind un grup de informaţii, transmisibil în sistemul reţea prin modul lui de realizare. Din această cauză, un program poate fi disponibil pentru întreaga reţea sau numai pentru un anumit număr de terminale.

Din punctul de vedere al acordării licenţelor pot fi identificate mai multe tipuri de reţele, şi anume:

- o reţea simplă, în care controlul este realizat doar de o singură componentă a acesteia. Cel mai elocvent exemplu este cel în care într-o unitate există câteva calculatoare dispersate, conectate într-o reţea. Sistemul este folosit doar de salariaţii firmei sau de alte persoane care au autorizarea necesară utilizării lui. Pentru astfel de cazuri poate fi obţinută o licenţă de loc (site licence) pentru programele care vor fi instalate în toată reţeaua prin achiziţie sau prin închiriere. În aceste cazuri, termenii de încheiere a contractului de licenţă trebuie să se bazeze pe un anumit grad de încredere între licenţiator şi licenţiat;
- un alt tip de reţea poate fi definit ca un sistem bazat pe subscrieri sau abonamente. Un exemplu tipic îl constituie bazele de date comerciale, ce conţin informaţii şi programe protejate prin patente, informaţii despre o serie de decizii legale, proiecte, clienţi etc. Oricine poate plăti un operator care să-i descopere parola sau instrucţiunile de utilizare a acestui sistem şi de acces la baza de date prin intermediul liniilor telefonice sau a unui terminal. În general, programele în astfel de reţele sunt foarte bine protejate şi nu pot fi accesate foarte uşor nici chiar de către abonat;

- o altă categorie de reţea este caracterizată printr-un grad mare de acces, adesea fiind folosită de către organizaţii mari, cum sunt universităţile, pentru a încuraja schimbul de informaţii. Sistemul poate fi destul de vulnerabil la un nivel minim de securitate a soft-ului, ca urmare a dorinţei de a simplifica accesul utilizatorilor începători. Un potenţial spărgător poate obţine destul de uşor accesul prin simple tehnici de pătrundere în sistem sau prin descoperirea parolelor de la un terminal;
- sistemele mari de reţele sunt caracterizate de transferul datelor şi/sau programelor între calculatoare situate în diferite ţări. În aceste condiţii pot să apară numeroase probleme legate de nivelurile diferite de protecţie pe care le asigură ţările. Legile privind licenţele nu sunt uniforme; de aceea este necesar să se realizeze contracte de licenţe separate în funcţie de ţara în care urmează a fi folosite programele.

Un alt domeniu al legislaţiei se referă la nivelul de securitate naţională garantat, libertatea de circulaţie a informaţiilor şi confidenţialitatea datelor.

De asemenea, nu trebuie uitaţi nici factorii politici şi economici, care pot influenţa foarte mult cadrul legal al protecţiei diferitelor componente informatice.

*Proiectarea şi producţia asistată de calculator*

Câteva dintre argumentele care au stat la baza asigurării protecţiei proprietăţii intelectuale a programelor şi a ieşirilor obţinute în urma prelucrării datelor şi a utilizării programelor s-au bazat pe conceptul că prin sistem se asigură doar procesul de prelucrare a datelor de intrare pentru a obţine informaţiile de ieşire. Cu toate acestea, ieşirile dintr-un sistem de proiectare asistată de calculator reprezintă, direct sau indirect, proiectul unui obiect fizic. De multe ori, calculatoarele şi programele folosite sunt o parte integrantă a procesului de producţie.

Noua generaţie de sisteme de producţie încearcă să integreze un grup cât mai mare de funcţii de producţie, ca şi în cazul sistemelor care înglobează protocoalele standard ale reţelelor care asigură schimbul de informaţii între diferite unităţi.

De multe ori copierea ilegală este considerată de către producători drept o vânzare pierdută. Experienţa zilnică arată că principalul motiv al efectuării de copii ilegale de către diferite persoane, altele decât „piraţii profesionişti", îl constituie comoditatea sau indiferenţa faţă de drepturile de proprietate intelectuală. Cel mai elocvent exemplu este o persoană care este interesată să consulte doar câteva pagini dintr-o carte, care costă 50-60 de dolari. Pentru el este mult mai avantajos să copie acele pagini necesare, decât să cumpere întregul material. Dacă nu poate să realizeze copiile, atunci, cu siguranţă, va consulta cartea într-o librărie sau o bibliotecă şi îşi va face câteva notiţe. În acest caz nu se va cumpăra nici o copie a întregului document, ceea va determina o posibilă pierdere de profit faţă de cazul în care materialul ar fi fost cumpărat. Majoritatea editurilor au devenit conştiente de acest fenomen şi au luat o serie de măsuri de înregistrare a unei menţiuni prin care se specifică că sunt autorizate doar copiile făcute în scopuri non-profit.

## 8.2.5 Măsuri tehnice de protecţie a licenţei software-ului

Din studiile efectuate, s-a ajuns la concluzia că măsurile privind protecţia programelor prin legile în vigoare nu sunt suficiente pentru a asigura protejarea drepturilor de proprietate intelectuală, ceea ce a determinat elaborarea unor măsuri care urmăresc prevenirea sau depistarea copierii neautorizate, piratării sau utilizării neautorizate a produselor-program. Aceste măsuri, denumite măsuri tehnice de protecţie, sprijină protecţia oferită de copyright sau de alte drepturi de proprietate intelectuală producătorilor de soft sau editorilor de materiale privind soft-ul realizat.

Licenţa privind programele specifică ce clienţi pot utiliza sau nu programul aflat sub licenţă. Principalele restricţii în utilizarea unor astfel de programe includ:

- un număr limitat de copii autorizate ale programului;

- orice copie realizată poate fi folosită numai în scopul asigurării unei copii de siguranţă a programului original;
- stabilirea unei perioade maxime de utilizare a programului;
- programul trebuie să fie folosit numai în scopurile proprii ale celui care l-a cumpărat;
- programul va fi folosit doar pe un singur procesor sau într-o anumită configuraţie hard sau soft, sau poate rula doar pe un singur calculator la un moment dat;
- nu se va permite realizarea de copii ale manualelor de utilizare sau ale altor documentaţii asociate.

Măsurile tehnice de protecţie au fost recent recunoscute ca fiind unele din cele mai benefice metode de prevenire sau detectare a copierii neautorizate, pirăterii sau a utilizării soft-ului fără a avea licenţa necesară.

În perioada de început a utilizării microcalculatoarelor au fost foarte puţine cazuri de încălcare a drepturilor producătorilor de soft. Acest lucru se datora mai ales faptului că multe programe specifice mainframe-urilor şi minicalculatoarelor dispuneau de caracteristici care ofereau, în mod automat, un anumit nivel de protecţie. Unele programe au fost realizate pentru a satisface cerinţele unui singur client sau pentru o mică piaţă specializată, în care numărul clienţilor era destul de redus. În aceste cazuri, era puţin probabil ca un client autorizat să realizeze copii ale programului pentru un alt utilizator. Dacă, totuşi, se întâmpla acest lucru, el putea fi foarte uşor descoperit de către producător, datorită numărului mic de utilizatori al unui astfel de program.

Aproape toate produsele-program standard necesită servicii de întreţinere după ce au fost implementate. În cazurile în care apar unele erori în timpul utilizării programului ele pot fi corectate doar de către producător pentru că el este cel care deţine codul-sursă al programului. De obicei, producătorii consideră codul-sursă ca fiind o informaţie confidenţială a firmei producătoare. Deci, fără acces la codul-sursă, utilizatorul nu poate depista defecţiunea din program care generează erorile şi nu va şti ce instrucţiuni trebuie corectate pentru a face disponibil programul.

Un alt gen de servicii post-implementare îl constituie actualizarea sau înlocuirea soft-ului, care poate interveni la înnoirea hard-ului sau sistemului de operare al utilizatorului. Acest lucru nu poate fi realizat dacă programul a fost achiziţionat de la persoane neautorizate (firme sau alţi utilizatori). De cele mai multe ori, însă, utilizatorii caută să-şi înregistreze sub licenţă programele achiziţionate.

Aceste modalităţi de asigurare a protecţiei soft-ului sunt considerate ca metode implicite de protejare. Nu este cazul şi pentru programele specifice microcalculatoarelor.

Ca urmare a exploziei calculatoarelor pe piaţa produselor informatice, copiile produselor program sunt identice pentru a putea fi folosite de miile de utilizatori pe configuraţii hard şi sisteme de operare similare.

Toate sistemele de operare au făcută o copie de către operatorul de sistem, cu scopul de a asigura funcţionalitatea sistemului în caz de defectare. Dar, aceste copii pot fi distribuite altor utilizatori pentru a le permite realizarea procesului de prelucrare a datelor din activitatea lor.

Majoritatea producătorilor de soft nu au vânzări foarte mari în mod direct, ei oferind mai mult sprijin post-implementare pentru corectarea erorilor şi alte servicii specifice miilor de utilizatori din ţară şi de pretutindeni. Mai concret, ei, în mod normal, oferă şi sprijină aceste servicii prin intermediul unui lanţ de distribuitori, care pot realiza copii ilicite şi pot distribui soft în propriul lor folos. În majoritatea cazurilor, clienţii nu intră în contact direct cu producătorul, ci cu intermediarii acestuia.

Mulţi producători încearcă să-şi verifice distribuitorii prin interzicerea realizării de copii ale programelor. În plus, ei oferă, pentru fiecare produs, o fişă de înregistrare ce va fi completată de către cumpărător, căruia i se cere să o returneze completată producătorului şi nu distribuitorului, ca o condiţie de a obţine serviciile post-implementare direct de la producător. Astfel, din punct de

vedere teoretic, producătorul va avea câte o înregistrare pentru fiecare client, indiferent de distribuitorul de la care a fost cumpărat produsul, putând verifica dacă i-au fost achitate sumele ce i se cuvin ca drept de autor. Această metodă nu este prea eficientă, pentru că de cele mai multe ori clienţii uită să trimită fişele, în timp ce alţii nu primesc din start o astfel de fişă. Distribuitorul ar putea să reproducă produsul împreună cu documentaţia asociată, producătorul neavând o evidenţă a tranzacţiilor ilegale care au fost efectuate şi nici a drepturilor lui de autor ce i s-ar fi cuvenit pentru produsele astfel vândute. Din punctul de vedere al unor producători, este mult mai eficient să se prevină sau să se depisteze acţiunile de copiere ilegală folosind metode de protecţie tehnică proiectate cu scopul de a preveni copierea sau utilizarea neautorizată a produselor lor.

Alţi producători au încercat să împiedice astfel de activităţi fără a interveni efectiv în program, ci prin realizarea unor manuale de utilizare şi a altor materiale similare dificil de copiat, în timp ce soft-ul nu poate fi utilizat fără a avea accesul la aceste materiale. Tehnicile care se aplică în aceste cazuri constau în utilizarea unui tip de hârtie care nu are dimensiune standard, a unor culori rezistente la fotocopiere etc.

Din studiile întreprinse în diverse firme din Marea Britanie, s-au desprins următoarele metode tehnice de protecţie:

1. *măsuri pentru depistarea copierii şi utilizării neautorizate a programelor*, care constau în includerea notaţiei copyright-ului sau a altor observaţii în cadrul programului. Aceste notaţii vor fi afişate în momentul folosirii programului, astfel că operatorul va fi atenţionat asupra dreptului de copyright al furnizorului şi/sau a numelui cumpărătorilor autorizaţi să realizeze copii ale programului;
2. *măsuri de prevenire a copierii neautorizate a soft-ului* prin care furnizorii, pentru programele oferite pe diferite suporturi de memorare, folosesc diferite metode de protecţie, cum ar fi formatarea non-standard a discurilor şi nesincronizarea biţilor. Aceste măsuri previn reîncărcarea unui program în momentul în care clientul poate invoca o cădere a acestuia. Programul poate fi reîncărcat numai apelând la furnizor, care deţine un program specific de reîncărcare, înlocuind temporar sistemul de operare al clientului, în timpul operaţiunii de refacere a programului;
3. *măsuri de prevenire a utilizării neautorizate a programului*, care includ un mod de blocare temporară a programului după ce a expirat termenul legal de utilizare sau un număr serial pe chip-uri, astfel încât programul să poată fi folosit numai pe un anumit calculator care conţine numărul de chip specificat. O altă măsură o constituie legarea programului de un dispozitiv periferic, care în momentul operării trebuie să fie localizat la un port specific sistemului utilizatorului în măsură să facă posibilă utilizarea programului. Prezenţa dispozitivului sau a unui număr va fi verificată permanent, iar în cazul în care acesta lipseşte programul se va opri prin blocare.

Deşi multe firme au inclus în strategiile lor şi măsuri tehnice de protecţie, ele afirmă că se confruntă în continuare cu pierderea de venituri din reproducerea neautorizată sau pirateria soft-ului.

Din studiile efectuate în Marea Britanie şi SUA s-a ajuns la o serie de concluzii care converg spre a considera că problemele industriei informatice, în ceea ce priveşte asigurarea protecţiei drepturilor de proprietate intelectuală, sunt mult mai grave decât cele din alte sectoare industriale. Deşi perceperea importanţei problemelor este diferită de la o firmă la alta, se pare că majoritatea companiilor producătoare de soft sunt interesate şi încearcă, pe cât le este posibil, să prevină şi să descopere activităţile de copiere sau utilizare neautorizată a programelor sau pe cele de piraterie. Există, însă, unele firme care îşi motivează imposibilitatea de a face faţă pierderilor cauzate de concurenţă pe seama unor astfel de activităţi. Deci, pentru astfel de firme activităţile ilegale pot constitui o scuză destul de plauzibilă în faţa publicului în ceea ce priveşte incapacitatea lor de a obţine profit pentru produsele lor.

Daţi exemple de încălcări ale dreptului de autor, mărcii înregistrate, patentelor şi licenţelor cu care v-aţi întâlnit în viaţa reală sau în literatură.

## Rezumat

Capitolul de faţă a avut rolul de a oferi informaţii privind reglementările legislative existente în România pe linia securităţii informaţiilor, sistemelor informatice şi spaţiului cibernetic. Au fost tratate pe scurt principalele legi emise în domeniu în România.

De asemenea, s-au prezentat principalele aspecte privind copyright-ul, marcarea produselor software, licenţele şi modalităţile de protejare a acestora.

# Bibliografie generală


1. **Allen, J.H** – *The CERT Guide to System and Network Security Practice*, Addison-Wesley Publishing Company, Inc., Reading Massachusetts, 2001.
2. **Anderson, R.** – *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Computer Publishing, John Wiley & Sons, Inc., New York, 2001.
3. **Andress, M.** – *Surviving Security: How to Integrate People, Process, and Technology,* Sams Publishing, 2002.
4. **Baker, R.** – *Network Security: How to Plan for It and Achieve It*, McGraw-Hill, New York, 1995.
5. **Barman, S.** – *Writing Information Security Policies*, New Riders Publishing, Boston, 2002.
6. **Bishop, M.A.** – *Computer Security: Art and Science*, Addison Wesley Professional, Reading, Massachusetts, 2001.
7. **Davis, D.** – „The Problems Catch Up With The Solution", in *Card Technology*, April 2003, Volume 8, Number 4.
8. **Denning, D.** – *Information Warfare and Security*, Addison Wesley, Reading, Massachusetts, 1999.
9. **Desman, M.B.** – *Building an Information Security Awareness Program*, Auerbach Publications, New York, 2001.
10. **Frank, A.G., Gills, B.K.** – „The Five Thousand Year World System: An Interdisciplinary Introduction", in *Humboldt Journal of Social Relations*, vol. 18, No. 2, Spring 1992.
11. **Gros, A.Y**. – What is "Trade Secret" So As to Render Actionable Under State Law Its Use or Disclosure by Former Employee, 59 ALR 4th, 641, 652 (1988).
12. **Hawker, A.** – *Security and Control in Information Systems: A guide for Business and Accounting*, Routledge Information Systems Textbooks, London and New York, 2001.
13. **Howard, M., LeBlanc, D.** – *Writing Secure Code*, 2nd Edition, Microsoft Press, Redmond, Washington, 2003.
14. **Igbaria, M, Anandarajan, M., Chen, C.C-H.** – „Global Information Systems", in *Encyclopedia of Information Systems*, vol. 2, Academic Press, San Diego, CA, 2003.
15. **Jenkins, G., Wallace, M.** – *IT Policies and Procedures: Tools and Techniques that Work*, Third edition, Prentice Hall, New York, 2001.
16. **Katz, A.H.** – „Classification: System or Security Blanket", in *J. Natl. Class. Mgmt. Soc.*, 8, 76-82 (1972).
17. **King, C.M., Dalton, C.E., Osmanoglu, T.E.** – *Security Arhitecture: Design, Deployment and Operations*, Osborne/McGraw-Hill, Berkely, CA, 2001.
18. **Krause, M., Tipton, H.F.** – *Information Security Management Handbook*, Fourth Edition, Volume I, Auerbach Publications, New York, 1999.
19. **Kristof, R., Anderson, D., a.o.** – *Mission Critical Internet Security*, Syngress Publishing, Inc., Rokland, MA, 2001.
20. **Krutz, R.L., Vines, R.D.** – *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, Wiley Computer Publishing, John Wiley & Sons, Inc., New York, 2001.
21. **Lubbers, R.** – *Globalization, Economists and the Real World*, Tilburg University, Contribution To the Lunchseminar of March, March 3, 1998.
22. **Micro Modeling Associates, Inc.** – *Microsoft Commerce Solution Web Technology*, Microsoft Press, Redmond, Washington, 1999.
23. **Miller, M.** – *Absolute PC Security and Privacy,* Sybex, San Francisco, 2002.
24. **Munteanu, A.** – *Auditarea sistemelor informaţionale contabile: cadru general*, Editura Polirom, Iaşi, 2001.
25. **Năstase, D.** – *„Necunoscute" ale izvoarelor istoriei româneşti*, Extras din Anuarul Institutului „A. D. Xenopol", XXX, Ed. Academiei Române, Iaşi, 1993.
26. **Oprea, D.** – *Premisele şi consecinţele informatizării contabilităţii*, Editura Graphix, Iaşi, 1995.
27. **Oprea, D.** – „Particularităţi ale securităţii sistemelor informatice bazate pe partajarea resurselor", în *Tribuna Economică*, 13, 1995.

28. **Oprea, D.** – „Vulnerabilitatea securităţii sistemelor bazate pe microcalculatoare”, în *Tribuna Economică*, 15, 1995.
29. **Oprea, D.** – „Pericole ce vizează sistemele informatice”, în *Tribuna Economică*, 16, 1995.
30. **Oprea, D.** – „Protecţia fizică a sistemelor informatice”, I-IV, în *Tribuna Economică*, 39-42, 1995.
31. **Oprea, D.** – „Securitatea comunicaţiilor”, I-II, în *Tribuna Economică*, 40, 43, 1996.
32. **Oprea, D.** – „Security Particularities of Information Systems”, in *Contributi allo studio della transizime dell'agricultora rumena verso il mercator: aspetti struttorali, economici ed estimativi*, Edizioni Conquiste, Bologna, Italy, 1997.
33. **Oprea, D.** – „Tipologia hackerilor”, în *Tribuna Economică*, 50, 1997.
34. **Oprea, D.** – „Tipologia hackerilor”, în *Tribuna Economică*, 1-2, 1998.
35. **Oprea, D.** – *Analiza şi proiectarea sistemelor informaţionale economice*, Editura Polirom, Iaşi, 1999.
36. **Oprea, D.** – *Managementul proiectelor: teorie şi cazuri practice*, Editura Sedcom Libris, Iaşi, 2001.
37. **Oprea, D., Airinei, D., Fotache, M. (coord.)** – *Sisteme informaţionale pentru afaceri*, Editura Polirom, Iaşi, 2002.
38. **Oprea, D., Meşniţă, G.** – *Sisteme informaţionale pentru manageri*, Editura Polirom, Iaşi, 2002.
39. **Patriciu, V.V., Pietroşanu-Ene, M., Bica, I., Cristea, C.** – *Securitatea informatică în Unix şi Internet*, Editura Tehnică, Bucureşti, 1998.
40. **Peltier, T.R.** – *Information Security Policies, procedures and Standards: Guidelines for Effective Information Security Management*, Book News, Inc., New York, 2001.
41. **Renesse, R.** – *Optical Document Security*, 2nd Edition., Artech House, 1997
42. **Renesse, R.** – „Verifying versus Falsyfying Banknotes”, in *Optical Security and Counterfeit Deterrence Techiques II*, IS&T (The Society for Imaging Science and Technology) and SPIE (The International Society for Optical Engineering), v 3314, IS1314, 0-8194-2754-3, 1998.
43. **Rivest, R.L., Shamir, A., Adleman, L.M.** – „A Method for Obtaining Digital Signatures and Public Key Cryptosystems”, in *Communication of the ACM*, v.21, n.2, feb. 1978.
44. **Schwartan, W.** – *Information Warfare*, 2nd Edition, Thunder's Mouth Press, New York, 1996.
45. **Simmons, G.J.** – „The Prisoners' Problem and the Subliminal Channel”, in *Proceedings of Crypto '83*, Plenum Press (1984).
46. **Smith, MA.** – *Commonsense Computer Security: Your Practical Guide to Information Protection*, 2nd Edition, McGraw-Hill Book Company, London, 1993.
47. **Tudor, J.K.** – *Information Security Arhitecture: An Integrated Approach to Security in the Organization*, Auerbach Publications, New York, 2000.
48. **U.S. Department of Energy** – „Identification of Classified Information”, *Office of Classification*, December 1991, Chapter IV, Part B, § 3.
49. *** – „Securing the Cloud. A Survey of Digital Security”, in *The Economist*, Volume 365, Number 8296, October 26th-November 1 st, 2002.

# Referinţe Internet

50. Central Command: *www.vexira.com*
51. Command Software System – Antivirus: *www.commandsoftware.com*
52. Command Software System : *www.commandondemand.com*
53. Computer World Romania: *www.computerworld.ro*
54. Counterpane Internet Security: *wwww.counterpane.com*
55. Cyber Crime … and Punishment? Archaic Laws Threaten Global Information: *www.mcconnellinternational.com*
56. Dice-Tech Jobds. Tech Talent: *www.dice.com*
57. EuroCERT –The European Security Incident Information Service: *www.eurocert.net*
58. FAQ – IT Investments: *www.rms.net/lc_faq_cat_itv.htm*
59. Final Rule: Privacy of Consumer Financial Information (Regulation S-P): *www.sec.gov/rules/final/34-42974.htm*
60. Frisk Software International: *www.f-prot.com*
61. F-Secure Corp.: *www.f-secure.com/products/antivirus*

62. Grisoft, Inc. – Antivirus: *www.grisoft*
63. International Federation for Information Processing: *www.ifip.org*
64. Introducing the Secure Enterprise: *www.symantec.com*
65. Kaspersky Lab: *www.viruslist.com*
66. Ministerul Justiției – România, Superlex: *http://domino2.kappa.ro/mj/superlex.nsf*
67. Monster – The World's Leading Career Network: *www.monster.com*
68. NetReport: *www.netreport.ro*
69. Network Associates: *www.mcafee.com*
70. Norman Virus Control: *www.norma.com*
71. Office of the Information and Privacy Commissioner: *www.opcbc.org*
72. Panda Antivirus Platinum: *www.panda-security.com*
73. Pinkerton: *www.pinkerton.com*
74. Protecţia informaţiilor clasificate: *www.sri.ro/biblioteca_art_infclas.html*
75. Rău, P. – Infracţionalitatea pe calculator, *www.rap.freehosting.net/Infract/index.html*
76. Sophos – Antivirus: *www.sophos.com*
77. The Biometric Consortium: *www.biometrics.org*
78. The Computer Security Institute (CSI): *www.gocsi.com/homepage.shtml*
79. The European Union On-Line: *www.europa.eu.int/*
80. The Information Systems Security Association (ISSA): *www.issa.org*
81. Trend Micro-Antivirus: *www.antivirus.com/pc-cillin*
82. The National Strategy to SECURE CYBERSPACE, February 2003, The White House, Washington: *www.whitehouse.gov/pcipb/cyberspace_strategy.pdf*

# Bibliografie disponibilă în biblioteca FEAA

Generală, cu arie mare de cuprindere:

1. **Bigdoli, H**. - *Handbook of Information Security*, vol.1- 3, John Wiley - Sons, 2006
2. **De Leeuw, K., Bergstra, J**. - *The History of Information Security. A Comprehensive Handbook*, Elsevier, Amsterdam, 2007

Securitatea la nivelul organizațiilor:

1. **Calder, A**.- *A Business Guide to Information Security*, Kogan Page, London, 2005
2. **Dhillon, G**. - *Principles of Information System Security. Text and cases*, John Wiley & Sons,USA, 2007
3. **Gregory, P., G.** - *Securitatea informaţiilor în firmă*, Traducere Nicolae Ionescu Cruţan, Ed. Rentrop & Straton, București, 2005
4. **Herold, R.** - *Managing an Information Security and Privacy Awareness and Training Program*, Auerbach Publications, Taylor&Francis Group, New York, 2005
5. **Killmeyer, J.** - *Information Security Architecture. An Integrated Approach to Security in the Organization*, Auerbach Publications, Taylor&Francis Group, New York, 2006
6. **Layton, T.** - *Information Security. Design, Implementation, Measurement and Compliance*, Auerbach Publications, Taylor&Francis Group, New York, 2007
7. **LeVeque, V.** - *Information security – A strategic approach*, Wiley Interscience, USA, 2006
8. **Tipton, H., Krause, M.** - *Information Security Management Handbook*, vol. 3, Auerbach Publications, Taylor&Francis Group, New York, 2006

Hackeri:

1. **Davis, C., Cowen, D., Philipp, A.** - *Hacking Exposed. Computer Forensics Secrets & Solutions*, McGraw Hill/Osborne, New York, 2005
2. **McClure, S., Scambray, J., Kurtz, G.** - *Hacking Exposed Fifth Edition: Network Security Secrets & Solutions*, McGraw Hill/Osborne, New York, 2005
3. **Mitnick, K., Simon, W.** - *Arta de a stoarce informații,* Ed. Teora, București, 2005
4. **Taylor, P.** - *Hackers*, Routledge, London, 1999

Cărţi tehnice:

1. ***** (Microsoft)** - *Microsoft Solutions for Security*, 2003
2. **Banks, M.** - *PC Confidential*, Ed. BIC All, București, 2001

Criptografie:

1. **Loepp, S., Wootters, W.** - *Protecting Information. From Classical Error Correction to Quantum Cryptography*, Cambridge University Press, 2006
2. **Patriciu, V.V., Ene-Pietroșanu, M, Bica, I., Priescu, J.** - *Semnături electronice și securitate informatică. Aspecte criptografice, tehnice, juridice și de standardizare*, Ed. BIC All, București, 2006
3. **Stamp, M.** - *Information Security. Principles and Practices*, Wiley-Interscience, John Wiley&Sons, New Jersey, 2005

Securitatea informației la nivel internațional:

1. **Chen, H. &al**. - *Intelligence and Security Informatics (WISI 2006 International Workshop Proceedings)*, Springer, 2006
2. **Chen, H**. - *Intelligence and Security Informatics for International Security. Information Sharing & Data Mining*, Springer, 2006