

Dumitru Oprea

PROTECȚIA ȘI SECURITATEA SISTEMELOR INFORMAȚIONALE

SUPPORT DE CURS

2017

Cuprins

Cuprins	2
Prefață	6
CAPITOLUL I Cadrul general al protecției și securității sistemelor informaționale	7
1.1 Scurtă istorie modernă a (in)securității informațiilor	7
1.2. Particularități ale securității sistemelor informaționale	15
1.2.1 Vulnerabilitatea microcalculatoarelor	18
1.2.2 Forme de manifestare a pericolelor în sistemele informaționale	20
1.2.3 Asigurarea securității sistemelor informaționale	23
1.3 Mecanisme de apărare – prezentare generală	25
Rezumat	26
CAPITOLUL II Protecția informațiilor prin clasificarea lor	28
2.1 Forme embrionare de protejare a informațiilor	28
2.2 Începuturile clasificării moderne a informațiilor	29
2.3 Clasificarea informațiilor	31
2.3.1 Informații subiective	31
2.3.2 Informații obiective	31
2.3.3 Informații tehnice, văzute ca secrete obiective	32
2.3.5 Secrete subiective, secrete obiective și secrete comerciale	32
2.3.6 Determinarea necesității clasificării informațiilor	33
2.4 Clasificarea asocierilor de informații	35
2.5 Clasificarea compilărilor de informații	35
2.6 Declassificarea și degradarea informațiilor clasificate	36
2.7 Principiile clasificării informațiilor și legea secretului comercial	37
2.8 Principiile protejării informațiilor speciale	38
2.9 Protejarea suporturilor informaționale	39
2.9.1 Marcarea materialelor cu regim special	40
2.9.2 Păstrarea și distrugerea materialelor speciale	40
2.10 Clasificarea informațiilor organizațiilor	41
2.10.1 Criterii de clasificare a informațiilor	42
2.10.2 Procedurile de clasificare a informațiilor	42
2.10.3 Roluri și responsabilități în procesul de clasificare a informațiilor	42
Rezumat	44
CAPITOLUL III Controlul accesului în sistemele informaționale	46
3.1 Tipuri de control al accesului în sistem	46
3.2 Identificarea și autentificarea	48
3.2.1 Principii de bază ale controlului accesului	49
3.2.2 Controlul accesului prin obiecte	50

3.2.3 Controlul accesului prin biometrie	51
3.2.4 Controlul accesului prin parole	53
3.2.5 Controlul geografic al accesului în sistem	55
Rezumat	56

CAPITOLUL IV Politici, standarde, norme și proceduri de securitate 57

4.1 Modele de politici de securitate	57
4.1.1 Modele de securitate multinivel	57
4.1.2 Modele ale securității multilaterale	61
4.2 Programul de securitate	63
4.2.1 Politicile	63
4.2.2 Standardele, normele și procedurile de securitate	64
4.2.3 Aspecte practice ale politicii de securitate informațională	65
4.2.4 Exemple de politici de securitate	70
Rezumat	74

CAPITOLUL V Criptografia 75

5.1 Concepte de bază	75
5.2 Scurt istoric al criptografiei	76
5.3 Tehnologii criptografice	77
5.3.1 Substituția	77
5.3.2 Transpoziția (permutarea)	79
5.3.3 Cifrul lui Vernam	80
5.3.4 Cifrul carte	80
5.3.5 Codurile	81
5.3.6 Ascunderea informațiilor	81
5.4 Sisteme de criptare prin chei secrete (simetrice)	88
5.4.1 Sistemul DES	88
5.4.2 Sistemul AES	89
5.4.3 Cifrul IDEA	89
5.5 Sisteme de criptare prin chei publice (asimetrice)	89
5.5.1 Schimbul de chei Diffie-Hellman	90
5.5.2 RSA	91
5.5.3 Semnătura digitală	93
5.5.4 Sisteme de certificare a cheilor publice	95
5.5.5 Infrastructura cheilor publice (PKI)	95
5.6 Atacuri criptografice	96
Rezumat	98

CAPITOLUL VI Asigurarea securității sistemelor informaționale publice și private 99

6.1 Securitatea locului de amplasare a centrelor de prelucrare a datelor	99
6.1.1 Alegerea amplasamentului centrelor de calcul	99
6.1.2 Proiectarea centrului de calcul	100
6.1.3 Protecția și securitatea mediului de lucru al calculatoarelor	101
6.2 Securitatea echipamentelor	102
6.2.1 Asigurarea echipamentelor împotriva intențiilor de modificare a lor	103
6.2.2 Controlul integrității echipamentelor	104
6.2.3 Proceduri de întreținere a echipamentelor	104

6.2.4 Toleranța la cădere a echipamentelor _____	105
6.2.5 Contractele _____	106
6.3 Securitatea software-ului _____	107
6.3.1 Obiectivele securității prin software _____	107
6.3.2 Limitele softului pentru asigurarea securității _____	107
6.3.3 Măsuri generale de asigurare a securității softului _____	108
6.4 Securitatea personalului _____	109
6.4.1 Responsabilități manageriale pe linia personalului _____	113
6.4.2 Măsuri pe linia securității din punct de vedere al personalului _____	114
6.5 Securitatea la nivelul întregului sistem informatic _____	118
6.5.1 Izolarea sistemelor informatice _____	119
6.5.2 Controlul accesului sistemelor informatice _____	120
6.5.3 Detecția amenințărilor și supravegherea sistemului _____	121
6.5.3.1 Urmărirea amenințărilor _____	121
6.5.3.2 Analiza tendințelor _____	122
6.5.3.3 Investigarea _____	123
6.5.3.4 Aspecte generale privind controlul și auditarea sistemelor informatice _____	125
6.5.3.5 Acțiunile de răspuns _____	125
6.5.3.6 Infracții tipice ai sistemelor informatice _____	126
6.5.4 Integritatea sistemelor _____	127
6.5.4.1 Securitatea programelor _____	127
6.5.4.2 Protecția funcțiilor securității _____	127
6.5.5 Înregistrarea activităților efectuate și a măsurilor de securitate _____	128
6.6 Măsuri administrative pe linia securității sistemelor _____	130
6.6.1 Securitatea sectorului public _____	130
6.6.2 Securitatea sistemelor informaționale din domeniul privat _____	131
6.6.2.1 Obligațiile contabilului șef _____	131
6.6.2.2 Obligațiile secretariatului și oficiului juridic _____	131
6.6.2.3 Rolul vicepreședintelui cu probleme administrative _____	132
6.6.2.4 Organizarea securității firmelor _____	132
6.6.3 Responsabilități intra-organizaționale pe linia prelucrării automate a datelor _____	132
6.6.3.1 Responsabilitățile directorului sistemului de prelucrare automată a datelor _____	132
6.6.3.2 Obligațiile responsabilului cu securitatea _____	133
6.6.3.3 Controlul accesului la elementele patrimoniale _____	133
6.6.3.4 Urmărirea respectării măsurilor de securitate _____	134
6.6.3.5 Principii administrative privind responsabilitățile de securitate _____	134
Rezumat _____	136
CAPITOLUL VII Securitatea telecomunicațiilor _____	137
7.1 Interceptarea conversațiilor _____	137
7.1.1 Telefoanele standard _____	138
7.1.2 Securitatea celulelor _____	141
7.1.3 Securitatea telefoanelor portabile _____	144
7.1.4 Securitatea poștei vocale (Voice Mail, V-Mail) _____	144
7.1.5 Securitatea robotului telefonic _____	145
7.1.6 Interfonul casei și supraveghetorii de copii (<i>Baby Monitors</i>) _____	145
7.2 Securitatea transmisiilor _____	146
7.3 Securitatea radiațiilor _____	147
7.3.1 Cadrul general al radiațiilor necontrolate _____	147
7.3.2 Măsuri elementare de precauție împotriva captării radiațiilor necontrolate _____	149
7.3.3 Echipamente de testare a existenței radiațiilor de date _____	149

7.4 Securitatea tehnică	150
7.4.1 Metode de apărare împotriva supravegherii tehnice	150
7.4.2 Tipuri de dispozitive intrus	152
Rezumat	153
CAPITOLUL VIII Aspecte juridice privind protecția și securitatea sistemelor informaționale	154
8.1 Legislația în România	154
8.2 Protecția prin patente, copyright și mărci înregistrate	171
8.2.1 Patentele la nivelul Oficiului European de Patente (EPO – European Patent Office)	172
8.2.2 Copyright-ul	173
8.2.3 Protejarea mărcilor înregistrate	177
8.2.4 Licențele	177
8.2.5 Măsuri tehnice de protecție a licenței software-ului	183
Rezumat	186
Bibliografie generală	187
Referințe Internet	188
Bibliografie disponibilă în biblioteca FEAA	189

Prefață

Informația, a treia formă de manifestare a Existenței Fundamentale, la confluența dintre milenii, a devenit cea mai apreciată comoară a omenirii. Cu mult temei, s-a făcut afirmația de către japonezi că fericirii stăpâni ai informației de la sfârșitul secolului XX vor fi și stăpânii lumii. Nu energiile controlate de om, oricât de puternice ar fi ele sau efectele lor, nu aurul și alte averi materiale, sub orice formă ar exista acestea, ci informația va fi semnul puterii. Așadar, nu sceptorul de aur, ci aureola informațională. 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 și mesajul de suflet al lui Gabriel Garcia Marquez. Iată ce ar face marele scriitor, dacă Dumnezeu i-ar mai dăruia o bucată de viață: *„Aș da valoare lucrurilor mărunte, dar nu pentru ce valorează ele, ci mai curând pentru ceea ce ele semnifică ...; de-abia acum înțeleg că pentru fiecare minut în care închidem ochii pierdem șaiszeci de secunde de lumină. Aș merge în timp ce alții ar sta pe loc, aș rămâne treaz în timp ce toți ceilalți ar dormi. Aș asculta în timp ce alții ar vorbi ...”*. Doamne, cât respect pentru lumina minții, care este informația. Și cum să nu fie protejată pe măsură!?!

În sprijinul afirmațiilor noastre vin preocupările privind protecția și securitatea informațiilor, care datează de mii de ani. Cu riscul de a intra în contradicție 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 protecție și securitate a informațiilor începe în urmă cu peste zece mii de ani. Ne referim la primul protocol de securitate a informațiilor, realizat de mesopotamieni, devenit ulterior, la o altă scară, standard internațional. Peruvianii, prin quippos-urile lor, au făcut același lucru, în urmă cu șase mii de ani. Egiptenii, acum cinci mii de ani, indirect, au introdus conceptul de clasificare a informațiilor, interzicând preoților să scrie pe pământul reavăn, din dorința de a nu se face publice informațiile cu caracter secret. De asemenea, de multe mii de ani, informațiile sensibile au fost ascunse privirilor curioase, de cele mai multe ori rău intenționate, prin operațiunea de camuflare a lor, sau au fost plasate printre informațiile obișnuite, prin steganografie, sau au fost codificate, criptate – pentru a le face accesibile doar persoanelor autorizate. Acestor tehnici li s-au adăugat multe altele, cu același scop, tănuirea informațiilor secrete.

Acum, la începutul mileniului trei, prea multe nu s-au schimbat pe planul operațiilor de protejare și securizare a informațiilor, ci doar tehnicile și mediile de lucru, firesc, sunt altele. Până și tradiționalul sistem bazat pe un calculator central a devenit desuet, vorbindu-se în orice colț al planetei despre Internet, Intranet, Extranet, despre includerea în structura lor a calculatoarelor personale (PDA), a diverselor generații de telefonie și multe altele, inclusiv despre rețeaua rețelelor, ceea ce dă noi dimensiuni spațiului cibernetic. Pe planul globalizării, o tendință este evidentă, a preocupărilor comune, public-privat, pentru securizarea spațiului cibernetic global, îndeosebi după 11 septembrie 2001. Dependența de informație este tot mai mare, chiar periculoasă. Sunt state care depind total de informațiile oferite de componentele spațiului cibernetic național. Blocarea acestuia timp de câteva ore poate să conducă la instaurarea haosului în țara respectivă, afectând, în bună măsură, și securitatea sistemului informațional global planetar.

Prin diferite niveluri de detalieri, cam toate aspectele menționate mai sus își găsesc un tratament adecvat în cartea de față. Tocmai datorită acestui lucru, ea poate fi utilă și accesibilă, integral sau în parte, mai multor categorii de cititori. Printre ei, cu siguranță, se vor afla elevi și studenți, profesori și cercetători, specialiști din diferite domenii, dar și omul de rând.

Tuturor cititorilor, indiferent de grupul de apartenență, le mulțumim anticipat pentru exprimările de păreri sau pentru propunerile de îmbunătățire a ediției de față.

Autorul
Iași, 2016

CAPITOLUL I

Cadrul general al protecției și securității sistemelor informaționale

Orice material publicat sub titlul „Protecția și securitatea informațiilor”, la o analiză mai atentă, este destul de derutant, întrucât în lumea afacerilor s-ar putea vorbi cu mai multă ușurință despre ... insecuritatea datelor decât despre securitatea lor. Mai mult, nici nu se pune problema că uneori și prea multă informatizare este dăunătoare. Din momentul conștientizării utilizatorilor de avantajele folosirii calculatoarelor, o mulțime de organizații au declanșat un imens proces de re tehnologizare informațională, raportând cu satisfacție ce investiții masive au făcut în tehnica de calcul. Sunt și cazuri de informatizare cauzate de „modă”, fără să fie luate în seamă riscurile acestui proces.

În acest spirit, capitolul de față dorește să-și convingă cititorii că:

- averile informaționale sunt foarte importante în activitatea organizațiilor mai mici și mai mari, iar preocupările pe linia asigurării securității lor, deși există din cele mai vechi timpuri, s-au intensificat o dată cu dezvoltarea tehnicii de calcul;
- există o gamă largă de pericole și vulnerabilități asociate acestor averi, iar ea se extinde simultan cu dezvoltarea tot mai rapidă a tehnologiilor informaționale și de comunicații;
- securitatea averilor informaționale este o componentă de bază a ecuației succesului organizațional și o problemă mai degrabă umană decât tehnică, posibil de rezolvat cu mijloace ieftine.

1.1 Scurtă istorie modernă a (in)securității informațiilor

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

Insecuritatea, amintită anterior, rezidă și din faptul că orice persoană care dialoghează cu calculatorul unei firme, fie prin multitudinea tipurilor de rețele, fie prin sistemele de poștă electronică (e-mail) sau prin intermediul dischetelor, CD-urilor, DVD-urilor, USB-urilor, al benzilor magnetice sau al altor suporturi de informații, aduse din afara unității, sau prin scrierea unor programe cu rol special, poate să facă următoarele lucruri: să copieze fișierele importante ale altor firme, să influențeze evidențele altora pentru a le cauza pierderi, să reprogrameze calculatoarele incluse în configurația sistemelor de producție pentru a provoca avariile utilajelor sau pentru producerea accidentelor umane (inclusiv uciderea lor), să șteargă programe sau fișiere și multe altele.

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

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

- generația a II-a, securitatea sistemelor distribuite;
- generația a III-a, securitatea microcalculatoarelor, inclusiv a rețelelor locale;
- generația a IV-a, securitatea Internetului;
- generația a V-a, securitatea comerțului și afacerilor electronice;
- generația a VI-a, securitatea comerțului și afacerilor mobile;
- generația a VII-a, securitatea globală a lumii virtuale, a întregului spațiu cibernetic.

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

- securitatea datelor;
- securitatea datelor și informațiilor;
- securitatea datelor, informațiilor și cunoștințelor.

Prin această ultimă prezentare, am intenționat să surprindem trecerea de la societatea preocupată de creșterea performanțelor prin colectarea mai rapidă a datelor, la societatea informațională a zilelor noastre, până la societatea ce se conturează în mileniul III, a cunoașterii.

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

Dacă, din curiozitate, veți accesa www.attrition.org, veți afla cât de vulnerabile sunt până și site-urile marilor corporații. 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.

Soluția? 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 veți 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 vieții noastre, a tuturor. Despre aspectele securității sistemelor informaționale, pe plan mondial, s-au scris o mulțime de cărți, s-au ținut conferințe sau seminarii internaționale, dar s-a făcut încă puțin pentru transpunerea lor în practică. Mulți cred că n-au nevoie de ea sau consideră că necazurile se pot ține doar de alții.

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

Preocupări deosebite pe linia securității 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 naționale și internaționale, cu un astfel de obiectiv. Au apărut numeroase cărți, inclusiv cursuri universitare, cu teme apropiate, cum ar fi *Criptografia și securitatea datelor*, curs predat din anii 1970 la Universitatea George Washington, *Securitatea datelor și informațiilor și contabilitatea analitică*, la universitățile din Delaware și Ohio. Rezultate remarcabile a înregistrat și Universitatea din Ontario de Vest, din Canada. Ulterior, în Europa, rețeaua specialiștilor în securitatea sistemelor informaționale s-a extins din Anglia în

Olanda, Belgia, Suedia, Germania, cuprinzând întreaga arie a țărilor puternic dezvoltate. În numeroase țări se predau cursuri universitare care conțin tematici apropiate ca formulare, dar toate au un obiectiv comun: securitatea informațiilor în sistemele de prelucrare automată a datelor. Ca efect, în universități se creează diverse grupuri de inițiați în domeniu, cei mai reprezentativi fiind experții sau realizatorii de sisteme expert pentru verificarea securității, analiza riscului și evaluarea potențialelor pagube, sau producătorii de software specializat în auditarea sistemelor informaționale.

Din anul universitar 1999/2000, la Georgetown University, se predă cursul *Războiul informațional și securitatea* pentru studenții din diverse domenii, cum ar fi cei de la politici internaționale, de la administrație publică, administrarea afacerilor, comunicare, științe exacte și în toate domeniile socio-umane.

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

La nivel internațional, semnificativă este constituirea, încă din 1960, a **IFIP** (International Federation for Information Processing = Federația Internațională pentru Prelucrarea Informațiilor), creată sub auspiciile UNESCO, care reunește cadrele didactice și alți specialiști preocupați de prelucrarea informațiilor, în număr de peste 3500. Din ea fac parte organizații din 58 de țări 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 tehnice¹ sunt:

TC1 – Bazele științei calculatoarelor

TC2 – Software: teorie și practică

TC3 – Educație informatică

TC4 - neatribuită

TC5 – Aplicații în tehnologia informatică

TC6 – Sisteme de comunicații

TC7 – Modelarea și optimizarea sistemelor

TC8 – Sisteme informaționale (comisia cea mai puternică), cu 7 grupuri de lucru:

WG8.1 Evaluarea și proiectarea sistemelor informaționale

WG8.2 Interacțiunea sisteme informaționale – organizație

WG8.3 Sisteme de sprijinire a procesului decizional

WG8.4 Afaceri electronice (E-Business: cercetare și practică multidisciplinară)

WG8.5 Sisteme informaționale în administrația publică

WG8.6 Difuzia, transferul și implementarea tehnologiilor informaționale

WG8.7 – neatribuit

WG8.8 Carduri inteligente, tehnologie, aplicații și metode

WG8.9 Sisteme informaționale ale întreprinderilor

TC9 – Relația calculatoare - societate

TC10 – Tehnologia sistemelor electronice de calcul

TC11 – *Protecția și securitatea în sistemele de prelucrare a informațiilor*, cu următoarele grupuri de lucru:

WG11.1 Managementul securității informațiilor

WG11.2 Securitatea sistemelor omniprezente (*Pervasive Systems Security*)

WG11.3 Securitatea datelor și aplicațiilor

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

- WG11.4 Securitatea rețelelor și sistemelor distribuite
- WG11.5 Integritatea și controlul sistemelor – dizolvat în 2007
- WG11.6 Managementul identității
- WG11.7 Tehnologii informaționale: Abuzurile și cadrul legal
- WG11.8 Educația în domeniul securității informațiilor
- WG11.9 Criminalistică în mediul digital (*Digital Forensics*)
- WG11.10 Protecția infrastructurilor critice
- WG11.11 Managementul încrederii (*Trust Management*)
- WG11.12 Aspecte umane ale securității și asigurării informaționale
- WG11.13 Cercetări în domeniul securității sistemelor informaționale

TC12 – Inteligența artificială

TC13 – Interacțiunea om-calculator

TC14 – Utilizarea informaticii în divertisment (*Entertainment Computing*)

Pentru a ne edifica asupra rolului unor astfel de organizații, vom face o descriere succintă a grupurilor de lucru din comisia tehnică *TC11 – Protecția și securitatea în sistemele de prelucrare a informațiilor*, evidențiind scopul înființării și obiectivele urmărite de fiecare dintre ele.

Comisia TC11 a fost înființată în 1984.

Scopul ei este de creștere a siguranței și încrederii în informațiile prelucrate automat, precum și cel de constituire a unui forum al responsabililor cu securitatea și al altor specialiști care activează în domeniul securității sistemelor de prelucrare a informațiilor.

Obiectivele urmărite sunt:

- stabilirea unui cadru comun de referință pe linia securității, pentru organizații, specialiști și publicul interesat;
- promovarea protecției și a securității ca o componentă esențială a sistemelor de prelucrare a informațiilor.

Grupul de lucru WG11.1 – Managementul securității informațiilor, înființat în 1985 și revizuit în 1992.

Scopul: crearea unui cadru managerial pe linia securității sistemelor informaționale ale organizațiilor, identic celui din domeniul financiar-contabil.

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

Obiectivele grupului sunt:

- studierea și promovarea metodelor de sensibilizare a factorilor de decizie pe linia acordării unei importanțe deosebite valorii informațiilor, considerându-le la fel de importante ca și valorile patrimoniale, obligându-i să ia toate măsurile necesare pentru protejarea noilor valori;
- studierea și promovarea metodelor și căilor de măsurare și evaluare a nivelului securității dintr-o organizație și sensibilizarea conducerii despre importanța acestora;
- cercetarea și realizarea de noi căi de identificare a amenințărilor și vulnerabilității sistemelor din orice organizație;
- cercetarea și realizarea influenței noilor echipamente și produse software asupra managementului securității informaționale;
- studierea și dezvoltarea mijloacelor și căilor pentru a veni în sprijinul managerilor cu securitatea informațiilor, prin evidențierea eficienței muncii lor și a calității controlului exercitat în unitate;
- fixarea standardelor pe linia securității informațiilor.

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

Scopul său este să identifice metodele și problemele din domeniul securității informațiilor, în particular al celor privind sistemele omniprezente - definite ca fiind sistemele ce includ calculatoarele personale, rețelele locale, dispozitivele mobile, etichetele RFID², nodurile de senzori și alte configurații similare, conectate wireless, în care nu există echipamente anume pentru administrarea securității, iar utilizatorul final este singurul ce se ocupă de protecția sistemului.

Grupul de lucru WG11.3 – Securitatea datelor și aplicațiilor, creat în 1987 și revizuit în 2001.

Scopul:

- să promoveze pe o scară cât mai largă înțelegerea riscului la care se expun societățile bazate pe sistemele de operare ale bazelor de date cărora le lipsesc măsurile adecvate pe linia securității și integrității datelor;
- să încurajeze aplicarea tehnologiilor existente pentru îmbunătățirea securității sistemelor bazelor de date.

Obiective:

- promovarea tehnologiilor care sprijină definirea cerințelor pe linia securității pentru sistemele bazelor de date;
- proiectarea, implementarea și exploatarea sistemelor bazelor de date care să aibă incluse și funcții de securitate;
- asigurarea că sistemele bazelor de date implementate satisfac și cerințele de securitate.

Grupul de lucru WG 11.4 – Securitatea rețelelor, constituit în 1985, revizuit în 1992, 1997 și 2003.

Scopul:

- să studieze și promoveze procesele acceptate internațional care să permită echipelor de conducere și specialiștilor să înțeleagă deplin responsabilitățile ce le revin pe linia exploatarea cu încredere și în condiții de securitate a rețelelor informaționale, care vin în sprijinul organizațiilor, clienților acestora sau publicului larg;
- să studieze și promoveze educația și instruirea pe linia aplicării principiilor, metodelor și tehnologiile de securitate a rețelelor.

Obiectivele sunt:

- promovarea stărilor de încredere și înțelegere a aspectelor privind rețelele din punct de vedere al securității sistemelor informaționale;
- asigurarea unui forum pentru discuții, înțelegerea și clarificarea tuturor aspectelor ce țin de securitatea rețelelor;
- studierea și identificarea aspectelor manageriale, procedurale și tehnice ale securității rețelelor;
- studierea și descrierea riscurilor apărute în contextul includerii sistemului informațional într-un mediu bazat pe rețele;
- promovarea tehnologiilor și practicilor care să asigure controlul securității rețelelor, să facă posibilă definirea cerințelor securității rețelelor și, în general, să avanseze constituirea cadrului de bază pentru o securitate eficientă a rețelelor;
- să contribuie, în măsura în care este fezabil și posibil, la standardizarea internațională a securității rețelelor.

² Radio Frequency IDentification

În noul context, aspectele securității depășesc frontierele organizației, întrucât se intră în legătură cu o mulțime de alte sisteme externe, regăsite prin rețelele locale, metropolitane sau internaționale. În aceste rețele se includ conectările dial-up (telefonice) sau de alte tipuri care permit angajaților să lucreze de acasă, dar și conexiunile ce-i permit organizației să efectueze operațiuni bazate pe legături reciproce, astfel încât acestea să aibă loc în cadrul acordurilor EDI sau ale comerțului electronic.

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

Scopul:

- să promoveze, prin educație și cercetare, conștientizarea și înțelegerea următoarelor concepte: managementul identității (aplicații și metodologii, securitatea documentelor optice și electronice, rolul și funcțiile actuale și potențiale ale biometriei), metodele și tehnicile care sprijină evaluarea unor tehnologii biometrice particulare (aspecte operaționale și legale ale biometriei, impactul său asupra societății) și managementul identității naționale (printre altele, și rolul acestuia în combaterea fraudei, terorismului și delictelor internaționale).

Obiectivele grupului:

- stabilirea și promovarea unui lexic comun pentru problemele legate de managementul identității, astfel încât întreaga comunitate interesată să vorbească aceeași limbă;
- propunerea, definirea și elaborarea de metodologii și aplicații ale managementului identității, care să răspundă standardelor formulate de responsabili cu deciziile din sectorul public și privat;
- propunerea, definirea și elaborarea tehnologiilor de securitate ale documentelor optice și electronice, care să răspundă standardelor formulate de responsabili cu deciziile din sectorul public și privat;
- propunerea, definirea și elaborarea de metodologii și tehnologii biometrice, care să fie încorporate în managementul identității (naționale) și care să răspundă standardelor formulate de responsabili cu deciziile din sectorul public și privat;
- promovarea, prin educație și cercetare, a unei largi înțelegeri a aspectelor sociale și operaționale legate de managementul identității naționale în general și de tehnologiile menționate mai sus în particular.

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

Scopul:

- să analizeze amenințările existente și în curs de apariție pe linia tehnologiilor informaționale, precum și a riscurilor la care se expun oamenii, organizațiile și societatea;
- să analizeze principiile securității;
- aspecte ale impactului tehnologiilor informaționale asupra cadrului legal existent, ce poate fi învechit față de noul mediu;
- să analizeze mijloacele, cadrul legal, standardele etice, procedurile manageriale, precum și alți factori sociali aplicabili în domeniul tehnologiilor informaționale;
- să identifice soluții posibile;
- să depisteze noi consecințe legale, sociale și organizaționale ale dezvoltării și utilizării sistemelor tehnologiilor informaționale.

Obiectivele grupului sunt:

- consolidarea relațiilor de cooperare dintre comunitățile tratate în comisiile „Calculatoarele și societatea” și „Securitatea informațiilor” pe problematica folosirii inadecvate a tehnologiilor informaționale și cadrul legal;
- dezvoltarea echipelor orientate spre studierea:

- amenințărilor prezente din domeniul tehnologiilor informaționale și cadrul legal adecvat;
- riscul la care sunt expuși oamenii și organizațiile din cauza acestor amenințări;
- responsabilitățile oamenilor și organizațiilor pe linia legalității utilizării tehnologiilor informaționale;
- riscul înregistrării unor nesincronizări între prevederile legale, tehnice și manageriale;
- impactul tehnologiilor informaționale asupra cadrului juridic existent;
- să propună și/sau să evalueze prevederile legale pe linia combaterii amenințărilor la care sunt expuse tehnologiile informaționale.

Grupul de lucru WG 11.8 – Educația în domeniul securității informațiilor, constituit în 1991.

Scopul:

- să promoveze educația și instruirea pe linia securității informațiilor la nivel de universitate, guvern și întreaga economie.

Obiective:

- crearea unui centru de resurse internaționale pentru schimbul de informații privind educația și instruirea în securitatea informațiilor;
- realizarea de modele de cursuri de securitate a informațiilor la nivel de universități;
- încurajarea facultăților și universităților să includă modele de cursuri adecvate pe linia securității informațiilor, la nivel universitar și postuniversitar, prin disciplinele de informatică, sisteme informaționale și servicii publice;
- realizarea de module de securitate a informațiilor care să poată fi integrate în planurile de învățământ ale școlilor de afaceri și/sau în cursurile introductive de informatică la nivel de facultăți și universități;
- promovarea unui modul adecvat despre securitatea informațiilor pentru facultăți, universități, economie și organizații guvernamentale;
- colectarea, transmiterea și difuzarea de informații privind cursurile de securitate a informațiilor prin intermediul organizațiilor private în folosul întregii economii;
- colectarea și difuzarea periodică a bibliografiei cărților de securitate a informațiilor, articolelor, rapoartelor și altor suporturi educaționale.

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

Scopul:

- să promoveze, prin educație și cercetare, conștientizarea și înțelegerea:
 - metodelor și tehnicilor științifice capabile să stabilească circumstanțele producerii unui incident informatic (ce, când, cum s-a întâmplat, cine a fost autorul și care au fost consecințele incidentului), în vederea inițierii unei acțiuni legale;
 - aspectelor legale și operaționale ale tehnologiilor noi, capabile să ajute dezvoltarea de asemenea metode și tehnici.

Obiective:

- stabilirea și promovarea unui lexic comun pentru problemele legate de criminalistica în mediul digital, astfel încât întreaga comunitate internațională să vorbească aceeași limbă;
- propunerea, definirea și elaborarea de tehnologii care să sprijine tribunalele și alți factori de decizie din mediul civil și militar prin probe digitale credibile;
- promovarea, prin educație și cercetare, a unei înțelegeri cât mai ample a aspectelor legale, operaționale și sociale legate de criminalistica în mediul digital;
- sprijinirea cooperării între comunitățile internaționale, pentru a le implica în discuții academice privind cercetarea în domeniul criminalisticii digitale și a aplicațiilor acesteia.

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

Scopul:

- sprijinirea colaborării între știință, tehnologie și politică, pentru a dezvolta și implementa soluții sofisticate și practice în același timp, care vor duce la securizarea averilor informaționale în sectoarele critice. Grupul dorește să întărească protecția infrastructurii informaționale la toate nivelurile – local, regional, național și internațional – prin cercetare, dezvoltare și educație.

Obiective:

- identificarea aspectelor de securitate informaționale comune sectoarelor infrastructurii;
- stabilirea interdependențelor dintre infrastructuri și importanța asigurării securității lor;
- identificarea principiilor și tehnicilor de securitate care pot fi aplicate pentru protecția infrastructurilor critice;
- dezvoltarea de soluții mixte de protecție a infrastructurilor, care să înglobeze metode științifice, tehnici de inginerie și 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 siguranței și credibilității infrastructurii de calcul globale. Disciplinele implicate provin atât din zona tehnică, cât și din domenii ca dreptul, științele sociale și filosofia.

Obiective:

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

Despre grupurile de lucru WG11.12 - *Aspecte umane ale securității și asigurării informaționale* și WG11.13 *Cercetări în domeniul securității sistemelor informaționale* nu există, deocamdată, informații detaliate pe site-ul IFIP.

În 1974, s-a înființat Institutul pentru Securitatea Calculatoarelor (*Computer Security Institute – CSI* –, cu site-ul www.gocsi.com) pentru formarea și perfecționarea continuă a specialiștilor în securitatea informațiilor, a calculatoarelor și a rețelelor.

În anul 1990, Comitetul pentru Informații, Calculatoare și Politici de Comunicație ale Organizației pentru Cooperare și Dezvoltare Economică (OECD) a constituit un grup de experți pentru a pregăti ghidul securității sistemelor informaționale. În octombrie 1992, s-a realizat *Ghidul pentru securitatea sistemelor informaționale*, iar, în noiembrie 1992, cele 24 de țări membre ale OECD l-au aprobat. Obiectivul de bază l-a constituit crearea unui cadru de bază care să înlesnească dezvoltarea și introducerea mecanismelor, practicilor și a procedurilor pentru asigurarea securității sistemelor informaționale. Ghidul se adresa tuturor sistemelor informaționale din sectorul public și privat, supuse jurisdicției naționale, prin enunțarea a nouă principii de bază: responsabilitate, conștientizare, etică, multidisciplinaritate, proporționalitate, integrare, oportunitate, reevaluare periodică, democrație.

De asemenea, la nivelul anului 1990, Consiliul Cercetării Naționale al SUA, printr-un raport special, *Computer at Risk (CAR)*, prezenta starea securității sistemelor informaționale din SUA și recomanda șase seturi de acțiuni. Prima recomandare se referea la crearea și promulgarea *principiilor general acceptate de securitate a sistemelor* (Generally Accepted System Security Principles, GASSP). Recomandarea pentru crearea GASSP a condus la înființarea, la sfârșitul anului 1992, a *Fundației Internaționale pentru Securitatea Informațiilor*.

În 1997, comitetul GASSP, care era format din experți în securitatea informațiilor din zece țări, inclusiv SUA, a lansat GASSP, versiunea 1.0, care conține nouă principii de bază, referite

ca principii universale, bazate pe principiile OECD. În același timp, Institutul Național de Standarde și Tehnologie din SUA a emis un raport cu aceleași nouă principii, aplicabile la nivelul organismelor guvernamentale federale.

Menționăm și 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 țări membre. Acestea erau Australia, Belgia, Canada, Danemarca, Franța, Germania, Grecia, Italia, Japonia, Luxemburg, Marea Britanie, Norvegia, Olanda, Portugalia, Spania, Statele Unite ale Americii, Turcia. Ca membri asociați erau Austria, Coreea de Sud, Elveția, Finlanda, Irlanda, Noua Zeelandă, Polonia, Singapore, Slovacia, Suedia, Taiwan și Ungaria – în total 12 țări. Scopul principal îl constituie restricționarea exporturilor spre anumite țări, cum ar fi Libia, Irak, Iran, Coreea de Nord – considerate a fi țări ce sprijină mișcările teroriste. Exporturile spre alte țări erau permise, însă pe bază de licențe.

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 țărilor membre. De asemenea, erau acceptate exporturile criptografice folosite pentru autentificare, inclusiv produsele folosite pentru criptarea parolelor. Toate țările membre au respectat Nota, cu excepția SUA, Marea Britanie și Franța.

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

Deci, dacă de peste patru decenii sunt preocupări pe linia securității informațiilor prelucrate în sistemele de prelucrare automată, prin cursuri universitare, cărți, simpozioane ș.a., dacă pe plan internațional există atâtea organisme care se ocupă de problematica menționată, considerăm firescă abordarea și la noi, cu mai multă seriozitate, a *Protecției și securității informațiilor*.



Identificați câteva repere istorice (la nivel statal, academic sau organizațional) privind protecția și securitatea informațiilor în România.

1.2. Particularități ale securității sistemelor informaționale

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

În vederea obținerii noilor performanțe, datele prelucrate sunt supuse unor operațiuni suplimentare în faza de culegere, astfel încât să poată fi valorificate ulterior pe mai multe planuri. Prelucrarea datelor din două sau mai multe documente operative în unul sau mai multe fișiere, având suportul de înregistrare specific noii variante de prelucrare, constituie o îndepărtare vizibilă de modul tradițional de păstrare a documentelor primare, de gestionare a lor, și duce la apariția mai multor persoane care pot accesa aceleași date. Mai mult, prin agregarea înregistrărilor anterioare, pot rezulta chiar noi informații.

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

sporește grija asigurării securității lor, întrucât riscul pierderii lor sau al consultării neautorizate este și mai mare. Într-un astfel de caz, nu trebuie uitat principiul dominant al prelucrării automate a datelor, GIGI (Gunoii la Intrare, Gunoii la Ieșire), 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 obține ulterior.

Alt element, deosebit de important, îl constituie factorul uman. Dacă în vechile sisteme erau ușor de controlat locurile de păstrare a informației, acum, într-un mediu puternic informatizat, persoanele cu atribuții de urmărire a modului de realizare a securității 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 reușesc să descopere de unde și cine, cu ajutorul unui calculator aflat la distanță 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 aplicații. Loialitatea excesivă, în acest caz, poate da de gândit.

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

Densitatea informației 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 ușurință într-un buzunar. CD-urile, DVD-urile, cardurile, memoriile flash, hard-discurile portabile și alte suporturi moderne pot fi astfel subtilizate discret, cu eforturi minime dar cu efecte distructive majore.

Obscuritatea sau invizibilitatea constituie o altă problemă, întrucât conținutul documentelor electronice și 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 puși să controleze nu au pregătirea informatică și nici echipamentele necesare pentru a observa o eventuală sustragere de fișiere.

Accesibilitatea datelor din sistemele de calcul este mai mare, cel puțin pentru o nouă categorie de infractori, catalogați „hoți 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. Ștersăturile din vechile documente pentru schimbarea sumelor, precum și adăugările de noi înregistrări „cu creionul” nu mai există, modificările în fișierele electronice sunt efectuate cu multă lejeritate și foarte greu de depistat ulterior.

Remanența suporturilor, după ce au fost șterse, poate constitui o cale sigură de intrare în posesia informațiilor memorate anterior. Se cunosc numeroase programe de restaurare a fișierelor șterse.

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

Necunoașterea calculatoarelor. Pentru foarte multe persoane, îndeosebi de vârstă înaintată, calculatorul este investit cu forțe supraomenești, ceea ce le conferă o încredere oarbă în datele obținute prin intermediul lui. De asemenea, din motive de nepricepere, acești anagajați pot fi victime ușoare ale corupătorilor ... informatizați.

Progresul tehnologic. Rezultatele cercetărilor tehnico-științifice se transformă zi de zi în tehnologii din ce în ce mai performante de accesare a datelor. Nu același lucru se poate spune și despre progresele înregistrate în domeniul securității datelor.

Comunicațiile și rețelele, devenind tot mai performante, au extins aria utilizatorilor, atât din punct de vedere numeric, cât și al dispersiei în teritoriu, întregul spațiu terestru fiind accesibil

rețelelor foarte mari. Odată cu noile progrese, și aria utilizatorilor rău intenționați s-a mărit, precum și variantele de furt informatizat.

Integrarea puternică a sistemelor apare ca o consecință a îmbunătățirii formelor de comunicație și a proliferării rețelelor de calculatoare. Pe același canal de comunicație 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 fișiere și, implicit, aplicații ale firmei. Comerțul și afacerile electronice au deschis și mai mult apetitul „specialiștilor” în fraudă.

Apariția utilizatorilor finali informatizați constituie un veritabil succes, dar sporește și riscul pierderii datelor importante din calculatorul principal al companiilor.

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

Totuși, 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 și ianuarie 2011, folosind motorul de căutare Google. După cum se observă, se detașează net conceptele: *internet security*, *network security*, *information security*, *computer security*, *data protection*, *digital signature*, *e-security* – în ordinea numărului de apariții în site-uri.

În concluzie, odată cu dezvoltarea noilor sisteme informaționale și cu transferarea către acestea a secretelor firmelor, trebuie văzut în ele, în același timp, ajutorul numărului unu, dar și elementele cele mai tentante pentru noii criminali. Hardul și softul pot fi manevrate cu multă ușurință de către om. În acest caz, ca și în altele intrate în obișnuința cotidiană, „inteligența” calculatorului lasă de dorit, putându-se spune că tot omul (a)sfințește ... calculatorul, motiv esențial pentru sporirea preocupărilor tuturor specialiștilor din domeniul securității sistemelor informaționale.

Tabel nr. 1.1 – Numărul site-urilor ce tratează concepte specifice protecției și securității sistemelor informaționale

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



Propuneți alte concepte relevante pentru domeniul protecției și securității informaționale și completați 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 producția 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.

Apariția milioane de utilizatori a dus la constituirea unei adevărate bresle de specialiști în „butonat” – a se citi apăsarea tastelor –, cu destul de puține cunoștințe despre teoria sistemelor informaționale și cu nici o teamă de implicațiile posibile ale unui sistem fără securitate. De la utilizatorii izolați s-a trecut la constituirea de rețele puternice, care au împânzit orice colț al organizațiilor. Următoarele trepte au constat în depășirea granițelor firmei, ale orașului, respectiv ale țării. S-a creat, astfel, posibilitatea ca sistemele bazate pe calculatoare mari să fie accesate din sute sau mii de locuri, afectând substanțial integritatea, confidențialitatea și accesibilitatea datelor.

Datorită microcalculatoarelor, se poate spune că s-a înregistrat un progres colosal pe linia domeniilor de aplicabilitate ale informaticii. Ele rezolvă rapid și ieftin o mulțime de probleme de planificare tehnico-economică, de exploatare, de administrare, procesare de texte, comunicații și alte facilități de lucru în rețea. În aceste condiții, microcalculatoarele aduc și noi forme de manifestare a slăbiciunii sistemelor electronice de calcul și a vulnerabilității 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 și de copiii și de funcționarii fără prea multe cunoștințe tehnice, aceasta concretizându-se în:
 - a) *aparitia numeroaselor eșecuri sau erori în operațiunea de creare a copiilor de siguranță* – de exemplu, realizarea lor pe suportul intern de memorare al aceluiași microcalculator, chiar pe aceeași partiție de disc;
 - b) *eșecuri în controlul accesului sistemului*. Sistemele de protecție prin parole nu se folosesc la toate microcalculatoarele, iar când există nu sunt folosite corespunzător, parolele fiind cunoscute de mai mulți utilizatori, și nu numai atât, ele aflându-se scrise pe o bucată de hârtie, lipită pe colțul monitorului sau pe masa de lucru;
 - c) *tratarea tuturor datelor la fel*, omițându-se cele de o importanță deosebită, care ar trebui să aibă cu totul alt regim;
 - d) *greșeli în păstrarea și utilizarea resurselor sistemului*. Discurile de orice tip, casetele, benzile sunt împânzite prin toată unitatea, prin toate birourile, putând fi folosite sau sustrase cu multă ușurință de alte persoane. Un suport din afară poate fi introdus printre cele deja existente, strecurându-se astfel și virușii distructivi. Hârtia de imprimantă (de regulă cea care conține mici greșeli sau a doua copie a unei lucrări efectuate în două exemplare), benzile tușate ale acesteia (riboanele), celelalte „resturi” sunt accesibile noilor „scormonitori în gunoaie informatice”, cu scopul de a găsi „un colț de pâine” printre informațiile conținute de aceste materiale;

- e) *scrutarea cu ușurință a sistemului*. Deseori, din pură curiozitate, un coleg, un prieten, un copil venit în vizită la biroul părinților, având cunoștințe limitate despre calculatoare, încep să „se joace” cu tastele unui microcalculator pornit, situație 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 dispoziția specialiștilor, ci și a altor persoane, care nu cunosc prea multe lucruri despre alte tipuri de sisteme. Odată cu apariția microcalculatoarelor, problemele de instruire informatică se pun într-un alt mod;
 3. Prin politica de instaurare a unor restricții în utilizare, apelându-se la sistemul parolelor multiple, din faza de inițializare a sistemului până la accesul la căi și fișiere, se reduce dramatic viteza de prelucrare, deci scade productivitatea sistemului;
 4. Fiind plasate în aproape toate birourile, iar condițiile de păstrare puternic diversificate, riscul defectării este diferit de la un birou la altul;
 5. Resursele întregului sistem fiind împrăștiate prin toate colțurile unității, securitatea tradițională a sălii calculatorului unic dispare, aceasta având ca rezultat:
 - a) documentația sistemului, softul, manualele de utilizare sunt inefficient folosite sau în condiții de risc sporit;
 - b) pierderea cheilor de deschidere a PC-urilor le poate face inutilizabile o perioadă de timp;
 - c) softul de aplicații se realizează în mod haotic, ducând uneori la lucrul în paralel la aceeași problemă, neexistând o evidență 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 săvârșite cu mai multă ușurință și de către mai multe persoane, ceea ce diminuează eficiența controlului;
 7. Prin preluarea de către calculator a activităților prestate anterior de mai multe persoane, posibilitatea de furt, fără complotul mai multor angajați, devine mult mai lejeră;
 8. Persoanele care în condițiile prelucrării clasice aveau grija și posibilitatea de a lucra doar într-un domeniu, destul de limitat, pot să-și extindă aria „cunoașterii” asupra întregii baze de date a unității;
 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 operațiunea este mult mai ușoară;
 10. Sistemele de operare ale microcalculatoarelor nu dispun de aceleași performanțe de protecție precum sistemele mari;
 11. Slaba securitate, însoțită de facilitățile de lucru în rețea, conduce la sporirea posibilităților de accesare neautorizată a sistemului;
 12. Datele pot fi preluate pe un PC fie din rețea, fie din calculatorul mare și 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 rețeaua sau calculatorul central;
 14. Prin dimensiunile lor reduse și greutatea mică, PC-urile sunt ușor de mutat dintr-un loc în altul, ceea ce sporește 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, identificați elemente similare de vulnerabilitate a calculatoarelor portabile și, respectiv, a telefoanelor mobile folosite în organizații.

1.2.2 Forme de manifestare a pericolelor în sistemele informaționale

Datelor supuse prelucrării automate trebuie să li se asigure cel puțin aceleași condiții de protecție ca și celor prelucrate manual. Totuși, din cauza creșterii riscului prin informatizare, așa cum rezultă din descrierea sumară a vulnerabilității noilor sisteme, se impun și unele măsuri suplimentare de realizare a protecției, situație în care utilizatorii trebuie să cunoască în detaliu natura noilor amenințări. Literatura de specialitate le grupează în diverse moduri. Oricum, ele pot fi sintetizate în trei mari categorii:

- amenințări cauzate de incidente ivite în sistem;
- factori naturali, bazați pe hazard;
- amenințarea sistemelor prin acțiunea voită a omului.

1.2.2.1 Amenințări cauzate de incidente ivite în sistem

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

1. *Apariția unor defecțiuni la echipamentele sistemului.* De multe ori micile defecțiuni, în special cele cu o perioadă de manifestare foarte scurtă, sunt mai greu de detectat și 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. *Apariția inevitabilelor erori umane*, conform dictonului „errare humanum est”, conduce la luarea elementarelor măsuri preventive de reducere substanțială a intervenției umane în procesul de prelucrare a datelor cu ajutorul calculatorului electronic. Cauzele erorilor pot fi: indiferența cu care se exercită o anumită operațiune, slaba instruire, entuziasmul excesiv, înțelegerea greșită a modului de funcționare a sistemului. Erorile pot să aparțină operatorilor, dar, și mai grav, programatorilor. Riscul cel mai mare provine din posibilitatea perpetuării modului eronat de exercitare a operațiunilor sau a programării. Soluțiile 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. *Funcționarea defectuoasă a softului.* Chiar și 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 funcție informatică din ministerul apărării, întrucât spunea că pericolul producerii unor grave incidente, cu efecte nebănuite asupra securității omenirii, devine tot mai mare, din cauza imposibilității controlării programelor. Multitudinea ramificațiilor din program poate să ducă la „scurt-circuitarea” lor, generând căi imprevizibile de execuție, concretizate în luarea unor decizii surprinzătoare;
4. *Întreruperea sistemului de alimentare cu energie sau funcționarea lui în afara parametrilor tehnici admiși.* În această categorie intră și “căderea” legăturilor de comunicație, precum și a altor utilități necesare sistemului.

1.2.2.2 Factorii naturali, bazați 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 funcționează eronat sau poate să-și înceteze exercitarea funcțiilor sale. „Cheagurile” calculatoarelor pot fi: exces de umiditate, exces de căldură, praf, fire de păr, scrum de țigară ș.a. Nu sunt de neglijat diversele insecte, îndeosebi muște, fânțari, păianjeni, gândaci, viespi, viermi. Cel mai mare pericol îl reprezintă „mouse”-ul, dar de data aceasta cel adevărat, adică micuțul șoricel.

Tot în această categorie intră cutremurele, vijeliile, furtunile, inundațiile și alte forme de dezlănțuire a naturii.

1.2.2.3 Amenințarea sistemelor prin acțiunea voită a omului

Ca orice avere, și cea informațională stârnește tentații umane, iar regula decalogului, care îndeamnă să „nu furi”, nici în acest caz nu este respectată. S-au constituit, în timp, grupuri de „specialiști” care exploatează slăbiciunile sistemelor. Cel mai grav este faptul că unii realizatori de sisteme sunt și cei mai periculoși dușmani ai propriilor creații, fiind un fel de „Kronoși” ai vremurilor noastre, devorându-și 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 (ascuse).

1. *Spionajul și serviciile secrete* acționează, de regulă, în domeniul militar, dar își fac simțită prezența și în industrie, comerț, învățământ, cercetare ș.a. Căile de obținere a informațiilor 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. *Dușmanii, nedreptățiții și neloyalii dintre angajații firmei.* Această categorie nu apelează la tehnici prea performante, deoarece, desfășurându-și activitatea în interiorul sistemului, pot îndeplini acte criminale cu mijloace mult mai simple. Motivația lor poate să fie un câștig personal sau o răzbunare. Mai grav este cazul când o terță persoană din sistem, investită cu autorizarea unor operațiuni, în mod involuntar, contribuie la îndeplinirea atacului.
Trecerea spre PC-uri, culturalizarea informatică a utilizatorilor constituie reale amenințări pentru sistemele informaționale. Cu banii plătiți de firmă, întrucât efectuează atacul în timpul programului de lucru din birou, angajații devin dușmanii cei mai periculoși ai unității. Tot în această categorie sunt încadrați și greviștii.
3. *Vandalii și huliganii* au la dispoziție forme noi de manifestare, renunțând la bâte și pietre, dar apelând la spargerii informatice, la viruși ș.a. Mai periculoși sunt cei strecurați în unitate pe principiul calului troian. Zicala „Doamne, spune-mi dușmanul care mi-e prieten, căci pe celălalt îl știu eu” trebuie să devină un adevărat crez pentru conducerea unităților.
4. *Utilizatorii* pot să contribuie substanțial la pierderile informatizate, îndeosebi prestând activități nestandardizate și neautorizate. Pe primul loc se află jocurile pe calculator, care, pe lângă faptul că înseamnă folosirea resurselor firmei în scop personal și irosirea timpului de lucru, chiar dacă este o simplă distracție, devin cea mai sigură sursă de „importare” a virușilor. Pe locul doi se află softul tentant, de ultimă oră, necumpărat de firmă, dar aflat în posesia unui „prieten”. Deși este „procurat” cu intenții vădit benefice firmei, se transformă în altceva.
Pentru evitarea acestor cazuri, se impun: instruirea personalului, controlarea și supravegherea permanentă a lui, precum și interzicerea utilizării altor materiale decât a celor aflate în posesia legală a unității.
5. *Organizațiile subversive și teroriste* și-au găsit noi căi de îndeplinire a obiectivelor. Există chiar organizații care își propun, în mod declarat, abolirea calculatoarelor. Din nou, cei mai periculoși sunt angajații unității care aparțin acestor grupuri. Formele lor de manifestare pot fi foarte inteligente, dar și foarte violente. Se pare că virușii cei mai periculoși sunt realizați de astfel de grupări.
6. *Ziarisții*, în intenția de a realiza articole de senzație, pe principiul „scopul scuză mijloacele”, scurmă în „Berevoieștiul informatic” sau chiar în locurile, aparent, bine tănuite.
7. *Publicul larg*, din pură curiozitate informațională sau din dorința de a-și verifica aptitudinile informatice, atentează la integritatea multor sisteme.

8. *Adolescenții*, deși fac parte din categoria anterioară, au forme specifice și rezultate deosebite în atacarea sistemelor. De cele mai multe ori, dispun de cunoștințe informatice impresionante, care, dacă se cuplează cu accesul la datele folosite de părinții lor în sistemele informaționale, devin extrem de periculoși. Printre ei se află cei mai împătimiți hackeri, phrackeri și alte categorii descrise ulterior.
9. *Criminalii* devin noii bogați ai zilelor noastre. Unele firme nu raportează pierderile cauzate de atacurile informatice, fie pentru a nu da curaj și 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 securității, fie pentru a nu face un nume prost aplicațiilor folosite. Cu calculatorul s-au înfăptuit cele mai multe crime perfecte. Cum motivația lor este evidentă, furtul, investițiile făcute de organizațiile care se ocupă cu o astfel de „activitate” sunt mult mai mari pe linia „cercetării științifice” decât ale oricărei firme în parte pe linia asigurării securității sistemului.

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

1. *Atacurile tănuite ale angajaților* (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 și a datelor, inclusiv crearea de drepturi bănești, distrugerea programelor și a datelor, furturile bunurilor materiale sau informatice, precum și folosirea voit eronată a componentelor sistemului, sub formă de sabotaj.
2. *Acțiunile neintenționate ale angajaților* (neglijența). Efectul acestor acțiuni poate să se concretizeze în dezvăluirea unor informații secrete, modificarea programelor și a datelor, întreruperea serviciilor, pierderea programelor și a datelor, precum și distrugerea echipamentelor.
3. *Evenimentele întâmplătoare*. Astfel de evenimente se pot concretiza în întreruperea funcționării echipamentelor/sistemelor, modificarea programelor și a datelor, pierderea programelor și a datelor, distrugerea echipamentelor.
4. *Atacuri secrete ale persoanelor din afara unității*. Scopul lor poate fi aflarea unor informații secrete, întreruperea funcționării sistemelor, modificarea programelor și a datelor, distrugerea echipamentelor și a celorlalte componente, furtul averilor informaționale.
5. *Atacuri deschise din afară* (în forță). Rolul lor este de întrerupere a funcționării sistemului sau de distrugere a lui.
6. *Atacurile deschise ale angajaților* au un scop identic celor anterioare.
7. *Acțiuni neintenționate din afara unității* (introduceri eronate). Prin astfel de acțiuni se pot produce întreruperi ale funcționării sistemului, modificări ale datelor sau ale programelor.

În S.U.A., în „topul atacurilor”, pe primul loc s-au aflat angajații incapabili ai firmelor, urmați de cei incorecți și de furturile din afară. Relativ recent, s-a extins categoria tinerilor pricepuți la calculatoare, care, de acasă, pot accesa sistemele mari, considerând acțiunile lor ca un test de istețime, dar care au devenit din ce în ce mai periculoase. În anii 1998-2001, pe locul întâi s-au aflat atacurile cu viruși, pe locul doi – utilizarea abuzivă, din interior, a rețelelor locale, iar pe locul trei – furtul de laptopuri.

La nivelul anului 2004, cele mai importante amenințări asupra securității organizațiilor Fortune 1000 au fost³:

1. violența 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, hoții cu gulere albe;
4. accesul angajaților în zone nepermise;
5. furtul de hardware/software;
6. furtul (în general) comis de către angajați;
7. atacurile prin Internet, intranet;
8. prezența drogurilor la locul de muncă;
9. lipsa de etică a managerilor;
10. furtul din exterior, vandalismul.

Se observă că 6 dintre cele 10 amenințări de top proveneau din interiorul organizațiilor.

Naivitatea angajaților care cad victime atacurilor phishing și dezvăluie informații confidențiale, furtul de laptop-uri care generează furtul de ... identitate, tot din neglijența posesorilor calculatoarelor portabile, lipsa de coerență a administratorilor care creează conturi de acces și uită să le schimbe la plecarea angajaților din firmă, imposibilitatea de a diferenția mesajele spam de cele legitime, alături de neutilizarea patch-urilor de securitate sunt, la nivelul anului 2006, potrivit Forrester Research, amenințările cele mai grave, care au ca numitor comun neglijența angajaților.

O tendință care poate fi extrasă din analiza rapoartelor CSI/FBI din perioada 2003 – 2007 este conștientizarea constantă a necesității investițiilor în securitate la nivelul firmelor analizate, care are ca efect reducerea breșelor de securitate și implicit a atacurilor. Dintre măsurile adoptate de firme menționăm training-urile în domeniul politicilor de securitate și al securității rețelelor, auditul sistemelor de securitate, introducerea de măsuri de securitate în rețele (inclusiv criptografie), ca și la nivelul controlului accesului.

În 2011, Panda Security ⁴ a menționat atacuri ca „hackivism” și cyber-war, malware orientat tot mai mult pe obținerea de profit, atacuri asupra rețelelor sociale, inginerii sociale și coduri malițioase ce au abilitatea de a se adapta, pentru a evita detectarea, ca și despre creșteri ale amenințărilor la adresa utilizatorilor de Mac și eforturi ale infractorilor de a ataca sistemele pe 64 de biți și de a exploata noi vulnerabilități “zero-day” (semnalate dar neacoperite încă de producător printr-un patch).



- Realizați un „top 3” al celor mai distructive incidente care pot afecta securitatea informațională a unei organizații cunoscute de dvs. Motivați „nominalizările”.
- Realizați un „top 3” al celor mai periculoși atacatori ai unui sistem informatic din cadrul unei organizații cunoscute de dvs. Motivați „nominalizările”.
- Realizați un „top 3” al celor mai grave erori umane care pot influența securitatea unui sistem informatic din cadrul unei organizații cunoscute de dvs. Motivați „nominalizările”.
- Care este, în opinia dvs., cea mai spectaculoasă amenințare informatică a zilelor noastre? Argumentați.

1.2.3 Asigurarea securității sistemelor informaționale

Când se proiectează noi aplicații 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.:

- *Confidențialitatea* se concretizează în oferirea condițiilor de păstrare în conformitate cu restricțiile legale descrise de utilizatori și proiectanți. 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 Bîrzoii, V., *De unde vor veni principalele amenințări informatice în 2011*, 16 decembrie 2011, la <http://businesscover.ro/de-unde-vor-veni-principalele-amenintari-informatic-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 și a asigurării încrederii în ele;
- *Accesibilitatea* se referă la asigurarea accesului la date, pentru cei autorizați, în orice moment.



Pentru o organizație cunoscută de dvs., realizați un clasament al celor mai importante 5 averi informaționale, precizând pentru fiecare dintre ele dacă este importantă asigurarea confidențialității și/sau integrității și/sau accesibilității. Justificați.

Sistemele informaționale, pe linia asigurării securității lor, au multe elemente comune cu celelalte sisteme. Dintre măsurile comune, amintim pe cele organizatorice și administrative, de personal, de protecție fizică și a mediului de lucru.

Particularitățile protecției unui sistem informațional se referă la luarea unor măsuri speciale de apărare a datelor, prin intermediul *echipamentelor* de prelucrare automată a datelor, *softului* de sistem sau de aplicații, precum și al *comunicațiilor*, 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 și evaluarea elementelor patrimoniale de protejat, astfel încât nimic să nu fie omis, iar valorile deosebite să aibă un tratament special;
2. recunoașterea de la bun început a vulnerabilității și slăbiciunii sistemelor informaționale;
3. specificarea tuturor atentatelor posibile asupra sistemelor electronice de calcul, în general, și asupra unei aplicații informaționale anume, în special;
4. evaluarea potențialelor pierderi sau riscuri generate de un anumit incident, cu toate consecințele care decurg de aici;
5. realizarea, implementarea și consolidarea unor metode de asigurare a securității, 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 și auditarea periodică a eficienței măsurilor de asigurare a securității sistemului.

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

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

15. Consemnarea, în scris, a faptelor care au afectat valorile patrimoniale;
16. Verificarea dublă a tuturor operațiunilor referitoare la valorile patrimoniale;
17. Elaborarea documentațiilor de analiză a operațiunilor cu valori patrimoniale;
18. Cercetarea tuturor neregulilor;
19. Sancționarea abaterilor;
20. Crearea posibilității de redresare, în orice moment, după unele acțiuni care au eșuat.

Fiecare mecanism de protecție trebuie să realizeze obiectivele pentru care a fost conceput. Eficiența lui nu trebuie să depindă de prezumții false privind imposibilitatea atacării sistemului. El trebuie să demonstreze *completitudine*, ceea ce se va concretiza printr-o funcționare normală la orice eventuală amenințare, *corectitudine*, prin oferirea răspunsurilor anticipate, îndeosebi atunci când s-ar înregistra intenții frauduloase sau s-ar produce erori în utilizare. Mecanismul perfect trebuie să fie *cât mai simplu posibil*, precum și *ușor de întrebuințat* și să ofere *un număr cât mai mic de erori sau alarme false*.

Supraviețuirea lui este o altă proprietate, stabilindu-se cu o precizie cât mai mare perioada de funcționare la un anumit nivel asigurat al protecției, în condiții optime de utilizare. De asemenea, trebuie să *ofere soluții pentru întreruperile de energie, defectarea sistemelor de comunicație, variații bruște ale temperaturii ș.a.*

Nu trebuie uitat raportul *cost sistem - eficiență*.



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

1.3 Mecanisme de apărare – prezentare generală

Literatura de specialitate consemnează șapte mecanisme de asigurare a eficienței securității sistemelor informaționale:

1. *Securitatea fizică* se referă la controlul accesului fizic în sistem și se va concretiza sub diverse moduri: de la împrejmuiri ale amplasamentelor și uși, la lacăte și sisteme de alarmă, inclusiv crearea cadrului de intervenție în cazuri de urgență.
2. *Securitatea personalului* presupune selecția, urmărirea, autorizarea și supravegherea angajaților.
3. *Criptarea informațiilor importante* înseamnă protejarea datelor comunicate la distanță, făcându-le neinteligibile pentru orice alte persoane decât cele autorizate a le recepționa.
4. *Studierea tehnicilor specializate ale intrușilor* astfel încât echipamentele acestora să nu poată pătrunde în configurația sistemului.
5. *Suprimarea radiațiilor compromițătoare* este o operațiune necesară pentru că echipamentele folosite în centrele de prelucrare automată a datelor produc radiații acustice și electromagnetice, care pot fi interceptate și analizate. Este cazul consolelor, imprimantelor, cablurilor de legătură, al echipamentelor de vizualizare ș.a.
6. *Securitatea liniilor de comunicație* se referă la garantarea comunicării corecte pe liniile care interconectează componentele sistemului, astfel încât intrușii 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 și a protejării datelor, stabilindu-se reguli foarte precise de folosire a lor.

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

Mecanism de securitate	Categoria informațiilor			
	Strict secrete	Secrete	Confidențiale	Cu restricții
Fizică	X	X	X	X
Personal	X	X	X	X
Criptografică	X	X		
Tehnică	X			
Radiații	X			
Linii de comunicație			X	
Sistemul de prelucrare automată a datelor			X	X

Fig. 1.1 Protecția informației prin mecanisme specializate

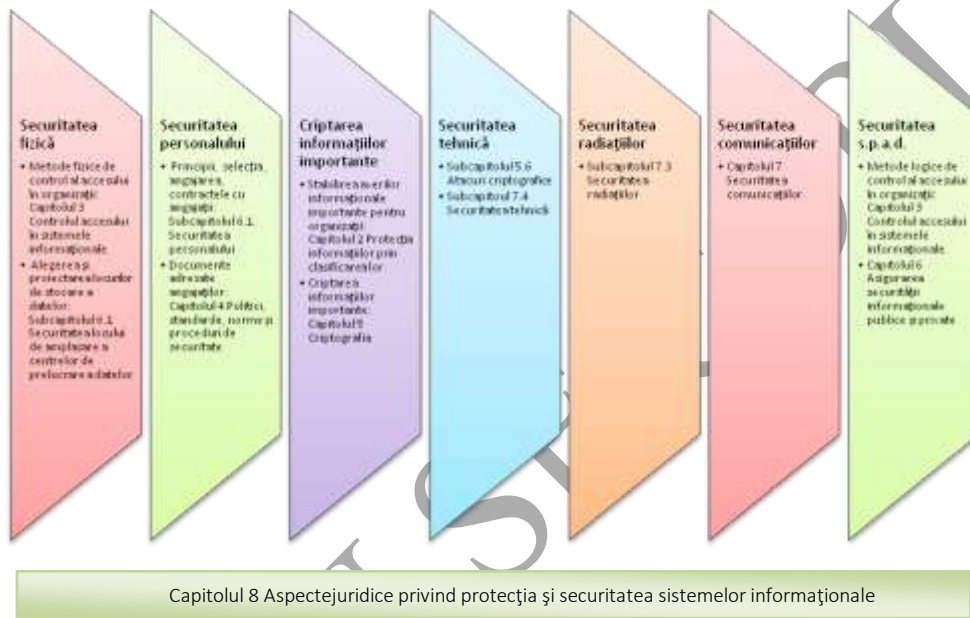


Fig. 1.2 Sinteza conținutului manualului pe mecanisme de securitate

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 organizație cunoscută de dvs.? Justificați, cu exemple.
- Din ce motiv credeți că nu au fost bifate cu X căsuțele cu fundal mai închis din Figura 1.1?

Rezumat

Alături de capital și oameni, informația este una dintre averile deosebite ale firmei. Pentru a periclita această resursă importantă, orice persoană care dialoghează cu calculatorul unei organizații poate să facă (cel puțin) următoarele lucruri: să copieze fișierele importante ale altor firme, să influențeze evidențele altora pentru a le cauza pierderi, să reprogrameze calculatoarele incluse în configurația sistemelor de producție pentru a provoca avarierea utilajelor sau pentru producerea accidentelor umane, să șteargă programe sau fișiere. Din acest motiv, considerăm absolut necesară tratarea cu prioritate de către manageri a problemelor de securitate informațională.

În funcție de tehnologiile folosite și de evoluția în timp a preocupărilor ce o privesc, securitatea informațională poate fi abordată prin prisma unui număr mai mare sau mai mic de generații. Capitolul 1 prezintă și câteva repere din istoria modernă a preocupărilor internaționale pe linia protecției și

securității informaționale, cu dorința de a conștientiza cititorii de necesitatea unei discipline de profil în cadrul Facultății de Economie și Administrarea Afacerilor.

În orice mediu de lucru, datele trebuie să respecte principiile C.I.A – Confidențialitate, Integritate, Accesibilitate. Urmărind această triadă, particularitățile protecției unui sistem informațional se referă la luarea unor măsuri speciale de apărare a datelor, prin intermediul echipamentelor de prelucrare automată a datelor, softului de sistem sau de aplicații, precum și al comunicațiilor, dacă se lucrează într-un astfel de mod. Măsurile de apărare sunt necesare pentru a contra-pondera pericolele care vizează informațiile dintr-o organizație: incidentele, factorii naturali, bazați pe hazard, atacurile.

Literatura de specialitate consemnează șapte mecanisme de asigurare a eficienței securității sistemelor informaționale: securitatea fizică, securitatea personalului, criptarea informațiilor importante, studierea tehnicilor specializate ale intrușilor, suprimarea radiațiilor compromițătoare, securitatea liniilor de comunicații, securitatea sistemelor de prelucrare automată a datelor, care vor fi tratate pe parcursul capitolelor următoare.

ANU SE COPIA

CAPITOLUL II

Protecția informațiilor prin clasificarea lor

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

Printre obiectivele capitolului de față se numără:

- (re)cunoașterea necesității de clasificare a informațiilor și a principalelor criterii folosite pentru aceasta;
- familiarizarea cu tipurile de informații ce sunt supuse clasificării;
- identificarea principalelor roluri și responsabilități în procesul de clasificare a datelor;
- cunoașterea modalităților de marcare și distrugere a materialelor cu regim special dintr-o organizație.

2.1 Forme embrionare de protejare a informațiilor

Dacă în urmă cu peste 10.000 de ani s-au realizat primele forme de ținere a evidenței produselor necesare hranei unei comunități umane, făcându-se trimitere la perioada neolitică a Orientului Mijlociu – cam în anii 8500 î.C. –, tot atunci s-au înregistrat și primele preocupări pe linia securizării informațiilor păstrate. Produsele obținute erau evidențiate prin mici forme realizate din lut, diferențiate după proprietar, dar, cum recolta se ținea în comun, în hambarele comunității, și obiectele se păstrau în vase speciale, cu particularități 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-și ia înapoi ceea ce-i aparținea, magazionerul spărgea vasul cu însemnele de lut ale acestuia, operațiune efectuată în prezența 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 evidență, prin intermediul nodurilor de pe funii sau sfori. La fel de bine, am putea spune că, în urmă cu șase mii de ani, oamenii au început să fie trași 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 condiții de securitate deplină.

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

După altă o mie de ani au apărut *formele echivalente ale actualelor obligațiuni, avize de expediție* ș.a. În același 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*, și 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 operațiunilor, au fost promovate principiile dublei reprezentări și dublei înregistrări, deși acestea apăruseră în anii 1300. După renașterea s-au înfăptuit multiple sisteme de securitate; o bună parte din ele se regăsesc în mai multe capitole ale cărții de față.



Cunoașteți și alte momente istorice relevante în clasificarea informațiilor? Prezentați-le succint, precizând sursa bibliografică.

2.2 Începuturile clasificării moderne a informațiilor

După scurta istorie a preocupărilor vizând securitatea, să ne apropiem de vremurile noastre și de punctul de vedere al securității sistemelor față de tipurile de informații protejate.

Dacă după cel de-al doilea război mondial au rămas atâtea amintiri neplăcute, se cuvine, totuși, să recunoaștem și câteva moșteniri teribile. Ne gândim la cercetarea operațională, 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 și 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 informațiilor, de la cel mai de jos nivel, unde se situează informațiile deschise (*open*) sau neclasificate (*unclassified*), la cele confidențiale, urcând spre informații secrete și strict secrete (*top secret*).

Inițial, s-a pornit de la ideea că informațiile care prin compromitere pot *costa vieți umane* sunt marcate „secrete”, în timp ce informațiile a căror compromitere costă *pierderea multor vieți umane* sunt definite „top secret” (strict secrete). Angajații în domeniul securității sistemelor sunt investiți cu responsabilități diverse, dar și cu dreptul de a lucra cu anumite categorii de informații. Se poate vorbi de o strânsă legătură între responsabilități și categoriile de informații cu care se dă dreptul de a lucra. În SUA, dreptul de verificare a fișierelor cu amprente ale FBI este acordat doar pentru verificarea unor informații 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 informații, pentru exercitarea controlului lucrurile sunt mai clare: un oficial poate citi documentele dintr-o anumită categorie numai dacă el are cel puțin împuternicirea de accesare a informațiilor din categoria respectivă sau dintr-una superioară. De exemplu, un împuternicit să acceseze informații „strict secrete” poate citi informații confidențiale, secrete și strict secrete, iar unul cu drept de accesare a informațiilor secrete nu le poate accesa pe cele „strict secrete”. Regula este că informațiile pot circula doar în sus, de la confidențial la secret și 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 declassifica.

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

Sunt foarte puține unități care au proceduri stricte pe linia asigurării securității informațiilor. Pe de altă parte, la nivel național 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 și alte elemente importante sunt încadrate într-o anumită categorie.

Se practică *două strategii de bază* pe linia securității naționale:

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 informațiile guvernamentale. În multe țări de pe glob, accesul la informațiile naționale este controlat prin legi privind secretul de stat, folosindu-se cea de-a doua strategie. Un angajat loial și 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 informațiilor deosebite:

- *controlul discreționar 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 poziției ce o deține, nu are drepturi nelimitate de a vedea informațiile deosebite, iar persoanele care au o astfel de facilitare trebuie să le vadă numai pe cele care intră în sfera lor de activitate. Controlul discreționar al accesului este aplicat printr-o matrice de control, conform modelului redat în fig 2.1. Pentru fiecare persoană (subiect) aflată pe listă și pentru fiecare informație (obiect), matricea arată ceea ce poate face fiecare subiect cu obiectele din listă: citire, scriere, execuție, aprobare ș.a.

SUBIECT/OBIECT	OBIECT 1	OBIECT 2	OBIECT 3
SUBIECT 1	Execută	Citește	Citește/Scrie
SUBIECT 2	Aprobă	Execută	Citește
SUBIECT 3	Citește/Scrie	Aprobă	Execută
SUBIECT 4	Citește	Citește/Scrie	Aprobă
SUBIECT 5	Execută	Citește	Citește/Scrie

Fig. 2.1 Matrice de control al accesului

Controlul legal al accesului își exercită forța pe baza legilor existente (legea securității naționale, legea energiei atomice ș.a.). În SUA, prin lege, sunt stabilite două tipuri de structuri de control: ierarhizate și neierarhizate.

Structura ierarhizată încadrează informațiile sensitive în patru categorii: strict secrete, secrete, confidențiale și neclasificate.

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

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

În structura neierarhizată sunt două categorii: *compartimentate* și *cu obiecții* 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 comunicației), *CRIPTA* (criptare), *COMSEC* (comunicații secrete), *HUMINT* (*Human INTelligence*), *SIGINT* (*SIGnal INTelligence*), *IMINT* (*IMage INTelligence*) ș.a. Categoria „cu obiecții” privește îndeosebi naționalitatea potențialilor cititori și autori ai obiectelor. În SUA, contestațiile (obiecțiile) sunt: *NOFOR* (*no foreign* = neaccesibile străinilor), *US/UK EYES ONLY* (de văzut numai de către englezi sau americani) ș.a.

Informațiile strict secrete, care sunt într-o anumită compartimentare, se numesc *informații sensitive compartimentate* și presupun o atenție deosebită la întrebuintare. Doar o categorie este superioară acestora din urmă. Este vorba despre *informațiile din planul operativ integrat unic sau răspunsul național în caz de război*.

Clasificarea și legislația din România sunt prezentate în capitolul 9.



Informați-vă despre cazul *Wikileaks*. Argumentați pro sau contra oportunității existenței acestui proiect.

2.3 Clasificarea informațiilor

Atunci când informațiile au fost împărțite în două mari categorii, clasificate și neclasificate, s-a ținut cont de anumite principii. Pentru a le cunoaște, însă, este nevoie de o abordare preliminară a unor concepte¹.

Guvernele pornesc de la o clasificare mai largă, împărțind informațiile în două mari tipuri: *informații subiective* și *informații obiective*. Anterior a operat o altă clasificare: *informații „operaționale”* și *informații „științifice”*. Unii chiar au menționat un al treilea tip de informații clasificate de guverne – *informații „tehnice”*, însă în multe materiale, informațiile tehnice și cele științifice sunt submulțimi ale informațiilor obiective.

2.3.1 Informații subiective

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

Aceste informații au următoarele caracteristici:

- *dimensiune redusă* – secretul poate fi exprimat prin doar câteva cuvinte; din această cauză poate să fie furat cu ușurință și dat altora;
- *perceptibilitate universală* – nu este nevoie de pregătire specială pentru a înțelege 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;
- *conținutul poate fi schimbat* – secretul poate fi modificat și în ultima clipă; dacă o țară a aflat că adversarul cunoaște momentul și locul invaziei, acestea pot fi schimbate;
- *sunt perisabile după scurt timp* – secretele au o viață scurtă; după declanșarea invaziei, adversarul a aflat secretul, el devenind public; în concluzie, secretul poate fi ținut doar pentru o perioadă scurtă de timp.



Dați exemple de informații subiective întâlnite în cadrul organizațiilor economice. Justificați importanța lor pentru respectivele organizații.

2.3.2 Informații obiective

Informațiile 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 țară. În această categorie intră *informațiile științifice* sau *secretele științifice*. Asupra acestui fel de informații nu se poate avea un control absolut. Ele țin de natura lucrurilor, nu de un secret. Oamenii de știință din alte țări, independenți unii de alții, pot face descoperiri identice. Informațiile de acest tip sunt referite și ca *informații obiective* sau *secrete „obiective”*.

Informațiile 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 informațiilor științifice sunt necesare rapoarte lungi; din această cauză ele nu se pot transmite cu ușurință;
- *pot fi înțelese numai de către oamenii de știință*;
- *nu sunt supuse arbitrarului* – și alții pot să afle răspunsul la o anumită întrebare științifică, dacă formulează întrebarea cuvenită;
- *nu sunt supuse schimbării* – au caracter etern; un fenomen natural are o singură valoare;
- *pot avea o viață lungă ca secret* – alții pot descoperi informațiile în mod independent, dar o astfel de descoperire necesită mult timp, ceea ce va conduce la păstrarea secretului pentru o lungă perioadă.



Dați exemple de trei informații obiective întâlnite în cadrul organizațiilor economice. Justificați importanța lor pentru respectivele organizații.

2.3.3 Informații tehnice, văzute ca secrete obiective

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

Caracteristicile informațiilor tehnice sunt similare cu cele ale informațiilor științifice, dar există unele diferențe între aceste două tipuri. Spre deosebire de informațiile științifice, informațiile 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 informațiile tehnice sunt utilizate pentru exploatarea informațiilor științifice. Cu toate acestea, în domeniul clasificării informațiilor, cele științifice și tehnice sunt considerate că formează un singur tip de informații.



Dați exemple de trei informații tehnice, văzute ca secrete obiective, întâlnite în cadrul organizațiilor economice. Justificați importanța lor pentru respectivele organizații.

2.3.5 Secrete subiective, secrete obiective și secrete comerciale

Cu toate că există două tipuri principale de informații clasificate (secrete subiective și obiective), legea secretului comercial recunoaște numai un tip al secretelor comerciale – secretele obiective. Secretele comerciale includ informațiile despre procesele de fabricație, „rețetele” unor produse (cum este cazul formulei de fabricație pentru Coca-Cola®), precum și alte informații obiective care pot fi descoperite independent de către alte afaceri. Multe secrete comerciale sunt asemănătoare informațiilor științifice și tehnice.

Secretele subiective nu sunt protejate prin legile secretului comercial. Dacă un guvern poate clasifica și proteja datele privind invazia unei alte țări (informații subiective), o firmă nu poate primi protecția secretului comercial pentru data la care își planifică să introducă în fabricație un nou produs.



Dați exemple de alte secrete comerciale cunoscute de dvs.

2.3.6 Determinarea necesității clasificării informațiilor

În vederea clasificării informațiilor 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 pași principali:

- a. definirea cu exactitate a informațiilor de clasificat (opțional, dar recomandat);
- b. stabilirea dacă informațiile se încadrează într-unul din domeniile supuse clasificării;
- c. verificarea dacă informațiile se află sub control guvernamental;
- d. concluzionarea dacă dezvăluirea informațiilor poate să conducă la cauzarea daunelor pentru securitatea națională;
- e. specificarea precisă a nevoii de clasificare a informațiilor (opțional, dar recomandat).

Determinarea nivelurilor clasificării

Atunci când o informație trebuie să fie clasificată ei i se va atribui un nivel de clasificare, ceea ce va evidenția importanța relativă a informației clasificate în sistemul național de securitate, specificându-se cerințele minime pe care trebuie să le îndeplinească acea informație.

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

În *sistemul american de clasificare a informațiilor* există trei niveluri de clasificare: top secret (strict secret), secret și confidențial. Informațiile neclasificate constituie o altă categorie. În Legea 182/2002 privind protecția informațiilor clasificate, din România, informațiile clasificate din clasa secretelor de stat sunt încadrate în trei niveluri, astfel: strict secrete de importanță deosebită, strict secrete și secrete.

Informațiile strict secrete (SUA), cărora le corespund *informațiile strict secrete de importanță deosebită* (România), sunt informațiile a căror divulgare neautorizată este de natură să producă daune de o gravitate excepțională securității naționale.

Informațiile secrete (SUA), ceea ce echivalează cu *informațiile strict secrete* (România), sunt informațiile a căror divulgare neautorizată este de natură să producă daune grave securității naționale.

Informațiile confidențiale (SUA), corespunzătoare *informațiilor secrete* (România), sunt informațiile a căror divulgare neautorizată este de natură să producă daune securității naționale.

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

Determinarea duratei clasificării

Guvernele clasifică informațiile și aplică proceduri de securitate specială documentelor și materialelor ce le conțin sau sunt purtătoare ale acelor informații pentru a preîntâmpina obținerea lor de către adversari, cu intenția de a le folosi împotriva deținătorului autorizat. Din păcate, informațiile clasificate nu stopează, în mod automat, accesul adversarilor la ele. Se

spune² că pentru păstrarea în mare taină a informațiilor trebuie fie să nu spui nimănui acele informații, fie să folosești metoda căpitanului Kidd. Totuși, cum informațiile trebuie să fie utilizate de mai mulți guvernanți, ele nu pot fi ținute în taină de o singură persoană. Pe de altă parte, metoda căpitanului Kidd, de păstrare a secretului, este de neacceptat. În consecință, *guvernele folosesc metoda clasificării informațiilor 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 își îngropa comorile cu scopul de a le recupera ulterior. Toți cei care participau la astfel de operațiuni erau uciși, încât nimeni altul decât Kidd nu mai știa 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, informațiile, oricât ar fi de prețioase, nu pot fi păstrate o perioadă nelimitată de timp fără să fie aflate de adversari. Uneori ei le obțin prin spionaj. Alteori, ele sunt aflate datorită proastei gestionări de către posesorul autorizat. Sunt și cazuri în care, îndeosebi pentru informațiile științifice și tehnice, adversarii le obțin cu eforturi proprii, prin invenții și inovații.

Chiar dacă informațiile pot fi păstrate ani mulți fără a fi aflate de adversari, nu este, de regulă, recomandat să se păstreze perioade îndelungate. Clasificatorii informațiilor sunt cei ce vor hotărî dacă este cazul să se specifice timpul de păstrare a informației clasificate sau să se indice momentul în care va interveni declasificarea automată. Durata informațiilor 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 și ar putea acționa pentru șubrezirea întregului sistem de securitate națională. În concluzie, doar clasificatorul trebuie să aibă grija stabilirii duratei de clasificare.

Când se încearcă a se discuta despre durata de păstrare a informațiilor clasificate, părerile sunt destul de diferite. În SUA, în 1970, într-un raport al unui organism specializat, s-a făcut următoarea declarație: „Este puțin probabil că informațiile clasificate să poată fi protejate o perioadă mai mare de cinci ani și este mult mai rezonabil să presupunem că ele devin cunoscute de către alții în perioade de cel mult un an, prin descoperire independentă, dezvăluire clandestină sau alte mijloace.” Alți specialiști au declarat că experiența 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 funcție de importanță. Un director al Departamentului Apărării din SUA declara că durata păstrării informațiilor clasificate poate fi influențată de o serie de factori, după cum urmează: nivelul la care se află tehnologia, succesele raportate de serviciile secrete proprii sau ale adversarilor, precum și realizările din domeniile politic, militar și tehnic. De reținut este faptul că nu există o formulă magică sau un anumit standard pentru stabilirea numărului de ani de păstrare a informațiilor clasificate sau a echipamentelor sau materialelor ce prelucrează sau conțin astfel de informații.

În final, se poate spune că perioada de păstrare a informațiilor clasificate depinde de tipul informației ce urmează a fi protejată (subiectivă sau obiectivă; operațională sau științifică), de numărul persoanelor care cunosc informația clasificată, de procedurile de securitate folosite pentru protejarea acestor informații, precum și de calitățile celor puși să le păstreze și protejeze.

Durata clasificării informațiilor se determină prin una dintre următoarele metode:

- a. ca o perioadă de timp măsurată de la data emiterii documentului;
- b. în funcție de un eveniment viitor ce poate să apară înaintea operațiunii de declasificare;
- c. dacă data, respectiv evenimentul nu pot fi specificate, atunci documentul conținând informații clasificate va fi marcat, pentru a se indica instituția 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



Dați exemple de trei informații dintr-o organizație care este necesar să fie clasificate. Precizați nivelul de clasificare pe care le așezați și propuneți durate de clasificare, în funcție de natura informațiilor și obiectul de activitate al organizației. Argumentați.

2.4 Clasificarea asocierilor de informații

Informațiile ce nu sunt clasificate, uneori, sunt supuse clasificării ca urmare a asocierii lor cu alte informații care, implicit sau explicit, conduc la dezvăluirea altor informații 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 informațiilor prin asociere este rezultatul cuplării informațiilor despre părțile echipamentelor sau despre materiale folosite pentru fabricarea echipamentelor clasificate. Astfel, un echipament comercial nu poate fi el însuși clasificat, dar asocierea lui cu un proiect clasificat poate conduce la clasificare numai în contextul asocierii cu acel proiect. La fel se întâmplă și cu materialele, îndeosebi chimice. Alteori, simpla prezență a numelui unei persoane pe o listă de distribuție 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 și vizita expertului trebuie să fie clasificată. Dacă se cere o astfel de clasificare, persoana vizitatoare va figura cu un nume fictiv.

În ultimul timp, localitățile în care se află amplasamente clasificate sunt subiectul unor supravegheri sporite, îndeosebi pe linia scurgerii de substanțe chimice care poluează mediul. Operațiunea este efectuată de agenții specializate, organizații neguvernamentale, echipe de investigare diverse. Toate acestea solicită date primare pentru identificarea chimicalelor folosite, inclusiv concentrațiile lor, pe baza unor probe preluate din atmosferă, din scurgeri de ape reziduale, din pânza de apă freatică, din sol ș.a. În cele mai multe cazuri, materialele întrebunțate sunt neclasificate, dar asocierea lor cu un loc cu destinație 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.



Dați exemple de informații (necesar a fi) clasificate prin asociere, din activitatea organizațiilor cunoscute de dvs.

2.5 Clasificarea compilărilor de informații

Așa cum am menționat anterior, informațiilor li se dă o clasificare pe linia securității atunci când dezvăluirea lor neautorizată poate să cauzeze daune de dimensiuni variate securității naționale. Clasificarea informațiilor conduce la înregistrarea unor costuri specifice inevitabile, motiv pentru care este necesară o atenție deosebită asupra informațiilor care trebuie neapărat să fie clasificate pentru a li se asigura protecția și pentru a fi ascunse potențialilor adversari. Și totuși, așa cum sunt informații ce devin clasificate în urma asocierii, există și informații neclasificate care, prin compilare, trebuie să fie tratate ca informații clasificate. Aceasta nu trebuie să fie o regulă, ci o excepție. 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 posibilității de a fi dezvăluite tendințele cercetării și dezvoltării din departamentele de apărare. La rândul lor, aceste tendințe 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 informațiile 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 menținerii credibilității programului de clasificare, ca aspect important al succesului politicii de clasificare.

Multitudinea punctelor de vedere referitoare la clasificarea compilării informațiilor neclasificate provine probabil din ambiguitatea cuvântului compilare. Unele dintre dispute ar putea să dispară dacă ar fi definită corect compilarea. Federația Oamenilor de Știință Americani definește compilarea ca pe o ordonare a materialelor preexistente (fapte, statistici ș.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 adaugă o valoare substanțială (informație) compilatorului;
2. compilări care adaugă o valoare substanțială compilatorului.

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



Dați exemple de informații (necesar a fi) clasificate prin compilare, din activitatea organizațiilor cunoscute de dvs.

2.6 Declasificarea și degradarea informațiilor clasificate

Atunci când se efectuează clasificarea unor informații se iau în calcul anumite cerințe de îndeplinit. Când, din diferite cauze, se schimbă circumstanțele, firesc, și cerințele îndeplinite inițial se modifică, situație în care informațiile clasificate se declasifică sau trec pe un nivel inferior de clasificare.

Declasificarea informațiilor se efectuează de către reprezentanți ai guvernului, cărora le revine misiunea de declasificare. Trebuie remarcat faptul că este o diferență între declasificarea informațiilor și declasificarea documentelor sau materialelor. Ultima categorie poate fi efectuată și de către contractorii guvernamentali.

A degrada informațiile clasificate înseamnă reducerea nivelului clasificării. În acest mod informațiile strict secrete pot fi degradate la nivelul secret sau confidențial. Informațiile secrete pot fi degradate în informații confidențiale, iar cele confidențiale 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 informaționale. Britanicii vorbesc despre gradarea informațiilor și nu despre clasificarea lor, atunci când se referă la ceea ce americanii numesc clasificarea informațiilor. Ulterior, după primul război mondial, și americanii au preluat termenul de degradare (*down-grading*), preluând sistemele folosite foarte mult de către britanici și francezi.

De regulă, degradarea se efectuează de către persoanele care au clasificat inițial informațiile, de către succesorii acestora, șefii lor sau de către alți oficiali delegați cu o astfel de autorizare, în scris, de către șefii agenției sau de către responsabilii pe această linie.



- Dați exemple de declasificări de informații.
- Dați exemple de informații supuse procesului de degradare (downgrading).

2.7 Principiile clasificării informațiilor și legea secretului comercial

Se spune că, în lumea afacerilor, organizațiile își protejează informațiile care le oferă avantaje în fața concurenților, așa cum guvernele își protejează informațiile care le conferă avantaje în confruntarea cu adversarii lor. Unul dintre cele mai bine păstrate secrete ale zilelor noastre este secretul comercial, așa cum este rețeta de fabricație pentru Coca-Cola Classic®. „Secretele de stat” probabil că au însoțit formarea primelor „state”, în timp ce „secretele comerciale” au fost cele mai importante averi ale primelor afaceri. Ocazional, secretele de stat și 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 comerțului exterior al Chinei cu alte țări. Abia în secolul VI d.C., cu ajutorul a doi călugări persani, ouăle viermilor de mătase și semințele dudului au părăsit China. Disperată, China a încercat să producă derută în rândul celor ce intenționau să dezvolte industria mătăsii, afirmând că mătasea se obține prin expunerea lânii la soare, stropirea ei cu apă și apoi se efectuau unele combinații pentru a rezulta produsul finit, mătasea.

Există o mulțime de asemănări între clasificarea și protejarea informațiilor de apărare națională și de relații internaționale de către guverne, pe de o parte, și protecția secretelor comerciale de către companii, pe de altă parte. În ambele ipostaze, informația protejată este atât de importantă încât ajungerea ei în posesia adversarilor (dușman/concurent) poate să aibă efecte negative asupra intereselor majore (securitatea națională/profitul) ale protectorului. Atât secretele comerciale, cât și informațiile clasificate necesită o vigoare continuă pentru asigurarea protecției împotriva dezvăluirilor neautorizate. De asemenea, ambele pot să-și 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 informațiile declassificate sau făcute publice pe cale oficială nu mai pot fi reclasificate.

Unele secrete comerciale, cum sunt formulele chimice sau cunoștințele despre anumite procese de fabricație, sunt comparabile cu informațiile științifice și tehnice clasificate. Alte secrete comerciale, cum este cazul listei clienților, sunt asemănătoare informațiilor subiective clasificate.

Informațiile despre un nou produs comercial sunt păstrate ca secrete ale unei firme pentru a avea prioritatea lansării pe piață și a păstrării unor avantaje în fața concurenților. Identic, informațiile despre conceperea și realizarea unei noi arme sunt considerate secrete naționale pentru a-i oferi țării deținătoare avantaje majore în fața adversarilor săi.

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

Protecția legală, permisă atât de secretele comerciale, cât și de secretele de stat, are rădăcinile în dreptul comun.

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

Legea secretului comercial nu protejează pe deținătorul secretului împotriva unor descoperiri normale, prin invenții sau inovații, 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 obțină aceleași informații prin eforturi independente sau prin ingineria inversă, ci de a evita sprijinirea adversarilor să

achiziționeze acele informații. Prin inginerie inversă se pornește de la un produs și se încearcă a se afla cum a fost realizat.

În general, se poate spune că există o puternică asemănare între caracteristicile informațiilor protejate sub forma secretului comercial și caracteristicile informațiilor protejate ca informații clasificate. Literatura de specialitate⁴ enumeră șase elemente sau factori care au fost propuși să fie utilizați atunci când se încearcă a se stabili dacă informațiile reprezintă sau nu un secret comercial, astfel:

1. gradul în care informația este cunoscută în afara organizației;
2. gradul în care este cunoscută de angajați și alte persoane implicate în afacere;
3. dimensiunea măsurilor luate pentru a se garanta secretul informațiilor;
4. valoarea informațiilor pentru proprietar și pentru competitorii lui;
5. mărimea efortului sau banii cheltuiți pentru obținerea acelor informații;
6. ușurința sau dificultatea cu care informația poate fi achiziționată sau multiplicată de către alții.



Justificați, cu exemple, importanța secretelor comerciale în activitatea firmelor.

2.8 Principiile protejării informațiilor speciale

Date fiind clasificările anterioare, pe linia protejării informațiilor speciale pot fi enunțate 10 principii:

Principiul delimitării autorizării

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

Principiul securității simple

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

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 integrității

Nici un program pentru calculator nu va accepta informații 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 și 6, 2 și 3, 4 și 5, reieșind cei 6 factori din *Restatement of the Law of Torts*

Al doilea principiu al integrității

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

Principiul etichetării

Fiecare purtător de informații va fi etichetat clar cu categoria informațiilor conținute, în format accesibil omului și în format sesizabil de către echipamentele periferice.

Principiul clarificării

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

Principiul inaccesibilității

Nici o informație nu va fi lăsată la dispoziția altor persoane sau procese, cu excepția celor consemnate prin norme interne.

Principiul verificabilității

Pentru toate activitățile semnificative pe linia securității (deschiderea fișierelor, ștergerea obiectelor, transmiterea în altă parte) se vor crea înregistrări imposibil de șters, cu rolul facilitării verificării sistemului.

Principiul încrederii în software

Cât timp nici un calculator nu poate controla perfect respectarea principiilor anterioare, dar, totuși, efectuează activități utile, încrederea în software va permite apariția unor excepții de la regulă, dacă este cazul.



Exemplificați modul în care principiile enunțate mai sus se aplică într-o organizație cunoscută de dvs.

2.9 Protejarea suporturilor informaționale

Întrucât calculatoarele generează ieșiri care, potențial, sunt mult mai valoroase decât intrările din fișierele ce le-au generat, obligația pe linia încadrării informațiilor în diverse categorii revine persoanelor care autorizează prelucrarea și directorului centrului de prelucrare automată a datelor (p.a.d.) sau delegatului acestuia.

Toate suporturile care conțin informații obținute 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 ș.a. Tratatul lor trebuie să fie similar documentelor ce conțineau aceleași date în condițiile prelucrării tradiționale.

Toate materialele intermediare și informațiile obținute 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 și discurilor magnetice, hârtiei de imprimantă, benzilor tușate ș.a. Aceste materiale auxiliare trebuie să fie supuse clasificărilor în funcție de informațiile ce le conțin.

Ștergerea informațiilor clasificate este o operațiune căreia trebuie să i se acorde o importanță deosebită. Suporturile de prelucrare automată a datelor care posedă caracteristici de remanență după ștergere, cum sunt suporturile magnetice, trebuie să fie tratate cu mare atenție din faza aprobării ștergerii lor. După ștergere ele pot fi folosite pentru păstrarea unor informații cel puțin la fel de importante ca și precedentele.

Fiecare persoană care autorizează operațiuni de prelucrare automată a datelor trebuie să verifice dacă există o fișă de securitate, care să conțină categoria persoanei executante, categoria informațiilor prelucrate și instrucțiuni privind statutul informațiilor rezultate. De asemenea, vor fi consemnate date privind durata prelucrării, timpul de utilizare a componentelor bazei de date, generațiile reținute (fiu, tată, bunic), astfel încât să poată fi reconstituită baza de date în caz de avarii, precum și alte cerințe pe linia păstrării copiilor de siguranță.

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

Toate documentele obținute 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 colțul din dreapta sus, precum și 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 accepțiunea prelucrării automate a datelor, un ecran cu informații este tratat ca o pagină de document, și încadrarea într-o categorie sau alta se va face pe o linie distinctă a acestuia.

Marcarea în cod mașină trebuie să se efectueze prin coduri sesizabile de echipamente, astfel încât să rezulte foarte clar din ce categorie fac parte informațiile prelucrate și la ce operațiuni pot fi supuse. Codul trebuie să fie una dintre primele informații ce vor fi date sistemului, astfel încât să nu fie posibilă accesarea altor date înainte de a se ști statutul lor. Codul poate fi ultimul caracter al numelui fișierului, iar caracterul utilizat să aibă valorile:

S = special, **C** = confidențial, **P** = privat, **R** = cu restricții, **N** = neclasificate.

Exemplu de nume de fișier: SALARIIC – ultimul caracter, C, arată că sunt informații confidențiale.

Marcarea fizică se referă la toate suporturile supuse prelucrării automate a datelor. Marcajul trebuie să reziste în timp și 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 conține. Suporturile reutilizabile trebuie să fie marcate cu etichete adezive sau creioane ce pot fi șterse ulterior.

Marcarea suporturilor de hârtie, cum au fost cartelele și benzile perforate, au marcajul prin culori distincte: portocaliu = informații care necesită control special, roz = confidențiale, verde = private, galben = cu restricții, albe = comune. Dacă numai o parte a benzii sau pachetului conține informații protejate, tot volumul va căpăta același statut.

Marcarea cutiilor și a carcaselor este necesară atunci când suporturile de memorare sunt păstrate în astfel de condiții, caz în care se impune etichetarea neambiguă a acestora, precum și scrierea fișierelor conținute 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 microfișele.

2.9.2 Păstrarea și distrugerea materialelor speciale

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

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

Operațiunea de distrugere trebuie să urmeze proceduri speciale. Cea mai bună cale de distrugere este *arderea*, folosită, de regulă, pentru gunoaiile informatice adunate în pungi speciale. Înaintea arderii ele trebuie păstrate în locuri cu o astfel de destinație. La operațiune vor participa două persoane, care sunt obligate să țină un registru special pentru consemnarea a ceea ce se supune arderii. Cenușa trebuie să fie împrăștiată pentru distrugerea oricărei posibilități de reconstituire a datelor conținute. La fel pot fi distruse și 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 și pentru banda magnetică, microfilm sau benzi tușate.

Fărămițarea se aplică resturilor de hârtie, indigo, bandă magnetică, microfilm, dar o astfel de operațiune trebuie să fie a treia și ca utilizare. Înaintea acestei operațiuni, în cazul benzii magnetice, în primul rând, trebuie tăiată întreaga rolă. Standardele internaționale prevăd ca particulele rezultate din această operațiune să nu fie mai mari de 1/32 inch. De regulă, fărămițarea este recomandată înaintea arderii.

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

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

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

2.10 Clasificarea informațiilor organizațiilor

La nivelul unei organizații, pe un plan corespunzător, ar trebui văzute la fel lucrurile ca și la nivel național, încadrându-se informațiile în mai multe categorii, cu protecții diferite, după cum urmează:

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

Informațiile confidențiale la nivel de unitate, notate cu **C**, corespund celor *secrete* la nivel național, și se atribuie acest calificativ informațiilor și materialelor a căror compromitere ar duce la pierderea unui procent din profitul net anual.

Informațiile private, asemănătoare celor *confidențiale* de la nivel național, notate cu **P**, cuprind informațiile și materialele a căror compromitere poate prejudicia statutul unei persoane din unitate sau al corporației.

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

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

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

La nivel privat, se înregistrează o rețineră mai mare pe linia informațiilor publice și numai documentele cu mențiunea „pentru public” pot fi accesibile tuturor. De fapt, deviza în acest caz este *tot ceea ce nu este permis este interzis*. Totuși, un tratament special îl au informațiile solicitate de organismele guvernamentale de la unitățile private.

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

Și în acest caz, detaliile din legislația românească se află în capitolul 10.

2.10.1 Criterii de clasificare a informațiilor

După amplele discuții din țara noastră privind legile care reglementează informațiile publice și pe cele clasificate, iată câteva criterii generale de clasificare a acestora la nivelul organizațiilor.

Valoarea. Îndeosebi în sectorul privat, valoarea constituie criteriul principal de clasificare. Dacă o informație este valoroasă pentru o organizație sau pentru concurenții ei, atunci ea trebuie să fie clasificată.

În domeniul militar s-a pornit de la valoarea inestimabilă a vieților omenești pierdute prin dezvăluirea informațiilor.

La nivel național, valoarea informațiilor este dată de nivelul prejudiciilor aduse unei țări prin dezvăluirea lor.

Vârsta. În clasificarea informațiilor, în funcție de natura lor, vârsta conduce la stabilirea unei valori diferențiate. Cu cât vechimea e mai mare, cu atât informațiile pierd din valoare, deci pierd din interesul pentru ele. De regulă, în domeniul apărării, informațiile clasificate se declassifică după un anumit număr de ani.

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

Asocierea cu persoanele are influență în procesul de clasificare în funcție de importanța persoanelor care reglementează regimul datelor personale.

2.10.2 Procedurile de clasificare a informațiilor

Atunci când se vorbește despre un sistem de clasificare, trebuie urmăriți pașii de parcurs, după o anumită ordine de prioritate, astfel:

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

2.10.3 Roluri și responsabilități în procesul de clasificare a informațiilor

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

Proprietarul informațiilor poate fi administratorul sau directorul unei organizații. O astfel de persoană răspunde de averile informaționale încredințate. Spre deosebire de custode, proprietarul are responsabilitatea finală a protecției datelor și răspunde în fața legii în cazul neachitării de această obligație. Cu toate acestea, tendința din zilele noastre pe planul protecției datelor este de deplasare în afara unității, de externalizare, prin semnarea actelor de custodie.

Printre responsabilitățile unui proprietar se află:

- întreprinde demersuri pentru stabilirea nivelului de clasificare a informațiilor, care înseamnă, de fapt, cerințele organizației de protejare a acestora;
- efectuează verificări periodice ale clasificărilor existente, în vederea adaptării la cerințele organizației;
- delegă responsabilitatea protejării datelor către un custode specializat și autorizat.

Custodele informațiilor este cel ce prestează un serviciu externalizat organizației, delegându-i-se responsabilitățile pe linia protejării informațiilor. Acest rol este îndeplinit de specialiști în tehnologii informaționale. Dintre obligațiile sale, amintim:

- efectuează copii de siguranță periodice și teste de rutină a validității datelor;
- efectuează restaurări de date din copiile de siguranță, când este cazul;
- întreține datele înregistrate, în concordanță cu politicile de clasificare a informațiilor.

Deseori, custodele are și obligația alcătuirii schemei de clasificare a informațiilor, preluând aceste prerogative de la proprietarul lor.

Utilizatorul. În schema clasificării informațiilor, un utilizator final este considerat orice persoană – operator, angajat, persoană din afară – care, prin prisma locului de muncă, folosește informații. El este considerat consumator de date care are nevoie, zilnic, să acceseze informații pentru a-și duce la îndeplinire obligațiile de serviciu ce îi revin.

În ceea ce-i privește pe utilizatori, aceștia au obligațiile:

- de a urma întocmai procedurile de funcționare, definite prin politicile de securitate ale organizației, și să respecte normele publicate privind utilizarea informațiilor;
- să acorde toată atenția menținerii securității informațiilor în timpul activității prestate, după cum se stipulează în politicile de utilizare a informațiilor emise de organizația proprietară. Ei trebuie să asigure protejarea împotriva accesului neautorizat la informațiile clasificate;
- să folosească resursele informaționale ale firmei numai în scopul urmărit de aceasta, nu și în scop personal.



Completați următorul tabel:

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

CD cu procesul tehnologic de obținere a principalului produs al firmei					
--	--	--	--	--	--

Rezumat

Clasificarea înseamnă etichetări crescătoare ale documentelor sau informațiilor, de la cel mai jos nivel, unde se situează informațiile deschise (*open*) sau neclasificate (*unclassified*), la cele confidențiale, urcând spre informații secrete și strict secrete (*top secret*). În domeniul militar, informațiile care prin compromitere pot *costa vieți umane* sunt marcate „secrete”, în timp ce informațiile a căror compromitere costă *pierderea multor vieți umane* sunt definite „top secret” (strict secrete).

Se practică *două strategii de bază* pe linia securității naționale:

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 informațiilor deosebite: *controlul discreționar al accesului* și *controlul legal al accesului*.

Guvernele împart informațiile în două mari tipuri: *informații subiective* și *informații obiective*. Anterior a operat o altă clasificare: *informații „operaționale”* și *informații „științifice”*. Unii autori au menționat și un al treilea tip de informații clasificate de guverne – *informații „tehnice”*.

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

În *sistemul american de clasificare a informațiilor* există trei niveluri de clasificare: top secret (strict secret), secret și confidențial. Informațiile neclasificate constituie o altă categorie. În România, informațiile clasificate din clasa secretelor de stat sunt încadrate tot în trei niveluri, astfel: strict secrete de importanță deosebită, strict secrete și secrete.

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

Există și informații neclasificate care, prin compilare, trebuie să fie tratate ca informații clasificate. Aceasta nu trebuie să fie o regulă, ci o excepție. Se consideră că sunt două tipuri principale de compilări: compilări care nu adaugă o valoare substanțială (informație) compilatorului; compilări care adaugă o valoare substanțială compilatorului.

Atunci când se efectuează clasificarea unor informații se iau în calcul anumite cerințe de îndeplinit. Când, din diferite cauze, se schimbă circumstanțele, firesc, și cerințele îndeplinite inițial se modifică, situație în care informațiile clasificate se *declasifică* sau trec pe un nivel inferior de clasificare (*degradarea informațiilor*).

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

Pe linia protejării informațiilor speciale pot fi enunțate *10 principii*: delimitării autorizării, securității simple, stea, al integrității I, al integrității II, etichetării, clarificării, inaccesibilității, verificabilității, încrederii în software.

Toate suporturile care conțin informații obținute din prelucrarea automată a datelor trebuie să fie catalogate ca documente ale prelucrării automate a datelor. Tratatamentul lor trebuie să fie similar

documentelor ce conțineau aceleași date în condițiile prelucrării tradiționale. Măsurile de protecție sunt: marcarea materialelor cu regim special, păstrarea și distrugerea materialelor speciale.

La nivelul unei organizații ar trebui văzute la fel lucrurile ca și la nivel național, încadrându-se informațiile în mai multe categorii, cu protecții diferite: *informațiile care necesită un control special, informațiile confidențiale la nivel de unitate, informațiile private, informațiile de uz intern, informațiile publice*. Criteriile generale de clasificare a informațiilor la nivelul organizațiilor sunt: valoarea, vârsta, uzura morală. Rolul și responsabilitățile procesului de clasificare revin proprietarului, utilizatorului sau custodelui.

ANU SE COPIA

CAPITOLUL III

Controlul accesului în sistemele informaționale

După fatidica zi de 11 septembrie 2001, sensul controlului accesului în sistem s-a schimbat radical, atât prin prisma *mijloacelor de exercitare*, cât și a *domeniilor de aplicare*. În privința mijloacelor, dominantă a fost discuția de la sfârșitul 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. Opoziția cea mai puternică venea din partea sistemului bancar, dar nu numai. Alte instrumente păreau incomode sau periculoase și, ca atare, erau refuzate în serie. După data susmenționată lucrurile s-au schimbat radical, în privința identificării biometrice – tendință ce va fi demonstrată într-un paragraf distinct al prezentului capitol. Domeniile de aplicare s-au extins, totul venind din convingerea intimă a proprietarilor și administratorilor de sisteme, văzându-se astfel alte modalități de verificare a persoanelor ce doresc accesul în mai toate instituțiile prezidențiale, guvernamentale și altele de tip public sau privat, iar aeroporturile și-au extins zonele supuse unei atenții speciale.

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

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

- dobândească suficiente cunoștințe pentru stabilirea tipurilor de control al accesului adecvate pentru o anumită organizație și pentru implementarea acestora;
- cunoască modele de control și a modalitățile de combinare a lor;
- dețină suficiente informații pentru stabilirea modalităților de identificare și autentificare a persoanelor necesare unei anumite organizații.

3.1 Tipuri de control al accesului în sistem

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

Controalele *preventive*, după cum sugerează și numele lor, au ca scop preîntâmpinarea apariției unor incidente în sistem; cele *detective* vizează descoperirea unor apariții 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* și *fizice*.

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

Controalele logice sau tehnice cuprind restricțiile de accesare a sistemului și măsurile prin care se asigură protecția informațiilor. Din această categorie fac parte sistemele de criptare, cardurile inteligente, listele de control al accesului și protocoalele de transmisie.

Controalele fizice încorporează, în general, gărzile de protecție și pază, securitatea clădirilor, cum sunt: sistemele de încuiere a ușilor, securizarea camerelor cu servere și 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.

protecția cablurilor, separarea atribuțiilor de serviciu, precum și realizarea copiilor de siguranță a fișierelor.

Controalele vizează responsabilizarea persoanelor care accesează informații sensibile. Responsabilizarea este înfăptuită prin mecanisme de control al accesului care necesită, la rândul lor, exercitarea funcțiilor de *identificare*, *autentificare* și *auditare*. Controalele trebuie să fie în deplină concordanță cu politica de securitate a organizației, iar *procedurile de asigurare* au scopul de a demonstra că prin mecanismele de control se implementează corect politicile de securitate pentru întregul ciclu de viață al sistemului informațional.

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

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

Schematic, aceste perechi sunt redată în figura 3.1.

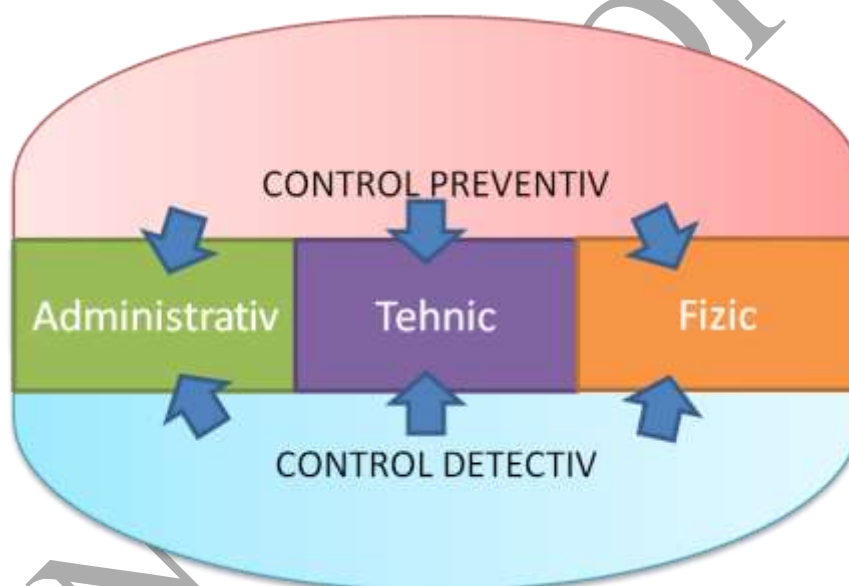


Fig. 3.1 Perechile formelor de control

Controlul preventiv/administrativ

În această variantă, accentul se pune pe responsabilitățile administrative care contribuie la atingerea obiectivelor controlului accesului. Aceste mecanisme cuprind politicile și procedurile organizaționale, verificările de fond înainte de angajare, practicile de încetare a contractului de muncă în condiții normale și anormale, planificarea plecărilor în concediu, etichetarea sau marcarea materialelor speciale, supravegherea mai exigentă, cursuri de instruire în scopul conștientizării importanței securității, conștientizarea modului de comportare, precum și procedurile de semnare a contractului în vederea obținerii accesului la sistemul informațional și la rețea.

Controlul preventiv/tehnic

Împerecherea preventiv-tehnic vizează utilizarea tehnologiilor pentru consolidarea politicilor de control al accesului. Controlul tehnic se mai numește și control logic și poate fi realizat prin sistemele de operare, prin aplicații 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 distanță, parolele, meniurile, softul de scanare a virușilor ș.a.

Controlul preventiv/fizic

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

În această categorie intră împrejuririle cu gard, ecusoanele, ușile multiple (după trecerea printr-o ușă, aceasta se blochează automat, iar la următoarea trebuie cunoscut sistemul de deschidere, persoana fiind captivă între două uși, motiv pentru care se numesc și *uși-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 ș.a.), schița clădirii și a căilor de acces, locurile special amenajate pentru depozitarea suporturilor de informații.

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 și politicile de securitate, verificările de fond, planificarea plecărilor în concediu, marcarea sau etichetarea materialelor speciale, o supraveghere mai exigentă, instruirii cu scopul conștientizării importanței securității. În plus, cu scop detectiv/administrativ sunt controalele ce vizează rotirea personalului la locurile de muncă, exercitarea în comun a unor responsabilități, precum și revizuirea înregistrărilor cu scop de auditare.

Controlul detectiv/tehnic

Măsurile controlului detectiv/tehnic vizează scoaterea în evidență a violării politicii de securitate folosindu-se mijloace tehnice. Aceste măsuri se referă la sistemele de detectare a intrușilor și la rapoartele privind violările securității, generate automat, pe baza informațiilor colectate cu scopul de a fi probă în auditare. Rapoartele pot evidenția abaterile de la funcționarea „normală” sau pot detecta semnături cunoscute ale unor episoade de acces neautorizat.

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

Controlul detectiv/fizic

De regulă, aceste controale necesită *intervenția 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 mișcare.



Analizați modalitățile de control al accesului implementate într-o organizație cunoscută de dvs., încadrându-le în formele combinate prezentate în subcapitolul anterior. Apreciați, în câteva fraze, eficiența controalelor folosite de organizația respectivă.

3.2 Identificarea și autentificarea

În orice sistem de bariere fizice, sistemul de securitate trebuie să discearnă care sunt persoanele autorizate și care sunt vizitatorii și 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 funcție.

De regulă, *identificarea și 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 și jetoane. Ele permit un prim pas de accesare a sistemului. Există marele pericol al pierderii lor sau de dare spre folosință altor persoane.
2. *Ceva care individualizează persoana.* Identificările biometrice sunt o altă variantă de condiționare a accesului. Ele pot fi: amprentele degetelor, buzelor, semnătura, vocea, forma mâinii, imaginea retinei, venele de pe fața externă a mâinii, liniile din palmă, imaginea feței ș.a. Toate aceste tehnici sunt foarte scumpe, în comparație cu cele clasice, și 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 știe.* O parolă, de exemplu, numai că ea se află la discreția oamenilor și, de modul de păstrare a secretului ei sau de ușurința 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 puțin două dintre cele patru căi enumerate; deseori se apelează la combinațiile cartelă-parolă, cheie-parolă, jeton-parolă. În ultimul timp se recomandă ca în sistemele de protecție să se folosească tot mai mult un al treilea element, cel biometric.



- Dați exemple de **2 situații** în care **identificarea și/sau autentificarea** unei persoane se fac folosind **locul geografic în care este înregistrat calculatorul său**. Precizați dacă în exemplul dvs. este vorba de identificare, autentificare sau ambele.
- Dați exemple de **2 situații** în care **identificarea și/sau autentificarea** unei persoane se fac folosind **ceva ce știe o persoană**. Precizați dacă în exemplul dvs. este vorba de identificare, autentificare sau ambele.
- Dați exemple de **2 situații** în care **identificarea și/sau autentificarea** unei persoane se fac folosind **ceva care individualizează persoana (o trăsătură biometrică)**. Precizați dacă în exemplul dvs. este vorba de identificare, autentificare sau ambele.
- Dați exemple de **2 situații** în care **identificarea și/sau autentificarea** unei persoane se fac folosind **ceva aflat în posesia persoanei**. Precizați 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 și proba accesului privilegiat* la informațiile importante ale firmei, întrucât el poate fi dobândit și pe căi ilegale sau poate fi contrafăcut.

Un al doilea principiu arată că *atunci când valorile patrimoniale sunt deosebit de importante și mecanismul de protecție trebuie să fie pe măsură*, iar persoanele cu drept de acces să fie cât mai puține, deci de principiul „trebuie să știe” să beneficieze cât mai puține persoane.

Al treilea principiu, de regulă aplicat informațiilor secrete, este acela că *nici unei persoane nu trebuie să i se garanteze accesul permanent, gestiunea sau cunoașterea informațiilor secrete numai pe motivul poziției ierarhice pe care o deține*. Este o replică la principiul „trebuie să știe”.

Fiecare centru de prelucrare automată a datelor cu mai mult de 25 angajați trebuie să apeleze la sistemul ecusoanelor și la biometrie, ca măsuri suplimentare față de protecțiile 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 distanță, oferă informații despre posesor.

Locurile care nu dispun de uși ce pot fi încuiate trebuie să aibă intrările supravegheate, iar o persoană, ofițer de serviciu, să răspundă de această operațiune, punându-i-se la dispoziție și un sistem de comunicație cu forțele de ordine. Cu același scop, poate fi folosită și televiziunea cu

circuit închis, utilizată de forțele de ordine, cu condiția 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 aceștia să aibă acces în zona prelucrării automate a datelor.



Imaginați câte un exemplu de aplicare pentru principiile de control al accesului enunțate 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 informații suplimentare despre purtător, cum ar fi numele, adresa, contul bancar, contul cardului de debit sau credit, informații medicale, drepturi de acces ș.a. Toate informațiile menționate pot fi codificate prin coduri bară, peliculă magnetică, microprocesoare. Unele dintre carduri conțin și o fotografie a proprietarului, realizată, prin noile tehnologii, direct pe card.

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

Practica oferă și *ecusoane-active*, care apelează la identificarea prin frecvențe radio (RFID - Radio-frequency identification), fără să fie nevoie de trecerea cartei prin fața unui cititor special. De asemenea, prin tehnologiile infraroșu se poate realiza citirea conținutului unei cartele de la câțiva 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-și schimbă culoarea după un timp bine controlat, astfel încât să nu mai poată fi reutilizate. Ambele metode se folosesc, îndeosebi, pentru vizitatorii organizațiilor.

Viitorul este al cardurilor inteligente, însă mulți potențiali beneficiari spun „Cardurile inteligente par a fi cea mai bună soluție pentru problema noastră. În schimb, le vrem mai performante pentru a răspunde la toate cerințele noastre”².

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

Lumea cardurilor este într-un moment crucial. Șansele sunt reale, dar parteneriatele aproape că sunt obligatorii. Don Davis (op. cit.) opina „Este mai bine să împarți 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, prezentați comparativ, în termeni de avantaje și dezavantaje, două soluții de control acces și pontaj al angajaților cu ajutorul ecusoanelor active RFID.

3.2.3 Controlul accesului prin biometrie

Dumnezeu l-a făcut pe om după chipul și asemănarea lui, dar, cum oamenii s-au înmulțit, s-a simțit 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 feței persoanei sau a vocii. După mii de ani s-au menținut aceste forme de identificare, întrucât și astăzi *portretele-robot* sunt realizate tot pe această cale, dar cu ajutorul calculatoarelor.

Un moment important l-a constituit *inventarea fotografiei*. Ea încă se folosește la identificarea și autentificarea persoanei prin plasarea pe buletinele de identitate, pașapoarte, legitimații ș.a. Sistemul este util poliției, lucrătorilor de la frontieră, organizațiilor comerciale, bancare, diverselor instituții ș.a.

Invenția *amprentelor digitale* a condus la apariția altui mod de identificare și 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 potențialii beneficiari direcți supuși unor metode de identificare ce le-ar fi afectat sănătatea sau intimitatea. Cum invențiile și inovațiile din domeniu nu au ținut cont de părerile lor, au apărut o mulțime de tehnologii biometrice în sistemele de securitate a organizațiilor. Unele dintre realizări sunt de-a dreptul stranii, deși nu au nimic în comun cu biometria. Ne referim la viitoarele camere de luat vederi presărate peste tot: pe străzi, pe holurile instituțiilor, acasă, în mijloacele de transport. În Anglia, există deja 1.500.000 de camere de luat vederi pe străzi, Londra având introdus sistemul cu mulți ani în urmă. Mai mult, noile camere de luat vederi pot dezbrăca, la propriu, trecând peste veșmintele protectoare ale persoanei, sau pot trece prin pereții camerelor. Unde mai este protejată intimitatea!?!

Revenind la biometrie, am putea face referire și la angajații 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 și identificarea celui ce dorește să lucreze la un calculator. Sistemul a cam bulversat angajații lui Bill Gates, dar se pare că s-au obișnuit cu el.

Mai șocantă 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 dețină un *document purtător al datelor biometrice*. Totul se bazează pe ideea ca posesorul unui pașaport furat sau al unei vize false să fie identificat prin amprenta digitală, a irisului, retinei sau feței – în funcție de tehnica biometrică adoptată. Oricum, se conturează obligativitatea includerii componentelor biometrice în toate actele de călătorie în doar câțiva ani, ceea ce conduce la dezvoltarea unei puternice industrii biometrice și a altelea, a cardurilor inteligente.

Se preconizează că vor avea un demaraj foarte puternic *tehnologiile bazate pe recunoașterea feței și a amprentelor digitale*, cărora li se va alătura, într-o mai mică măsură, *recunoașterea irisului*. Oricum acestea sunt și cele trei elemente biometrice recomandate de Organizația Internațională de Aviație Civilă, cu sediul la Montreal, din care fac parte peste 188 de țări. 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	Recunoașterea feței	Amprenta digitală	Recunoașterea 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 octeți	250-1000 octeți	512 octeți	9 octeți
Numărul furnizorilor principali	2	Peste 25	1	1
Prețul echipamentelor	Moderat	Mic	Mare	Moderat
Factorii ce afectează probele luate	Lumina, orientarea feței, 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.

Informații suplimentare despre biometrie se pot obține de pe următoarele adrese web:

- www.ibia.org – Asociația Internațională a Industriei Biometrice
- www.visionics.com – Recunoașterea feței
- www.identix.com – Amprenta digitală
- www.recogsys.com – Amprenta digitală
- www.iriscan.com – Recunoașterea irisului
- www.eyeticket.com – Recunoașterea irisului

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

- biometria și 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 aplicații în care este folosită. În funcție de aplicație, există mai multe opțiuni pentru soluția biometrică optimă, astfel încât să fie diminuate amenințările la care este supus sistemul;
- în ceea ce privește problema complexă a securității informaționale, cercetările în dezvoltare vor oferi soluții ce vor fi supuse testelor, ele constituind variante biometrice integrate pentru asigurarea protecției și securității noilor sisteme;
- tot pe linia preocupărilor internaționale, se vor realiza standarde și produse biometrice care să acopere o cât mai largă paletă a cerințelor beneficiarilor și ale aplicațiilor.

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



- Care este, în opinia dvs., cea mai spectaculoasă/utilă/eficientă/nouă tehnologie biometrică? Justificați
- Identificați alte tehnologii biometrice decât cele descrise mai sus și prezentați-le pe scurt.
- Prezentați și analizați controversa iscată la introducerea pașapoartelor 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 întrebunțat și în lumea calculatoarelor. Uneori, dintr-o dragoste excesivă față de trecut, utilizatorii greșesc, rămânând în aceeași lume, și, ca atare, apelează și în acest caz la arhicunoscutele cuvinte magice ale copilăriei. Un astfel de comportament este intuit și de spărgătorii de sisteme, care, nu de puține ori, reușesc să le acceseze pe această cale. Multe „uși informatice” s-au deschis la aflarea parolei „SESAM”, dar, oricât de drag ne-ar fi cuvântul, utilizarea lui este total neinspirată.

Așadar, 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, și, eventual, oferirea unui jeton de acces, cei interesați prezintă sistemului propria lor parolă, fie prin tastarea de la un terminal, fie prin introducerea într-un echipament special al unui document care să conțină parola. Calculatorul compară parola cu o listă aprobată a acestora, aflată în softul sistemului, permițându-i-se accesul și garantându-i-se respectarea privilegiilor predefinite la anumite resurse ale sistemului, astfel:

- *Execuție.* Poate lansa în execuție un program, dar nu i se permite să umble la structura acestuia, prin adăugarea sau modificarea unor linii.
- *Citire.* Se poate citi un fișier, dar nici o altă operațiune nu mai este permisă.
- *Scriere.* Se oferă posibilitatea de scriere a datelor în fișierul deschis, dar se interzic alte operațiuni.
- *Citire-Scriere.* Se poate citi fișierul și, 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 fișierului deschis.
- *Ștergere.* Utilizatorul poate efectua ștergerea unor date din fișier.

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

Problema parolelor nu este încă suficient de bine înțeleasă de utilizatorii lor, apelându-se la forme foarte scurte, la nume ale eroilor din filme, din basme, la numele soției sau soțului, al copiilor, la numărul autoturismului ș.a. – toate vulnerabile în fața unor spărgători calificați. O altă greșală, amintită și 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 funcții în sistem și nu trebuie să fie un proces generalizat, dându-se tuturor celor ce dețin poziții importante în conducerea firmei. În cazul sistemelor ce conțin informații speciale, parolele se atribuie de ofițerul cu securitatea sistemului. A da astfel de parole în folosința unor persoane echivalează cu permisiunea acestora de a accesa cele mai importante averi ale firmei.

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

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

2. utilizatorii își păstrează parolele, din precauția de a nu le uita, pe bucăți de hârtie lăsate în văzul tuturor;
3. pentru o memorare ușoară 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, totuși, cele mai uzuale parole date după celebrul mesaj al sistemului PASSWORD, ceea ce înseamnă parola sau cuvântul de trecere, sunt ... PASSWORD (ceea ce în românește ar însemna folosirea cuvântului PAROLA) și SECRET.

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

Din cele relatate, rezultă că o parolă este și o cheie și trebuie să i se poarte de grijă ca și 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 șase luni, dar pentru datele deosebit de importante se impun termene și mai scurte;
2. parolele comune trebuie schimbate imediat ce o persoană părăsește grupul sau nu mai are dreptul utilizării lor;
3. parolele trebuie să fie schimbate imediat ce se constată unele bănuieli privind cunoașterea lor de persoane neautorizate sau atunci când, din motive de forță majoră, secretul lor a trebuit să fie dezvăluit pentru redresarea unei stări anormale temporare;
4. parolele trebuie să fie ținute minte și nu scrise pe oriunde, cu excepția următoarelor cazuri:
 - a) trebuie să fie scrise pentru intervenții de urgență;
 - b) fiecare parolă scrisă va fi introdusă într-un plic sigilat și marcat în exterior cu scurte detalii privind calculatorul la care poate fi folosită și numele celor autorizați a le folosi;
 - c) plicul respectiv are tratamentul asemănător averilor protejate sau al categoriei de informații accesate prin parolă. După ruperea sigiliului, pe plic vor fi scrise data și 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 fișiere trebuie să fie protejate împotriva accesului neautorizat și create copii de siguranță. Accesul la acest fișier 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 afișate niciodată pe echipamentele din configurația 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 puțin opt caractere. Ele sunt caractere alfanumerice - litere (mari și mici), cifre și spații, folosite în ordine aleatoare, ceea ce ar însemna câteva mii de cuvinte de opt sau mai puține caractere, care pot fi testate cu ajutorul calculatorului, în doar câteva minute, deci sunt suficient de vulnerabile pentru „profioniștii” în spargeri de sisteme;
8. pentru blocarea operațiunilor 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 depășită de către utilizator, intenția trebuie să fie raportată conducătorului sistemului sau responsabilului cu securitatea, însoțită de un semnal sonor specific de avertizare. În acest timp trebuie să se blocheze terminalul de la care s-au efectuat prea multe încercări eșuate. Repunerea lui în funcțiune stă la îndemâna conducătorului sistemului. În cazul sistemelor speciale, se recomandă și 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-și schimbe identitatea cu care au efectuat deschiderea sesiunii și nici să nu poată pătrunde în partițiile alocate altor utilizatori;

10. dacă un terminal funcționează o perioadă lungă de timp, procesul de autentificare trebuie să aibă loc la intervale regulate de timp pentru a se asigura că nu folosește 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 cunoștință 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 aceleași și ambele să fie la fel de bune cunoșcătoare ale consecințelor declanșării unor operațiuni de la calculator.

Pentru preîntâmpinarea unor aspecte vulnerabile din sistemul de protecție prin parole, se recomandă apelarea la un semn special sau la o dovadă de recunoaștere 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 și 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 acționează pe principiul calculatoarelor portabile. Ele sunt sisteme speciale de criptare, care generează valori (parole) de autentificare personală a utilizatorilor și 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, îmbunătățindu-se substanțial principiul simplu al parolilor.



Faceți un inventar al parolilor pe care le folosiți în prezent. Enumerați greșelile pe care le faceți în legătură cu parolele și, dacă sunt necesare, propuneți câteva îmbunătățiri ale modului de utilizare a parolilor dvs.

3.2.5 Controlul geografic al accesului în sistem

Într-o declarație a unui cunoscut om de afaceri din Rusia, Kasperski, se pune problema legitimării persoanelor utilizatoare de servicii informatice și comunicații din spațiul global, tocmai pentru a se asigura responsabilizarea și conștientizarea participanților la noul tip de trafic. El făcea asemănarea cu sistemul de conducere a automobilelor de la începutul secolului XX, când, fiind atât de puține, în caz de accident, era foarte ușor de identificat proprietarul – de cele mai multe ori el fiind și conducătorul. Odată cu explozia de automobile de pe piață s-a simțit nevoia identificării proprietarului mașinii, prin *cartea de identitate a mașinii* și prin *certificatul de înmatriculare*, dar și a conducătorului auto, prin *permisul de conducere*.

La fel trebuie să se întâmple și cu deținătorii și utilizatorii de calculatoare, deoarece, în prezent, multe acțiuni malițioase se desfășoară de persoane necunoscute, aflate în locuri învăluite în mister.

Autentificarea bazată pe localizarea geodezică (*location-based authentication*) este o metodă de autentificare a entităților din spațiul cibernetic bazată pe localizarea geodezică (latitudinea, longitudinea și altitudinea unui loc geografic bine definit). Aceasta va avea ca efect delimitarea porțiunii din spațiul cibernetic de unde se declanșează un anumit eveniment. Se face astfel breșă într-un sistem destul de întrebuițat de atacatorii sistemelor aflați într-un colț al planetei, săvârșind fărădelegi în al colț al acesteia, susținând că se află în cu totul altul.

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

constelație de 24 de sateliți ai GPS (*Global Positioning System*) pentru calcularea și validarea unei *semnături a locației*, care este unică pentru fiecare loc de pe pământ în fiecare moment solicitat. Fiecare utilizator al unui sistem protejat are un senzor al semnăturii locației (SSL), care este un tip special al receptorului GPS. SSL interceptează semnalele GPS și transmite semnătura sa către o gazdă ce va face autentificarea. Gazda folosește semnalele GPS colectate de propriul SSL, plus informațiile 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 performanțe de acuratețe până la nivelul câtorva metri sau chiar și mai bune (zeci de centimetri). Pentru că observațiile GPS ale unui site anume sunt impredictibile prin simulări anticipate, la un nivel cerut de acuratețe, schimbate constant, unice oriunde ar fi, este practic imposibil de contrafăcut semnătura.

Autentificarea prin localizarea geodezică are câteva caracteristici esențiale. Ea asigură o protecție continuă împotriva celor rău intenționați aflați la distanță. Semnătura locației poate fi folosită ca un mijloc comun de autentificare. Știindu-se reperele unui utilizator, se poate identifica ușor un intrus, dar se pot oferi și probe că o persoană nu a fost în locația respectivă în momentul săvârșirii unei fapte condamnabile. O astfel de protecție este recomandată pentru site-urile fixe, în care se poate plasa un senzor pe acoperiș sau la fereastră, cu condiția orientării spre cer. Facem mențiunea că semnalele GPS nu trec prin ziduri și acoperișuri. Deocamdată sunt unele limite tehnologice ale utilizării senzorilor în cazul utilizatorilor mobili.

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



În ce sisteme/situații considerați 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 și a domeniilor de aplicare. Controalele sunt introduse pentru diminuarea riscurilor la care sunt expuse sistemele și pentru reducerea potențialelor pierderi. Controalele pot fi *preventive*, *detective* sau *corective*. Pentru atingerea obiectivelor, controalele pot fi *administrative*, *logice sau tehnice* și *fizice*. Există și forme combinate de control: preventiv/administrativ, preventiv/tehnice, preventiv/fizic, detectiv/administrativ, detectiv/tehnice, detectiv/fizic.

Identificarea și autentificarea persoanelor se efectuează în patru moduri: prin ceva aflat în posesia persoanei, ceva care individualizează persoana, ceva ce știe 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 și proba accesului privilegiat; atunci când valorile patrimoniale sunt deosebit de importante și mecanismul de protecție trebuie să fie pe măsură; nici unei persoane nu trebuie să i se garanteze accesul permanent, gestiunea sau cunoașterea informațiilor secrete numai pe motivul poziției ierarhice pe care o deține.*

CAPITOLUL IV

Politici, standarde, norme și proceduri de securitate

Orice organizație care dorește să-și apere valorile informaționale trebuie să conceapă o modalitate logică și coerentă de protejare a acestora, ținând seama de recomandările legale în domeniu și de realitățile specifice activității sale. Ea va analiza pe de o parte pericolele interne și externe, iar pe de altă parte metodele disponibile de contracarare a lor. Demersurile sale se vor concretiza, printre altele, în politici, standarde, norme și proceduri de securitate.

Obiectivele capitolului curent sunt:

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

4.1 Modele de politici de securitate

Situația definirii politicilor de securitate a devenit complicată atunci când sistemul militar de clasificare a informațiilor a fost preluat ca model de domenii civile, cum sunt cel economic, politic, medical ș.a., informațiile fiind grupate în două mari categorii: clasificate (confidențiale, secrete, strict secrete) și neclasificate (sau publice). Lucrurile s-au complicat și mai tare după ce britanicii au mai introdus un nivel, RESTRICTIONATE, între informațiile NECLASIFICATE și cele CONFIDENȚIALE. Și în SUA a existat acest nivel dar, odată cu promulgarea legii accesului liber la informații (*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 informații, în timp ce informațiile neclasificate, dar sensibile (*Unclassified but sensitive*) includ FOUO plus datele ce pot fi făcute publice, ca efect al FOIA.

În Marea Britanie, informațiile restricționate, în practică, sunt făcute publice, dar marcajul aplicat, RESTRICTIONATE, face ca jurnaliștii și alte categorii interesate de scurgeri de informații să fie sancționați dacă le fac publice, ca efect al legii secretului oficial. Este o ciudățenie care se adaugă altele: documentele neclasificate din SUA care traversează oceanul în Marea Britanie devin automat RESTRICTIONATE, iar dacă se transmit înapoi în SUA devin CONFIDENȚIALE – 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 informațiile de orice tip pot fi supuse altor restricții, numite *clasificare compartimentală* (în varianta americană) sau *securitate multilaterală* (în varianta europeană). Se utilizează în acest scop *descriptori, cuvinte-de-avertizare și marcaje internaționale de apărare (International Default Organization, IDO)*.

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

4.1.1 Modele de securitate multinivel

Când privim un sistem, din punct de vedere al securității lui, întregul este separat în părți, prin linii orizontale, realizându-se așa-zisa securitate pe niveluri multiple (multinivel) prin care se face o delimitare netă între categoriile de informații din sistem (publice, confidențiale, secrete,

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

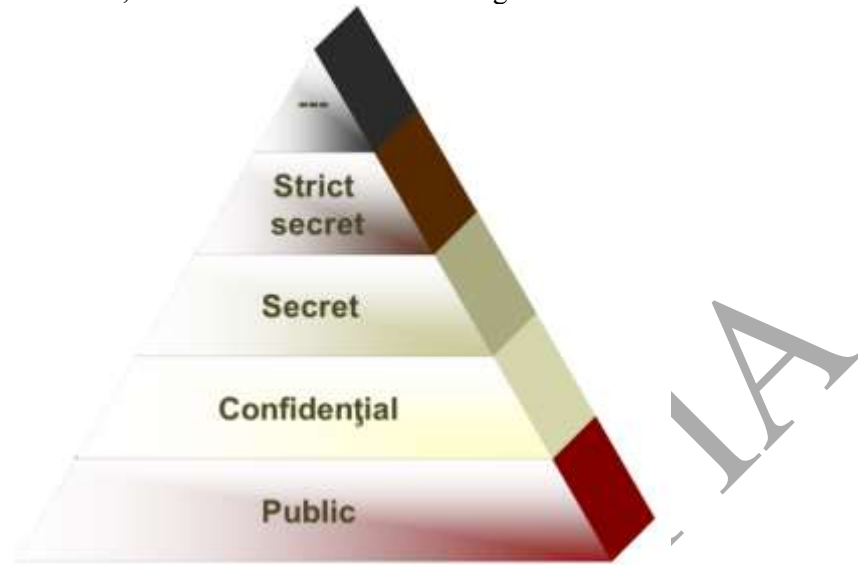


Fig. 4.1 Model de securitate multinivel

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

Modelul Bell-LaPadula

Cel mai cunoscut model al politicilor de securitate este cel propus de David Bell și Len LaPadula, în 1973, ca răspuns la preocupările Forțelor 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 și „sigure multinivel” sau MLS (*MultiLevel Secure*). Proprietatea de bază a acestor sisteme este aceea că *informațiile pot circula în jos*.

Formal, modelul Bell-LaPadula a introdus trei principii:

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

Cele trei principii sunt redată în figura 4.2.

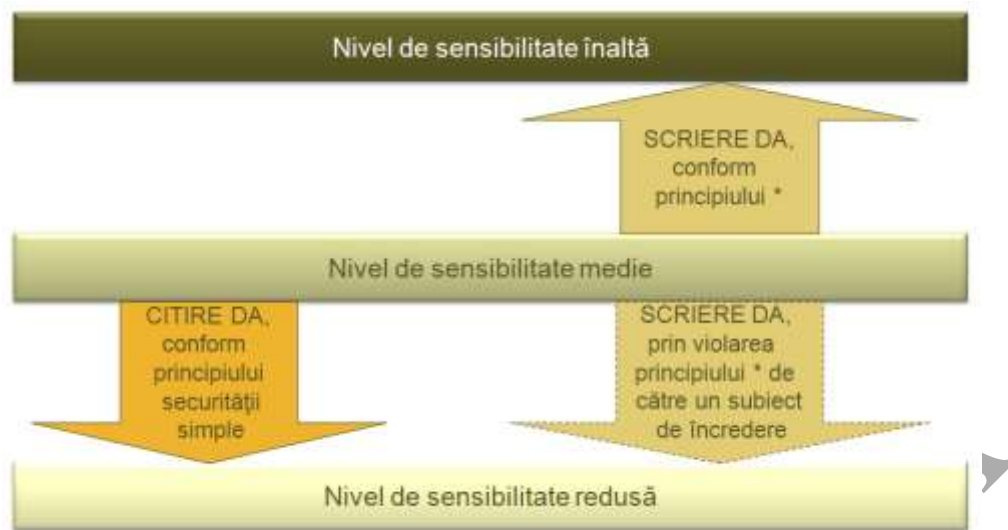


Fig. 4.2 Modelul Bell-LaPadula, cu cele trei principii

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 *citește, scrie, execută* ș.a. Un *subiect de încredere* este o entitate activă care își 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 fișierele sau o resursă de stocare. Sunt cazuri în care un element poate fi, într-un anumit context, subiect și, 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 competențe*. Modelul matricei de control al accesului acceptă controlul discreționar al accesului pentru că intrările în matrice sunt la discreția persoanelor care au autorizația de a completa tabelul.

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

SUBIECT /OBIECT	FIȘIER 1	FIȘIER 2	PROCES 1	FIȘIER 3
SUBIECT 1	Execută	Citește	Citește/ Scrie	Scrie
SUBIECT 2	Aprobă	Execută	Citește	Scrie
SUBIECT 3	Citește/Scrie	Aprobă	Execută	Nimic
SUBIECT 4	Citește	Citește/Scrie	Aprobă	Scrie

Fig. 4.3 Matrice de control al accesului

Modelul Biba

În multe cărți este amintit și modelul Biba, al lui Ken Biba, ocupându-se doar de integritatea sistemelor, nu și de confidențialitate. El se bazează pe observația că în multe cazuri confidențialitatea și integritatea sunt concepte duale: în timp ce prin confidențialitate se impun restricții celor ce pot citi un mesaj, prin integritate sunt controlați cei ce pot să scrie sau să modifice un mesaj.

În unele organizații guvernamentale sau comerciale există aplicații în care integritatea datelor este mult mai importantă decât confidențialitatea, ceea ce a făcut să apară modele formale ale integrității.

Integritatea vizează trei scopuri principale:

- protejarea datelor împotriva modificărilor efectuate de utilizatorii neautorizați;
- protejarea datelor împotriva modificărilor neautorizate efectuate de utilizatori autorizați;
- asigurarea consistenței interne și externe a datelor.

Modelul a fost realizat în 1977 ca unul al integrității datelor, așa cum modelul Bell-LaPadula este cunoscut ca modelul confidențialității datelor. Modelul Biba este unul de tip rețea și folosește *relația mai mic sau egal*. O structură a rețelei este definită ca un ansamblu parțial ordonat cu cea mai mică limită superioară, LUB (*Least Upper Bound*), și cea mai mare limită inferioară, GLB (*Greatest Lower Bound*).

O rețea reprezintă un ansamblu de clase de integritate (CI) și de relații ordonate între aceste clase. Ea poate fi definită astfel:

$$(CI, \leq, LUB, GLB).$$

Așa cum Bell-LaPadula operează cu niveluri diferite de sensibilitate, modelul Biba clasifică obiectele în diferite niveluri de integritate. Modelul enunță trei axiome ale integrității:

1. *axioma integrității simple*. Ea stabilește 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 integrității ** (se citește stea) stabilește 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 și modelul Biba sunt redată 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 ș.a.

4.1.2 Modele ale securității multilaterale

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

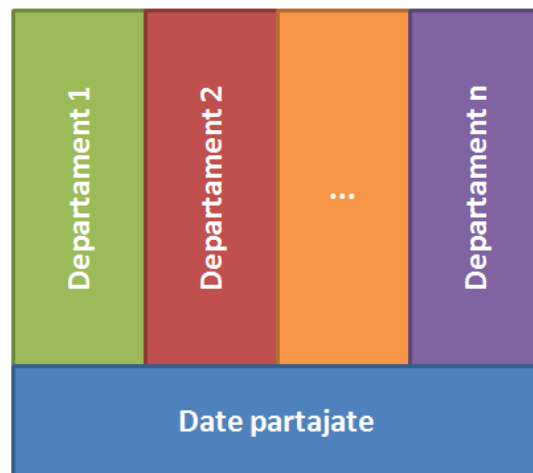


Fig. 4.5 Modelul securității multilaterale

Acest control al fluxurilor informaționale laterale este unul organizațional, așa cum este cel al organizațiilor secrete, pentru păstrarea în taină a numelor agenților care lucrează în alte țări, fără să fie cunoscuți de alte departamente speciale. La fel se întâmplă și în companii, unde separarea verticală a compartimentelor, după funcțiile îndeplinite (producție, comercială, personal-salarizare ș.a.), conduce la o situație identică.

Există cel puțin trei modele diferite de implementare a controlului accesului și de control al fluxurilor informaționale prin *modelul securității 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 informaționale din domeniul sănătății, conform cu etica medicală.

Compartimentarea și modelul rețea

Ani mulți acest model a servit ca practică standard, în SUA și guvernele aliate, pentru restricționarea accesului la informații, prin folosirea cuvintelor-cod și a clasificărilor. Este arhicunoscut cuvântul-cod *Ultra*, folosit în cel de-al doilea război mondial, de către englezi și americani, pentru decriptarea mesajelor criptate de germani cu mașina Enigma. Cercul persoanelor cu acces la mesajele decriptate fiind foarte redus, numărul autorizărilor pentru informații de pe cel mai înalt nivel de clasificare era mult mai mare. Prin folosirea cuvintelor-cod se creează o puternică subcompartimentare, chiar a categoriei strict secret și deasupra ei.

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

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

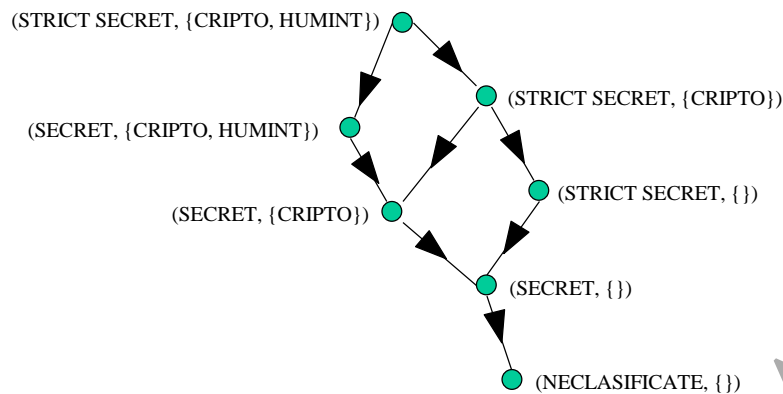


Fig. 4.6 Model rețea cu etichete de securitate

Modelul zidului chinezesc

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

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

Modelul BMA (British Medical Association)

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

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

Scopul modelului politicii de securitate BMA este acela de consolidare a *principiului consimțământului pacientului* și de a preveni accesul prea multor persoane la datele personale din bazele de date ce le conțin. Totul s-a rezumat la un nou sistem de codificare. Politica BMA se bazează pe nouă principii, formulate foarte pe scurt astfel: controlul accesului, deschiderea înregistrărilor, controlul modificărilor din liste, consimțământul și notificarea clientului, persistența, marcarea accesului pentru a servi ca probă în justiție, urmărirea fluxului informațiilor, controlul agregării informațiilor, încrederea în sistemele informatice.

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



Realizați o matrice de control al accesului pentru un (sub)sistem informațional cunoscut.

4.2 Programul de securitate

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

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

4.2.1 Politicile

O politică, deseori, înseamnă mai multe lucruri, atunci când ne referim la securitatea informațională a unei organizații. Cineva poate să se rezume doar la firewall-urile folosite pentru controlarea accesului și a traseelor pe care circulă informațiile, altcineva se gândește la lacătele, cardurile de acces, camerele de luat vederi ce înregistrează totul din perimetrele controlate. Dar, câte alte accepțiuni 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 *Declarația politicii organizației (Statement of Policy)*. Aceasta este o formulare generală, o declarație din care să reiasă:

- importanța resurselor informaționale pentru atingerea obiectivelor strategice ale organizației;
- formularea clară a sprijinului acordat tehnologiilor informaționale în unitate;
- angajamentul top managerilor de a autoriza sau coordona activitățile de definire a standardelor, procedurilor și normelor de securitate de pe nivelurile inferioare.

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

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

De regulă, politicile obligatorii au două scopuri de bază:

- asigurarea că o organizație urmează procedurile standard sau politicile de bază din domeniul ei de activitate;
- de a oferi încredere organizațiilor că ele urmează standardele și politicile de securitate din domeniul de activitate.

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

Politicile informative au scopul de a informa cititorii. Nu poate fi vorba de cerințe specifice, iar interesații de aceste politici pot să se afle în interiorul organizației 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 intenției vizate de politică și ea va scoate în relief și legăturile existente cu întreaga documentație a organizației. Formularea trebuie să fie scurtă și se plasează la începutul documentului;
- *declararea politicii top managerilor* se include la începutul documentului și are dimensiunea unui singur paragraf, specificând scopul global al politicii;
- *responsabilitățile* constituie conținutul unei secțiuni distincte și cuprind persoanele implicate în asigurarea bunei funcționări a politicii;
- *consecințele*: printr-o astfel de formulare se prezintă pierderile posibile dacă politica nu va fi respectată;
- *monitorizarea*: se specifică modul în care se monitorizează respectarea și actualizarea continuă a politicii;
- *excepțiile*: se menționează cazurile în care apar excepții și modalitățile de tratare a lor; de regulă, au o durată limitată de aplicare, de la un caz la altul.

4.2.2 Standardele, normele și procedurile de securitate

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

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

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

Standardele

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

- *scopul și aria de aplicare*, prin care se oferă o descriere a intenției standardului (realizarea unui tip de server pe o anumită platformă);
- *roluri și responsabilități* la nivel de corporație pe linia definirii, execuției și promovării standardului;
- *standardele cadrului de bază*, prin care sunt prezentate declarațiile de pe cel mai înalt nivel, aplicabile platformelor și aplicațiilor;

- *standardele tehnologiei* conțin declarațiile și descrierile aferente (configurația sistemului sau serviciile nesolicitate de sistem);
- *standardele administrării* reglementează administrarea inițială și în timpul exploatării platformei și aplicațiilor.

Normele

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

Elementele principale ale unei norme de securitate informațională sunt:

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

Procedurile

Procedurile prezintă pașii detaliați ce trebuie să fie parcurși pentru execuția unei activități. Se descriu acțiunile concrete pe care trebuie să le efectueze personalul. Prin ele se oferă cele mai mici detalii pentru implementarea politicilor, standardelor și normelor. Uneori se folosește în locul acestui concept cel de *practici*.

4.2.3 Aspecte practice ale politicii de securitate informațională¹

Pentru realizarea propriei politici de securitate există mai multe puncte de pornire. În primul rând, literatura de specialitate este destul de bogată și poate fi consultată cu multă ușurință. Pentru cei mai comози, 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 organizației. Și, fiindcă am amintit site-ul de mai sus, tot aici veți putea vedea structura standardului internațional de definire a politicii de securitate, ISO 17799, bazat pe standardul britanic BS7799. El este organizat pe 10 secțiuni, fiecare acoperind domenii sau teme diferite, după cum urmează:

1. *Planificarea funcționării neîntrerupte a unității*, cu obiectivul contracarării întreruperilor de activitate ale unității și ale proceselor principale ca efect al unor accidente majore sau dezastre.
2. *Controlul accesului în sistem*, cu obiectivele:
 - 2.1) controlarea accesului la informații;
 - 2.2) prevenirea accesului neautorizat în sistemul informațional;
 - 2.3) asigurarea protecției serviciilor prestate în rețea;
 - 2.4) prevenirea accesului neautorizat la calculatoare;
 - 2.5) detectarea activităților neautorizate;
 - 2.6) asigurarea securității informațiilor când se folosesc comunicațiile mobile și tele-activitățile.
3. *Dezvoltarea și întreținerea sistemului*, cu obiectivele:
 - 3.1) asigurarea securității prin sistemul operațional;

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

- 3.2) prevenirea pierderilor, modificărilor sau folosirii inadecvate a datelor din aplicațiile sistemului;
 - 3.3) protejarea confidențialității, integrității și autenticității informațiilor;
 - 3.4) asigurarea că proiectele informatice și activitățile colaterale se derulează după proceduri sigure;
 - 3.5) menținerea securității softului și datelor din aplicațiile sistemului.
4. *Securitatea fizică și a mediului*, cu obiectivele:
 - 4.1) prevenirea accesului neautorizat, a distrugerilor și interferențelor cu informațiile și celelalte componente ale sistemului;
 - 4.2) prevenirea pierderilor, distrugerilor sau compromiterilor valorilor patrimoniale, precum și stoparea întreruperilor de activitate;
 - 4.3) prevenirea compromiterii sau furtului de informații și al altor resurse informaționale.
 5. *Maleabilitatea*, cu obiectivele:
 - 5.1) preîntâmpinarea încălcării cadrului juridic, a celui statutar, regulamentar sau a oricărei obligații contractuale, precum și a cerințelor pe linia securității;
 - 5.2) asigurarea maleabilității sistemului la politicile și standardele organizaționale pe linia securității;
 - 5.3) maximizarea eficienței procesului de auditare a sistemului și minimizarea interferențelor 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 conștienți și preocupați de preîntâmpinarea sau diminuarea amenințărilor asupra securității informațiilor, susținând politica de securitate a organizației prin tot ceea ce fac zi de zi;
 - 6.3) minimizarea pagubelor provocate de incidentele apărute în sistem sau de proasta funcționare a acestuia, precum și reținerea incidentelor ca lecții pentru viitor.
 7. *Organizarea securității*, cu obiectivele:
 - 7.1) asigurarea managementului securității informaționale în cadrul organizației;
 - 7.2) asigurarea securității componentelor folosite în prelucrarea informațiilor organizației accesate de către terți;
 - 7.3) asigurarea securității informațiilor când responsabilitatea prelucrării acestora revine unei alte organizații, ca serviciu externalizat.
 8. *Managementul resurselor informatice și al exploatarii lor*, cu obiectivele:
 - 8.1) asigurarea funcționării corecte și sigure a componentelor sistemului informatic;
 - 8.2) minimizarea riscului căderii sistemului;
 - 8.3) protejarea integrității softului și a informațiilor;
 - 8.4) asigurarea integrității și disponibilității informațiilor prelucrate și comunicate;
 - 8.5) asigurarea încrederii în informațiile din rețele și protejarea infrastructurii corespunzătoare;
 - 8.6) prevenirea pierderilor de valori patrimoniale și a întreruperilor de activitate;
 - 8.7) prevenirea pierderilor, modificărilor sau utilizărilor ilegale în schimburile de informații cu alte organizații.
 9. *Clasificarea și controlarea valorilor patrimoniale*, cu obiectivele:
 - 9.1) menținerea unei protecții corespunzătoare a valorilor patrimoniale ale organizației;
 - 9.2) oferirea încrederii că valorile patrimoniale informaționale au asigurat un nivel de protecție corespunzător .
 10. *Politica de securitate*, cu obiectivele:
 - 10.1) oferirea de direcții manageriale;
 - 10.2) sprijinirea acțiunilor întreprinse pe planul securității informaționale.

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

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

În prezent, ISO/IEC 27001 este standardul formal în baza căror organizațiile își pot certifica sistemele de management al securității informațiilor (SMSI). Standardul acoperă toate domeniile de activitate și specifică cerințele pentru stabilirea, implementarea, operarea, monitorizarea, revizia, întreținerea și îmbunătățirea unui SMSI documentat.

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

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

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

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

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

- *Politica de Securitate*: orice organizație trebuie să aibă un document care să definească și să explice securitatea informațională;
- *organizarea securității*: definește principiile care stau la baza managementului securității în orice organizație;
- *securitatea personalului*: descrie cerințele legate de recrutarea și instruirea angajaților și managementul incidentelor din sistem;
- *securitatea fizică și a mediului de lucru*: sunt avute în vedere controalele generale implementate în cadrul organizației;
- *managementul operațional și al comunicațiilor*: acoperă procedurile documentate cu privire la operarea la calculator și comunicarea informațiilor;
- *controlul accesului*: principiile care guvernează accesul securizat la informații;
- *dezvoltarea și întreținerea sistemelor*: cerințele legate de securitate trebuie avute în vedere în fiecare etapă a ciclului de viață al unui sistem;
- *planificarea continuității afacerii*: analiza de impact, proceduri de refacere, testare;
- *conformitatea*: securitatea informațională trebuie să fie conformă cu orice prevedere legală aplicabilă.

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

² La adresa <http://www.bsi-global.com/>



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

Sistemul de management al securității (SMSI) trebuie să faciliteze relația dintre procesele IT și resursele implicate și se concentrează asupra:

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

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

Pe scurt, cele patru faze presupun:

Plan (stabilirea SMSI)

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

Do (Implementarea și operarea SMSI)

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

Check (Monitorizarea și revizia SMSI)

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

Act (Întreținerea și îmbunătățirea SMSI)

- Implementarea măsurilor de îmbunătățire identificate
- Formularea acțiunilor corective și preventive
- Validarea îmbunătățirilor

Pentru a fi în conformitate cu ISO 27001, o organizație trebuie să aibă implementat și documentat propriul sistem de management al securității informaționale, în conformitate cu obiectivele de control.

Certificarea ISO este cea care oferă probe și asigurări că o organizație 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 obține conformitatea cu acest standard este similar cu obținerea certificării ISO 9000. Etapele obținerii acestei certificări pot fi sintetizate astfel:

- organizația decide să implementeze prevederile ISO 27001;

- odată luată această decizie, conducerea trebuie să desemneze o echipă care să elaboreze Politica de Securitate a organizației;
- acest document trebuie revizuit, aprobat și adus la cunoștința tuturor angajaților;
- organizația trebuie să stabilească apoi scopul certificării, care poate fi o componentă funcțională, un departament sau întreaga organizație;
- acest scop trebuie documentat, rezultând *ISMS Scope Document* (Scopul Sistemului de Management al Securității Informaționale);
- în cadrul acestui Scop, trebuie identificate activele organizației (și valoarea asociată acestora) care trebuie protejate (Inventarul activelor);
- pentru acest inventar se va realiza Analiza de Risc: amenințările, vulnerabilitățile și impactul asupra activelor ce trebuie protejate;
- în baza rezultatului acestei analize se identifică riscul acceptabil;
- se documentează controalele care vor fi implementate pentru a menține 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 breșelor pentru a identifica controalele care nu au fost implementate în totalitate sau pentru care utilizatorii necesită instruire;
- se implementează acțiunile corective prin care se remediază situațiile identificate anterior;
- toată documentația se pune la dispoziția unei firme sau a unui evaluator acreditate să ofere certificare în baza ISO 27001;
- auditorii firmei vor efectua o verificare formală prin care certifică existența fizică a controalelor documentate;
- dacă situația faptică este conformă cu documentația 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 activitățile implicate trebuie gestionate ca un proiect de sine stătător, după cum urmează:

1. Definierea 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 amenințărilor
 - d. Identificarea unor controale posibile/aplicabile
3. Managementul proiectului
 - a. Management propriu-zis
 - b. Aspecte tehnice și 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. Amenințări-vulnerabilități
 - d. Estimarea riscurilor

5. Reducerea/eliminarea/externalizarea riscurilor
 - a. Selectarea măsurilor de protecție
 - b. Costuri asociate
 - c. Eficiență
 - d. Soluții 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 organizații care să aibă politici de securitate identice. Din multitudinea lor, vom prezenta, în continuare, o sinteză a formelor existente, reunind ceea ce se regăsește în mai multe locuri.

De regulă, se începe cu un program de securizare a sistemelor informaționale, situație în care se folosește conceptul de *politica programului de securitate informațională*. Ea este acoperișul sub care se vor realiza politici tehnice de securitate, standarde și norme de aplicare. Într-o unitate sunt necesare politici speciale pentru utilizarea Internetului și a e-mail-ului, pentru accesarea de la distanță a sistemului, pentru modurile de utilizare a unui sistem informatic, pentru protecția informațiilor ș.a. Așadar, se poate spune că printr-o politică a programului de securitate informațională se definește politica de ansamblu a organizației în acest domeniu, precum și responsabilitățile din sistem. În aceste condiții, politicile ce se vor emite sunt componente esențiale ale programului și ele trebuie să răspundă la cinci obiective majore:

- *prevenire*: abilitatea de prevenire a accesului neautorizat la valorile patrimoniale ale organizației;
- *asigurare*: asigurarea că politicile, standardele și normele sunt în concordanță cu intențiile organizației pe linia protejării valorilor patrimoniale informaționale;
- *detectare*: abilitatea de a detecta intrușii din sistem și de a lansa arsenalul de contramăsuri corespunzătoare;
- *investigare*: capacitatea de a folosi tehnici adecvate pentru obținerea informațiilor despre posibii intruși din sistem;
- *continuitate*: posibilitatea de a garanta funcționarea neîntreruptă prin existența unui plan de acțiune în cazul dezastrelor, dezvoltat și testat în organizație.

În continuare, vom face o descriere succintă a câtorva politici³.

Politica utilizării adecvate

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

- Trebuie ca utilizatorii să citească și copieze fișiere 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 Architecture: Design, Deployment & Operations*, Osborne/McGraw-Hill, New York, 2001, pp. 18-26

- Trebuie ca utilizatorii să modifice fișierele la care au drept de scriere, dar nu sunt ale lor?
- Trebuie ca utilizatorii să facă copii ale fișierelor 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 licență de utilizare?

Politica privind conturile utilizatorilor

Politica vizează normele după care se formulează cererile de deschidere a conturilor din sistem și cum se efectuează întreținerea lor. Este foarte utilă în organizațiile mari, în care utilizatorii au conturi în mai multe sisteme. Este recomandată modalitatea de citire și 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 (angajaților, soțiilor/soților, rudelor, copiilor, vizitatorilor ș.a.) îi este permis să folosească resursele informatice ale organizației?
- Poate un utilizator să aibă mai multe conturi în același sistem?
- Pot folosi utilizatorii în comun aceleași conturi?
- Care sunt drepturile și obligațiile utilizatorilor?
- Când va fi dezactivat și arhivat un cont?

Politica accesului de la distanță

Prin ea se definesc modalitățile de conectare de la distanță la rețeaua internă a organizației. Ea este necesară în organizațiile care au utilizatori și rețele dispersate geografic. Politica trebuie să răspundă următoarelor întrebări:

- Cine poate să aibă dreptul accesării de la distanță?
- Ce metode sunt acceptate de organizație (dial-up, modem)?
- Este permis accesul din afară la rețeaua internă prin modem?
- Se impun anumite condiții, cum ar fi soft antivirus și de securitate, pentru accesarea de la distanță?
- Pot alți membri ai familiei să acceseze rețeaua?
- Sunt restricții privind tipul datelor ce pot fi accesate de la distanță?

Politica protecției informațiilor

Printr-o astfel de politică se aduc la cunoștința utilizatorilor condițiile prelucrării, stocării și transmiterii informațiilor sensibile. Scopul principal al acestei politici este asigurarea că informațiile sunt protejate, în mod corespunzător, împotriva modificărilor sau dezvăluirii neautorizate. O astfel de politică trebuie semnată de toți angajații. Ea trebuie să dea răspuns cel puțin la următoarele întrebări:

- Care sunt nivelurile de sensibilitate ale informațiilor?
- Cine poate să aibă acces la informațiile sensibile?
- Cum sunt stocate și transmise informațiile sensibile?
- Ce niveluri de informații sensibile pot fi listate pe imprimante publice?
- Cum trebuie să fie șterse informațiile sensibile de pe suporturi (tocarea și arderea hârtiilor, curățirea discurilor ș.a.)?

Politica gestionării firewall-urilor

Politica gestionării firewall-urilor descrie modul în care sunt gestionate hardul și softul și cum sunt formulate și 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 configurația firewall-urilor?

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

Politica accesului special

Prin ea se definesc condițiile formulării cererilor de obținere a dreptului de utilizare a unor conturi speciale din sistem (root, Administrator ș.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 situațiile ce vor conduce la revocarea privilegiului de a avea acces special?

Politica de conectare la o rețea locală

Prin ea se definesc condițiile adăugării de noi echipamente la rețea și trebuie să răspundă la întrebările:

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

Politica partenerului de afaceri

O astfel de politică stabilește ce măsuri de securitate trebuie să respecte fiecare companie parteneră. Ea este o politică cu atât mai necesară acum când organizațiile oferă rețeaua lor internă partenerilor, clienților, furnizorilor. Deși o astfel de politică este diferită de la o organizație la alta, ea, totuși, trebuie să ofere răspunsuri la următoarele întrebări:

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

Politica managementului parolelor

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

- lungimea minimă a unei parole trebuie să fie de cel puțin opt caractere;
- parola nu trebuie să fie un cuvânt din dicționar;
- ea trebuie să fie o combinație de litere și simboluri speciale;
- parola trebuie să expire după o anumită perioadă de timp predeterminată;
- parolele administratorilor de rețele trebuie să expire mult mai repede și trebuie să fie mai lungi;
- parolele din organizație trebuie să difere de cele folosite în alte sisteme;
- trebuie să fie păstrată o listă cu vechile parole pentru a preveni reutilizarea (ultimele șase parole nu trebuie să se repete);
- parolele utilizatorilor noi trebuie să fie unice și 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 rețele a organizației trebuie să folosească serviciul public Internet. Politica va descrie softul folosit

pentru filtrare și blocare, cu scopul protejării organizației, dar și activitățile specifice permise, precum și cine sunt beneficiarii acestor drepturi de acces și cui i se interzic. Ea este bine să se refere și la metodele de autentificare înaintea accesării Internetului în afara organizației/țării pentru a preveni personalul că folosește rețeaua organizației în scopuri ilegale.

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

- *Poșta electronică.* Aceasta vizează toate formele de e-mail utilizate de o organizație, definindu-se ceea ce se acceptă a se folosi, declarându-se softul utilizat pentru filtrare și scanare. Ea trebuie să sublinieze cerințele specifice referitoare la datele ce nu pot fi transmise prin e-mail și procedurile de urmat în cazul în care un utilizator primește mesaje cu date de acest gen. Prin această politică trebuie prevăzute și măsurile luate în cazul nerespectării condițiilor de utilizare a e-mail-ului;
- *Web.* Politica va prevedea condițiile specifice de realizare a traficului Web. Cât timp WWW (World Wide Web) folosește HTTP-ul (HyperText Transport Protocol) pentru transferarea informațiilor, prin politica de față vor fi definite clar tipurile de site-uri Web care sunt strict interzise, de genul celor porno, jocurilor de noroc ș.a.;
- *FTP.* Permițând utilizatorilor accesul la FTP (File Transfer Protocol), se deschide calea descărcării cu ușurință în sistemul organizației a virușilor, dar și transmiterea pe serverele din afara organizației a unor informații confidențiale. Pentru specialiștii organizației trebuie să se asigure un nivel de acces FTP pentru efectuarea unor descărcări de fișiere în vederea actualizării softului existent, dar politica de față trebuie să stabilească autorizările de utilizare FTP;
- *Chat/IRC.* IRC-ul (Internet Relay Chat) este mai puțin folosit în mediul organizațional față de alte programe de chat (dialoguri Internet), cum sunt Yahoo, ICQ și AOL Instant Messenger (AIM). Astfel de programe sunt foarte riscante pentru organizație deoarece informațiile sunt transmise unor servere externe fără o protecție corespunzătoare. Politica de față trebuie să stabilească în ce măsură produsele de tip *chat* servesc intereselor organizației.

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

- acceptarea folosirii și condițiile de accept pentru:
 - descărcările de fișiere;
 - newsgroup-uri;
 - comunicarea datelor sensibile;
 - tipurile de fișiere atașate;
 - dimensiunea mesajelor;
 - softul fără licență;
 - pachete de aplicații soft neaprobat;
 - exportul informațiilor sensibile;
 - protecția fișierelor;
 - protecția împotriva virușilor;
- managementul schimbărilor din sistem;
- practicile de stocare a datelor;
- siguranță și disponibilitate;
- protecția informațiilor prin clasificarea lor;
- controlul accesului;
- e-mail-ul și datele ce pot fi reținute/stocate în unitate;
- monitorizarea;
- excepțiile și amendamentele politicii Internet.

După prezentarea exemplurilor de mai sus, dar și din studierea politicilor unor organizații pe linia securității informaționale, 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

- Întocmiți, pentru o organizație cunoscută de dvs., un set cât mai complet de recomandări ale politicilor de securitate aplicabile în cadrul acesteia.
- Comentați următorul citat:
 Multe dintre organizațiile pe care le cunosc sunt fortărețe impresionante. Limbajul pe care-l folosesc e unul puternic defensiv și apare oriunde e vorba de practicile CYA[1], de secrete păzite cu strictețe și de fișierele personale încuiate în seifuri, de activități referite drept „campanii”, „războaie”, „hărțuiri”, ca și în sintagmele împrumutate din sport, care descriu orice lucru în termeni de apărare sau atac. Multe organizații simt că trebuie să se apere chiar de proprii angajați cu reguli, ghiduri, cititoare de cartele pentru pontaj, politici și proceduri în care apar specificate, exhaustiv, toate situațiile comportamentale posibile. Una dintre organizațiile în care am lucrat își întâmpină noii angajați cu o listă de 27 de abateri pentru care pot fi concediați imediat și fără drept de apel – în plus, îi asigură și că pot fi dați afară la fel de ușor și pentru alte delictе, nespecificate. Multe firme au ierarhii rigide, care împiedică oamenii să vorbească nestingheriți 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 organizaționale să se recombine, reconfigureze, discute sincer unele cu altele. Suntem profund speriați 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 științific prin *modelele de politici de securitate*, grupate în *modele de securitate multinivel* și 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 și modelul rețea, modelul zidului chinezesc, modelul BMA (British Medical Association).

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

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

Standardele sunt obligatorii și sunt implementate la nivel de unitate, pentru asigurarea uniformității. *Normele* sunt oarecum asemănătoare standardelor, referindu-se la metodologiile sistemelor securizate, numai că ele sunt acțiuni recomandate, nu obligatorii. *Procedurile* prezintă pașii detaliați ce trebuie să fie parcurși pentru execuția unei activități.

CAPITOLUL V

Criptografia

Scopul criptografierii este de a proteja informațiile transmise fără să poată fi citite și înțelese decât de către persoanele cărora le sunt adresate. Obiectivele capitolului de față sunt:

- cunoașterea principalelor tehnologii criptografice;
- dobândirea de cunoștințe generale privind sistemele de criptare prin chei secrete (simetrice) și prin chei publice (asimetrice).

5.1 Concepte de bază

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

Cheia sau *variabila de criptare* este o informație sau o secvență prin care se controlează cifrarea și descifrarea mesajului.

Cifrarea este o transformare criptografică a unor caractere sau biți.

Criptograma sau *textul cifrat* reprezintă un mesaj neinteligibil.

Cifrul bloc se obține prin separarea textului inițial în blocuri de câte n caractere sau biți și aplicarea unui algoritm și a unei chei identice, k , pentru fiecare bloc. De exemplu, dacă textul unui mesaj inițial, M , este împărțit în blocurile M_1, M_2, \dots, M_p , atunci:

$$C(M,k) = C(M_1,k) C(M_2,k) \dots C(M_p,k)$$

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

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

Criptanaliza este actul obținerii textului clar sau a cheii din textul cifrat, care este folosit pentru obținerea informațiilor 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). Informațiile criptate sunt transmise din punctul de origine la destinația finală. În varianta criptării prin chei simetrice, atât expeditorul, cât și destinatarul folosesc aceeași cheie de criptare. Cheile asimetrice conduc la utilizarea unor valori diferite la cele două capete, expeditor și destinatar sau emițător și receptor.

Criptarea înlanțuită. Fiecare entitate are chei comune cu cele două noduri vecine din lanțul de transmisie. Astfel, un nod primește 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 destinația finală.

Criptografia este arta și știința ascunderii semnificației unei comunicări împotriva unor interceptări neautorizate. Cuvântul are rădăcini grecești, însemnând scriere ascunsă – *kryptos graphein*.

Criptologia reunește criptografia și criptanaliza.

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

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

Steganografia este o formă de comunicare secretă prin care se încearcă ascunderea mesajului secret. Prin ea, într-o imagine digitală, cel mai puțin 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 numește *steganografie*. Oricine știe că mediul respectiv conține un mesaj secret poate să-l identifice, presupunând că știe 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 semnificația 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 fâșii de papirus sau pergament înfășurată în jurul unui băț. Mesajul de codificat se scria de-a lungul bățului (de sus în jos sau invers) pe fâșia înfășurată care, după desfășurare, se transmitea la destinatar, ceea ce însemna o panglică plină de caractere aleatoare, firesc, fără noimă. Când ea ajungea la destinație și se înfășura pe un băț de același diametru, se afla mesajul inițial.

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

Substituția unei litere în alta, aflată la dreapta peste trei poziții, a făcut ca metoda să mai fie numită și metoda de substituție C3. Fiind invenția lui Cezar, metoda este alteori întâlnită și sub numele *inelul lui Cezar*.

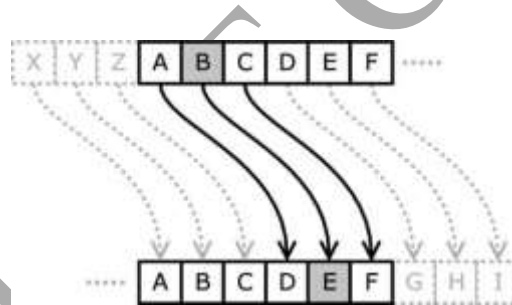


Fig. 5.1 Cifrul substituției C3 al lui Cezar

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 substituție monoalfabetică, iar C_i sunt caracterele textului clar. Iată un exemplu:

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

folosindu-se cifrul C3, conform substituțiilor 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 circumferința lui, iar prin rotirea unui disc față 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 și lingviști, 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.

Invențiile s-au înmulțit 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 „mașina japoneză de purpură” și mașina germană „Enigma”, ca fiind cele mai performante, dar și ele au fost sparte, la figurat.



Informați-vă în detaliu asupra unui moment din istoria criptografiei care v-a reținut atenția.

5.3 Tehnologii criptografice

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

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

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

5.3.1 Substituția

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

printre primii comandanți ai imperiilor care și-a inițiat generalii în taina transmiterii mesajelor criptate. Cifrul lui Cezar este o submulțime a cifrului polialfabetic al lui Vigenère. În cifrul lui Cezar, caracterele mesajului și numărul de repetiții 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 – Corespondența 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 înțelege modul de funcționare, să presupunem că $D = 3$ și $K = DAC$, 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 corespondențe, 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, așa cum reiese de mai sus: VTTLCV VEEUEV.

În cazul cifrului lui Cezar, D este 1 și cheia este $D(3)$. Luând exemplul anterior, cu mesajul STRICT SECRET, convertit în valorile numerice aferente pozițiilor 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 poziții. Atunci când sumele valorilor cheii și ale numărului aferent literelor sunt mai mari sau egale cu 26, se determină modulo 26 din sumă, adică rezultatul final este obținut 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, așa cum am menționat, 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 ecuația 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 monosubstituția folosită de Cezar, în care orice literă este înlocuită prin alta situată mai în dreapta cu n poziții (variante Cezar, $n = 3$, $A = D$, $B = E$, $C = F$ ș.a.m.d). O astfel de criptare este ușor atacabilă prin analiza frecvențelor de apariție a caracterelor. În fiecare limbă se știe care sunt frecvențele literelor din textele scrise. În limba engleză, frecvențele apariției literelor sunt prezentate în tabelul 5.2. Cifrul lui Cezar, bazându-se pe substituția simplă sau monoalfabetică, este ușor de „spart” pentru că un caracter este înlocuit de altul și această schimbare este valabilă în tot textul, iar analiza frecvențelor ne va conduce la caracterele adevărate ale textului clar.

Tabel nr. 5.2 – Frecvența apariției 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 substituția multiplă. De exemplu, dacă se folosesc patru alfabete pentru substituție, definite de cel ce intenționează să creeze, prima literă din textul clar este înlocuită cu prima literă din primul alfabet, a doua 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 ș.a.m.d. Exploatând această metodă, Balise de Vigenère, diplomat francez născut în 1523, a dus mai departe realizările lui Alberti Trithemius și 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.

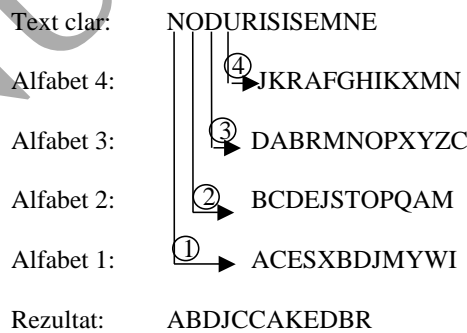


Fig. 5.3 Exemplu de cifru polialfabetic

5.3.2 Transpoziția (permutarea)

Pentru a înțelege transpoziția sunt necesare câteva informații acumulate anterior, cum ar fi: introducerea în sistemele criptate, permutări și matrice. Transpoziția se bazează pe o idee foarte simplă. În loc să înlocuiești un caracter cu altul, e mult mai simplu să înlocuiești ordinea caracterelor. În plus, acest cifru nu va fi ușor descoperit prin analiza frecvenței apariției unor caractere. De asemenea, cheia pentru un astfel de cifru nu este standard. În locul unei liste a

substituțiilor 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 transpoziție 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 ș.a.m.d. De exemplu, cuvântul SCOALA devine CLAOAS.

Permutările unui astfel de cifru acționează într-o matrice bloc, ceea ce înseamnă că va fi o matrice de tip „patul lui Procust”, în care tot ceea ce nu încapă într-o linie se va alinia în cea următoare ș.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:

PROTECTIE SI TEAMA.

Dacă se va lucra la coloane, prin folosirea transpoziției 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.

Aceleași reguli se pot aplica asupra coloanelor sau, și mai interesant, asupra liniilor și coloanelor.

Combinarea transpoziției cu substituția 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 folosește o singură dată pentru un singur mesaj și nu va mai putea fi folosită niciodată. Lungimea șirului 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:	CRIP TARE DATE	2	17	8	15	19	0	17	4	3	0	19	4
Cheie Vernam:	XYZABC PQRJDW	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 și 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 transmitător și potențialul receptor, poate fi formată din pagina cărții și numărul rândului de pe pagina în care se află textul.

5.3.5 Codurile

Codurile sunt utilizate pentru a putea transmite unele construcții predefinite din domenii diverse, de regulă din afaceri, prin intermediul lor. De exemplu, codul 500 ar putea să însemne „De efectuat recepția cantitativă și calitativă a mărfurilor expediate”. Odată cu generalizarea serviciilor telegrafice, pentru diminuarea prețului pe mesaj, s-a apelat la un astfel de sistem. De regulă, sunt două rânduri de cărți: una conține ordinea crescătoare a codurilor și, în dreptul lor, semnificația în clar; alta conține semnificația în clar, în ordine alfabetică și codul corespunzător.

5.3.6 Ascunderea informațiilor

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

În vechea Chină se folosea o altă tehnică a ascunderii informațiilor. „Cheia” consta într-o matriță de hârtie, în două exemplare – unul pentru emițător, celălalt pentru receptor, cu perforații ce se urmăreau într-o anumită ordine, firesc ele fiind plasate într-o totală dezordine. Emițătorul pune matrița pe o coală de hârtie și scria mesajul în ordinea știută a perforațiilor, după care, renunțându-se la matriță, 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 și din această cauză este cunoscută în criptografie sub numele *grila lui Cardan*.

Doar pentru frumusețea textului scris de profesorul Dumitru Năstase¹, vă prezentăm constatarea sa:

„Modul „inițiativ” de a comunica mesajele lor cele mai profunde, utilizat de scrierile și actele noastre medievale, trebuie confruntat cu un alt cod, despre caracterul simbolic al căruia nu se îndoiește nimeni, și anume cel heraldic. Cu condiția, însă, de a ști că și simbolurile heraldice ale Țărilor Române conțin 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 desăvârșire specialiștilor.

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

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

Iată, așadar, o sublimă tehnică de ascundere a informației prezentă de secole în heraldica românească prin apariții deosebit de interesante pe o mare varietate de obiecte sau în iconografia vremurilor. Aceasta este o probă vădită de steganografie, care înseamnă ascunderea informației în fața ochiului nevizat.

În vremurile noastre, ascunderea informației 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 românești, Extras din Anuarul Institutului „A. D. Xenopol”, XXX, 1993, Ed. Academiei Române, Iași, p. 489.

mecanism de protejare a copyright-ului, interes regăsit și în domeniul militar pentru comunicații care să nu dea nimic de bănuț interceptorilor neautorizați. Și populația era îngrijorată de agresivitatea discuțiilor guvernamentale în legătură cu nevoia de a controla comunicațiile criptate. Toate acestea au condus la o puternică dezvoltare a *ascunderii informației*.

Ascunderea modernă a informației viza ascunderea unor mesaje secrete într-un fișier audio MP3 sau seria unui program era încapsulată printre instrucțiunile executabile.

Interesele Hollywoodului vizau marca de înregistrare a copyright-ului, care să fie ascunsă percepției obișnuite din bucățile audio digitale, video și ale lucrărilor de artă. Ele sunt fie *filigrane (watermarks)*, care reprezintă mesajul copyright-ului ascuns, fie *amprente (fingerprints)*, care semnifică seriile ascunse.

5.3.6.1 Steganografia

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

Prin steganografie se exprimă interesul pentru confidențialitate, întrucât scopul ei este de a include mesaje într-un anumit mediu astfel încât să rămână insesizabil. Un model conceptual cunoscut, propus de Simmons², este următorul. Alice și Bob sunt în pușcărie și 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 și mai dură. Așadar, ei trebuie să găsească o modalitate de a ascunde mesajele secrete într-un inocent text care să le acopere. Așa cum se procedează în criptografie, presupunem că mecanismul folosit este cunoscut de gardian, așa că din motive de securitate, ei trebuie să apeleze la o cheie secretă comună pe care doar ei să o știe și să o folosească.

David Kahn, autorul cărții *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 bănuț. Doar primitorul mesei va ști 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 și micropunctele. *Micropunctele* sunt fotografiile 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 ș.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 biții imaginilor digitale*. Imaginile sunt reprezentate printr-o formă matriceală de *pixels (picture x elements)*, însemnând puncte din care se realizează imaginea. O imagine foto-CD Kodak are 3072 x 2048 pixeli, dar o imagine mai puțin clară poate să aibă 400 x 300 pixeli. Fiecare pixel este codificat printr-o secvență de biți care fixează culoarea. În cea mai simplă formă, codificarea se realizează prin 24 de biți, care, conform sistemului RGB – Red (roșu), Blue (albastru), Green (verde) –, înseamnă atribuirea a câte 8 biți pentru fiecare culoare. Cei 8 biți, care formează un octet, determină realizarea a 256 de posibilități; prin combinarea lor rezultă aproximativ 17 milioane de nuanțe de culori. Printr-o astfel de variantă se pot obține performanțe foarte mari, dar, unor biți li se poate da o altă destinație, pentru a se codifica mesaje scurte, fără să afecteze semnificativ imaginea.

În structura octeților, valoarea biților 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 influență 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!?!

Biții succesivi ai mesajului secret pot fi plasați pe poziția biților cel mai puțin semnificativi ai octeților următori, fără să altereze semnificativ imaginea. Putem face un calcul simplu al potențialilor biți utilizabili pentru ascunderea mesajului, știut fiind faptul că sunt 400×300 pixeli, fiecare cu câte 3 octeți (de la care se pot valorifica 3 biți, câte unul de la fiecare octet), rezultând $400 \times 300 \times 3 = 360.000$ biți. Alocând câte 8 biți 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 octeți (24 biți) ai imaginii au următoarea structură:

0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	0	1	1	1	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 biții cei mai nesemnificativi, a opta poziție, marcați cu bold. În codul ASCII:

A este 01000001

B este 01000010

C este 01000011

Deci, mesajul ABC înseamnă șirul

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 biți disponibili în exemplul dat, doar 3, înseamnă că vom putea plasa numai primii trei biți ai literei A, adică 010, astfel:

0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	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 biți din cei trei mai puțin semnificativi s-au schimbat, respectiv ultimul bit al celui de-al doilea octet și al celui de-al treilea. Pentru decodificarea mesajului, se vor extrage doar biții aflați pe a opta poziție a fiecărui octet, ceea ce cu calculatorul este o procedură foarte simplă. Printr-o astfel de operațiune biții inițiali ai imaginii nu mai pot fi reconstituiți.

Pentru cei ce doresc să se obișnuiască cu mediul de lucru al steganografiei, recomandăm vizitarea site-ului <http://members.tripod.com/steganography/stego/s-tools4.html>. De aici, intrați pe *Software* și veți putea găsi o mare varietate de programe din acest domeniu, prin care puteți afla ce imagini conțin mesaje ascunse sau, dacă doriți, vă ascundeți 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 cosmonauții 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.

Totuși, steganografia nu este la fel de sigură cum este criptarea prin chei, dar ea a fost (și este) folosită în multe acte criminale. Ea poate servi și la ascunderea existenței unui fișier pe hard disk pentru toți cei ce nu-i știu numele și parola.

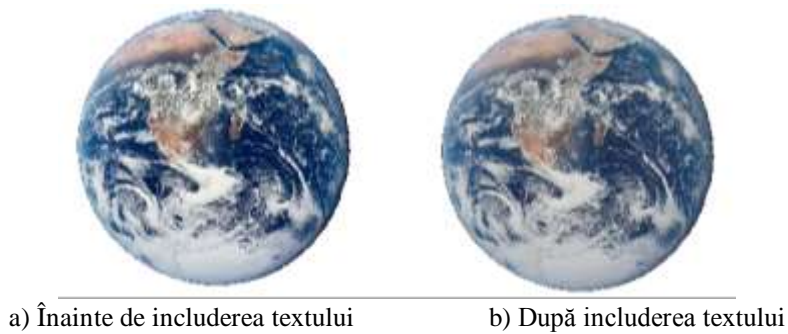


Fig. 5.4 Imaginea pământului de pe Apolo 17, diferite din punct de vedere al conținutului



- Identificați pe Internet programe care folosesc tehnica LSB pentru transmiterea mesajelor ascunse.
- Credeți că există situații în activitatea organizațiilor economice în care să fie utilă folosirea steganografiei? Exemplificați, justificați.

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, ținerea evidenței copiilor datelor, verificarea integrității datelor. Filigranele folosite în bancnote au scopul de a întări încrederea posesorilor că se află în fața banilor originali și nu a unora contrafăcuți, 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 și extragere a lui pentru a se verifica autenticitatea datelor sau a se afla sursa lor.

Datele filigranate sunt o funcție a unui identificator și/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 ținerea evidenței fiecărei chei folosite pentru fiecare beneficiar este ușor de urmărit cine a încălcat dreptul de proprietate.

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

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

În spațiul cibernetic, filigranele sunt folosite pentru stabilirea încălcărilor dreptului de autor. *Digimarc Technologies* (www.digimarc.com și www.digimarc-id.com) are un produs pentru protejarea imaginilor puse de proprietar în propriul său site. Deținătorii copyright-ului inserează filigranul lor, folosind *PhotoShop* al *Adobe*-ului, sau un alt editor de imagine care încorporează tehnologia *Digimarc*. Când receptorul folosește același editor pentru vizualizarea imaginilor va fi afișat simbolul de copyright al autorului. Prin selectarea simbolului se realizează legătura cu *Digimarc*, de unde vor afla cine este deținătorul 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 piraților de muzică. Softul lor, *MusiCode*, încapsulează informații-sursă (cum sunt titlul, artistul, compania de înregistrare) în fișierul audio. Softul este folosit pe Internet printr-un motor de căutare care combate pirații de melodii din acest mediu.

Realizări sunt foarte diverse, dar scopul prezentării de față este doar acela de a informa pe cei interesați de protejarea creației lor că au la dispoziție instrumente de apărare.



Identificați pe Internet programe cu ajutorul cărora să introduceți filigrane în imaginile digitale.

5.3.6.3 Securitatea tipăririi hârtiilor de valoare

Abordarea acestui subiect în cărțile de protecție și securitate este aproape inexistentă. Singurele materiale deosebit de interesante poartă semnătura lui Renesse³, deși există o mulțime de tratări parțiale ale subiectelor menționate. Probabil că acesta a fost și raționamentul lui Ross Anderson⁴ de a face o sinteză a acestor concepte într-un capitol distinct.

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

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

Mulți producători de calculatoare vor să ofere un plus de siguranță cumpărătorilor apelând la tipărirea securizată, tehnici de ambalare și sigilii. Hologramele, filigranele și 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 protecție împotriva pirateriei, realizând etichetele cu hologramă care trebuie să nu se dezlipească ușor, ci, dimpotrivă să se rupă la desigilare.

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

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

Dacă se urmărește istoria unui element de securizare se va observa cum lupta dintre cei ce l-au conceput și pirateria de pe piață a condus la o continuă evoluție 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 și autentificare, dar ea a condus la numeroase contrafaceri, ceea ce a determinat apariția imprimantelor color și a gravărilor metalice. Dar nici pozele color n-au putut să ofere liniște decât pentru o scurtă perioadă de timp, situație în care s-au inventat alte tehnici optice, cum ar fi echipamentele pentru realizarea hologramelor. Apărătorii și atacatorii țin pasul cu ultimele realizări din domeniu. Că reușesc și unii și alții sunt o mulțime 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 lățime, care parecă era cusut, fiecare bucățiță vizibilă cu

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

Renesse, R. – „Verifying versus Falsifying Banknotes”, in *Optical Security and Counterfeit Deterrence Techniques 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 așa-ceva poate fi contrafăcut? Și, totuși, niște „specialiști” 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 bucățele 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 organizații finanțate de guverne pentru contrafacerea bancnotelor altor țări, întreprinderi mici și 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. Baniile falși nu pot înșela un specialist din bănci, dar ei tocmai din această cauză se plasează în locuri cu oameni naivi sau în localuri mai întunecate și 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 puțină experiență în actele de vânzare-cumpărare;
- *nivelul secundar al verificării* se exercită de personal competent și motivat, cum este cazul experimenților operatori de la ghișeele băncilor sau inspectorii calificați ai produselor industriale marcate cu etichete și/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 și nici prea costisitoare, iar falsificatorii le știu 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 și nu pot da rateuri. O astfel de verificare depășește absolut toate contrafacerea, numai că ea se exercită asupra cazurilor cu totul speciale.

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

- *intaglio* sau *gravura cu acizi* se folosește pentru fixarea cu mare forță a cernelii pe hârtie, lăsând în urmă o imprimare în relief cu o mare rezoluție. Este tehnica folosită cel mai mult la tipărirea banilor sau realizarea pașapoartelor;
- *literă presată*, prin care cerneala este depusă prin rularea caracterelor în relief și presarea hârtiei pe care se face tipărirea, astfel încât să rămână și urmele presării. Tehnica este folosită pentru tipărirea numerelor ce indică valoarea bancnotelor. Mărimea lor și culoarea sunt atipice, ca elemente suplimentare de securitate, eliminând posibilitatea realizării lor cu materiale sau mijloace existente pe piață;
- *procesarea simultană* constă în transferarea completă a cernelii simultan pe ambele fețe ale bancnotei, ceea ce va conduce la o tipărire cu suprapunere perfectă. Se spune că reproducerea lor cu imprimantele color din comerț este aproape imposibilă. În plus, prin duze speciale, cerneala color este dispusă variat de-a lungul unei linii;
- *ștampilele de cauciuc* sunt folosite pentru andosarea documentelor sau pentru ștampilarea fotografiilor de pe documente;
- *gofrarea și laminarea*. Gofrarea sau scrierea în relief și laminarea sunt folosite pentru fixarea fotografiilor și marcarea caracterelor pe carduri pentru a scumpi costurile contrafacerea. 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 și fire fluorescente. Un exemplu aparte îl constituie Australia (țară în care au fost tipărite și unele bancnote românești), unde însemnele de 10 dolari sunt tipărite pe suport de plastic cu zone transparente.

Dintre *tehnicele mai moderne*, amintim:

- *cernelurile schimbătoare optic*, tehnică folosită pentru unele porțiuni ale bancnotelor canadiene de 20 dolari, care își schimbă culoarea de la verde la galben, în funcție de unghiul din care este privit obiectul. La noi, tehnica este cunoscută și sub numele de gât de rățoi sau gușă de porumbel;
- *cerneala cu proprietăți magnetice sau fotoacustice*;
- *imprimarea unor semne vizibile cu echipamente speciale*, așa cum este microtipărirea de pe bancnotele americane, care necesită o sticlă magnetizabilă pentru a urmări semnele, precum și tipărirea în cerneluri ultraviolete, infraroșii 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, așa cum sunt *hologramele* sau *kinegramele*, precum cele de pe bancnotele de 20 și 50 de lire sterline. Hologramele se produc, de regulă, optic și reprezintă obiecte întregi pe un plan îndepărtat, iar kinegramele sunt realizate cu calculatorul și oferă imagini diferite în funcție de unghiul din care sunt văzute;
- *marca digitală a copyright-ului* variază ca formă de prezentare și este recunoscută de copiatoare, scannere și 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 și 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 țină cont și de aspecte estetice, de rezistență la întrebuințare ș.a. Din experiențele acumulate de-a lungul timpului, s-au desprins următoarele lecții:

- 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-și găsească locul potrivit, să facă parte firească din ansamblul documentului, astfel încât și fixarea în mintea utilizatorului să fie naturală;
- efectul lor trebuie să fie evident, distinct și inteligibil;
- nu trebuie să intre în concurență 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 modalități de securizare care nu sunt mediatizate. Câteva dintre ele sunt aduse la cunoștința inspectorilor de specialitate. Cu timpul, acestea sunt aflate și 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 piață și se înlocuiesc cu alt model. Cercetările din domeniu anunță o posibilă apariție a unui sistem unic de marcă, constând într-un strat chimic special, conținând proteine sau chiar molecule DNA, prin care se vor codifica serii ascunse, citibile de către orice tip de mașină de verificare a lor.



Identificați în activitatea organizațiilor 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 și numele din paranteză, apelează la o singură cheie la ambele capete ale comunicării: emițătorul și receptorul. Emițătorul sau expeditorul criptează textul clar cu ajutorul unei chei secrete, iar receptorul sau destinatarul va decripta mesajul criptat folosind aceeași cheie, firească, reușita este asigurată de secretizarea cheii. Succesul cheilor simetrice este și 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 informație publică și privată. *Informația publică*, de regulă, constă în:

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

Informațiile private sunt:

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

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

Singura problemă a sistemului constă în folosirea în comun a cheii de criptare de către emițător și receptor, ceea ce înseamnă că emițătorul 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 știe că sistemele bazate pe chei simetrice nu oferă mecanismele necesare autentificării și 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 informații 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 Național pentru Standarde și 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 înlănțuite (*Cipher Block Chaining – CBC*);
- criptarea - carte electronică de coduri (*Electronic Code Block – ECB*);
- criptarea cu feedback la ieșire (*Output Feedback – OFB*).

Datorită vulnerabilității DES, din noiembrie 1998, guvernul SUA nu-l mai folosește, 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 specificația FIPS 46-3.

Inițiativa 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 competiție. Până în august 1998, NIST a anunțat 15 candidaturi, iar în 1999 au fost selectați 5 finaliști: MARS, RCG, Rijndael, Serpent și Twofish. Runda a doua de analiză publică a algoritmilor a fost închisă în 15 mai 2000. La data de 2 octombrie 2000, NIST a anunțat selecția *Rijndael Block Cipher*, având ca autori doi cercetători belgieni, Dr. Joan Daemen și Dr. Vincent Rijmen. Acesta va fi algoritmul AES propus, devenind un nou standard FIPS, utilizat de guvernul SUA să protejeze informații sensibile, dar neclasificate. Se speră că el va fi adoptat și de alte organizații publice sau private, atât din SUA, cât și de pe alte continente.

Algoritmul Rijndael a fost conceput să îndeplinească următoarele proprietăți:

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

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

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

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, același calculator va avea nevoie de 149×10^{12} ani pentru a sparge algoritmul Rijndael. Să nu uităm că universul este creat de ... doar 13×10^9 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 și folosește o cheie de 128 biți ce se aplică blocurilor de text clar de câte 64 de biți. El a fost realizat în 1992 de James Massey și Xuejia Lai, preluând algoritmi anteriori numiți *Proposed Encryption Standard (PES)* și *Improved Proposed Encryption Standard (IPES)*.

Prin lungimea cheii, de 128 biți, 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 emițător și receptor, sistemele bazate pe chei publice folosesc două chei: una publică și alta privată.

Cheia publică este pusă la dispoziția oricărei persoane care dorește să transmită un mesaj criptat.

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

Pentru înțelegerea 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 și cu P un text clar (P este notația consacrată pentru *plain text*), iar K_p este cheia publică și K_s cheia privată (secretă), procesul este ilustrat astfel: $C = K_p(P)$ și $P = K_s(C)$. Și invers este adevărat: $C = K_s(P)$ și $P = K_p(C)$.

Criptografia prin chei publice este posibilă în aplicațiile care funcționează într-un singur sens. O funcție în sens unic este aceea care este ușor de calculat într-o direcție, dar este dificil de calculat în sens invers. Pentru o astfel de funcție, dacă $y = f(x)$, este simplu de determinat valoarea lui y dacă se cunoaște x , dar este foarte dificil să-l determini pe x cunoscându-l pe y . Într-o astfel de situație se află căutările telefonice. Este ușor să găsești numărul cuiva dacă știi numele și adresa, dar este foarte dificil să găsești pe cineva într-o carte de telefon cunoscându-i doar numărul de telefon. Pentru ca funcțiile 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 ușurință a funcției inverse funcției în sens unic. Printr-o astfel de modalitate se poate obține 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 știe trapa.

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

Din cauza calculului numeroase solicitate de criptarea prin chei publice, aceasta este de la 1.000 la 10.000 de ori mai încheată 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 algoritmi importanți ai cheilor publice, amintim Diffie-Hellman, RSA, El Gamal Knapsak și curba eliptică, foarte utilizați fiind primii doi algoritmi.

5.5.1 Schimbul de chei Diffie-Hellman

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

Independent, Ralph Merkle a venit cu o soluție de distribuție a cheilor publice, numai că metoda propusă implica substanțiale cheltuieli pentru efectuarea calculului și a transmisiei. Varianta realizată de Diffie și Hellman a fost numită *sistemul distribuției 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 funcție matematică a cheilor private respective. Urmează schimbul de chei publice. În final, fiecare dintre cele două persoane calculează o funcție a propriei chei private și a cheii publice a celeilalte persoane. Matematica este cea care va face să se ajungă la aceeași valoare, care este derivată din cheile lor private. Ele vor folosi valoarea ca pe cheie a mesajului.

Diffie și Hellman folosesc exponențierea în aritmetica modulară pentru a calcula cheile publice și cheia mesajului. Aritmetica modulară este ca și aritmetica standard, cu excepția faptului că folosește numere numai în intervalul 0 la N , numit modulo. Atunci când o operație 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 și cum s-ar împărți la N și se ia în seamă

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

În aritmetica modulară, exponențierea este o funcție într-un singur sens. Aceasta înseamnă că este ușor de calculat un număr $y = g^x \bmod N$ 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 și N sunt cunoscute). Aceasta este referită ca și problema logaritmului discret pentru că x este logaritm din y în baza $g \pmod{N}$, iar numerele sunt finite și întregi.

Cu metoda Diffie-Hellman a schimbului de chei publice, Alice și Bob stabilesc cheia mesajului secret după cum urmează. Alice generează o cheie secretă x_a și Bob o cheie secretă x_b . După aceasta, Alice calculează o cheie publică y_a , care este g ridicat la puterea x_a 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 y_b , prin ridicarea lui g la puterea x_b modulo p . Ei vor schimba valorile publice ale acestora. Apoi, Alice ridică cheia publică a lui Bob la puterea exponentului său, x_a modulo p , în timp ce Bob ridică cheia publică a lui Alice la exponentul său, x_b modulo p . Amândoi vor obține același rezultat, g ridicat la puterea x_a și x_b , iar rezultatul obținut va fi folosit de amândoi drept cheia K a mesajului. Matematic, totul se va exprima astfel:

$$\begin{aligned} y_a &= g^{x_a} \bmod p \\ y_b &= g^{x_b} \bmod p \\ K &= y_a^{x_b} \bmod p = y_b^{x_a} \bmod p = g^{x_a \cdot x_b} \bmod p \end{aligned}$$

Deși în practică se folosesc numere foarte lungi, de câteva sute de cifre, pentru a ajuta la înțelegerea modului de funcționare, vom folosi numere mici.

Exemplul 1

Să presupunem că $p = 7$, $g = 3$, cheia lui Alice $x_a = 1$ și a lui Bob $x_b = 2$

Vom avea:

- Alice calculează cheia sa publică: $y_a = g^{x_a} \bmod p = 3^1 \bmod 7 = 3$
- Bob calculează cheia sa publică: $y_b = g^{x_b} \bmod p = 3^2 \bmod 7 = 2$
- Alice calculează $K = y_b^{x_a} \bmod p = 2^1 \bmod 7 = 2$
- Bob calculează $K = y_a^{x_b} \bmod p = 3^2 \bmod 7 = 2$

sau

$$K = g^{x_a \cdot x_b} \bmod p = 3^{2 \cdot 1} \bmod 7 = 9 \bmod 7 = 2.$$

Exemplul 2

Să presupunem că $p = 5$, $g = 4$, cheia lui Alice $x_a = 3$ și a lui Bob $x_b = 2$

- Alice calculează cheia sa publică: $y_a = g^{x_a} \bmod p = 4^3 \bmod 5 = 4$
- Bob calculează cheia sa publică: $y_b = g^{x_b} \bmod p = 4^2 \bmod 5 = 1$
- Alice calculează $K = y_b^{x_a} \bmod p = 1^3 \bmod 5 = 1$
- Bob calculează $K = y_a^{x_b} \bmod p = 4^2 \bmod 5 = 1$

sau

$$K = g^{x_a \cdot x_b} \bmod p = 4^{3 \cdot 2} \bmod 5 = 4096 \bmod 5 = 1.$$

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

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

5.5.2 RSA

RSA provine de la numele de familie ale inventatorilor săi, Rivest, Shamir și Adleman⁵.

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 și Hellman au inventat metoda distribuției prin chei publice, aceștia au gândit și la un alt concept mult mai performant, dar n-au găsit soluția 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 și 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 și „criptografie prin două chei” și „criptografie asimetrică”. Metodele convenționale, descrise anterior, care apelează la o singură cheie, sunt referite ca și „criptografie printr-o singură cheie”, „criptografie prin cheie privată”, „criptografie prin cheie secretă”, „criptografie simetrică” și „criptografie convențională”.

La scurt timp după ce Diffie și Hellman au lansat ideea revoluționară a criptografiei prin chei publice, trei profesori de la MIT (Massachusetts Institute of Technology), Ronald Rivest, Adi Shamir și Leonard Adleman, au venit cu soluția implementării ei. Varianta propusă se numea RSA. Concomitent, Hellman și 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 și o folosește prin intermediul criptosistemului convențional, cum ar fi DES, pentru criptarea mesajului. Utilizând criptografia prin chei publice, ea, de asemenea, criptează K , sub cheia publică a lui Bob, denumită K_{Bobpub} . Apoi, ea transmite atât cheia criptată, cât și 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 folosește 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 așa, din cauza încetirii procesului de transmitere prin mulțimea calculelor de efectuat. E mult mai rapid să folosești o metodă convențională de mare viteză pentru criptarea mesajului, rezervând metoda cheii publice doar pentru distribuția cheii. În plus, nu se consideră o practică prea inspirată să folosești aceeași cheie pentru criptarea mesajelor de-a lungul unei mari perioade de timp, din cauza sporirii șanselor 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).

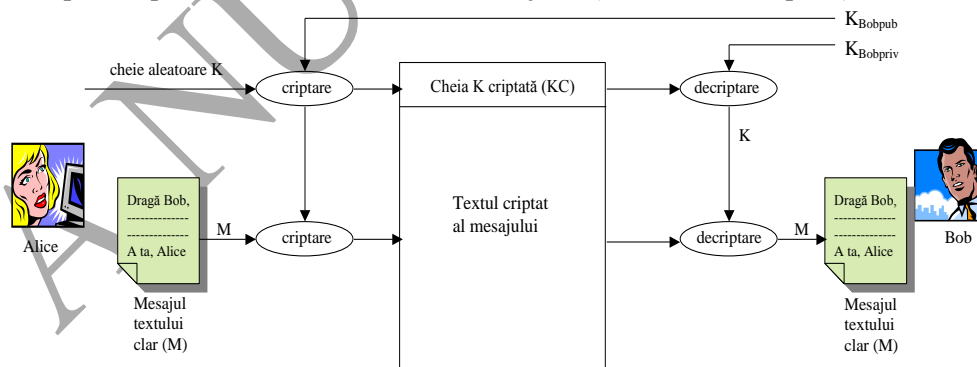


Fig. 5.5 Alice transmite un mesaj lui Bob folosind o combinație de cheie singulară și criptografie prin cheie publică (prelucrare după Denning, D. – *Op. cit.*, p. 302)

Ca și Diffie-Hellman, sistemul RSA calculează exponențierile în aritmetica modulară folosind numere cu lungimea de câteva sute de cifre. În RSA, totuși, 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:

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

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

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

În aceste condiții, oricine știe eb , pb și qb poate să folosească formula pentru a deduce db . Din acest motiv, pb și qb nu se divulgă, chiar dacă eb și 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 ușura înțelegerea mecanismului. Să presupunem că Bob a ales numerele prime secrete $pb = 5$ și $qb = 3$, de unde rezultă că $Nb = pb * qb = 5 * 3 = 15$. Apoi alege exponentul secret $db = 29$ și îl calculează pe eb după formula $eb * db = 1 \bmod (pb-1)(qb-1)$, ceea ce va conduce la $eb * 29 = 1 \bmod (4 * 2)$, $29 * eb = 1 \bmod 8$. Prin încercări succesive rezultă $eb = 5$.

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

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

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

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

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

5.5.3 Semnătura digitală

Inventarea criptografiei prin chei publice a adus două importante mutații 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 comunicație off-line pentru a transmite cheia secretă. A doua mutație 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 și digitală – exprimată printr-un șir de cifre) ce se atașează unui mesaj sau document pentru a întări încrederea unei alte persoane sau entități, legându-le de un anumit emițător. Legătura este astfel realizată încât semnătura digitală poate fi verificată de receptor sau de o terță persoană și 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 stabilește autenticitatea sursei mesajului. Dacă o persoană nu-și dă în vileag cheia personală privată nimeni nu poate să-i „imite” semnătura. O semnătură digitală nu înseamnă și recunoașterea dreptului de proprietate asupra textului transmis, ci ea atestă faptul că persoana semnatară a avut acces la el și l-a semnat. Documentul poate fi și sustras de undeva. Totuși, 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. Așa se procedează când se intenționează realizarea protecției împotriva manipulării imaginilor cu ajutorul calculatorului. La fel pot fi camerele video, radio-receptoarele și alți senzori care pot semna ieșirea pentru a-i certifica originea.

Deși 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 întrebuițată pentru semnarea mesajelor, iar cea publică este folosită de o altă parte pentru a verifica semnătura. Modul de funcționare este redat în figura 5.6.

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

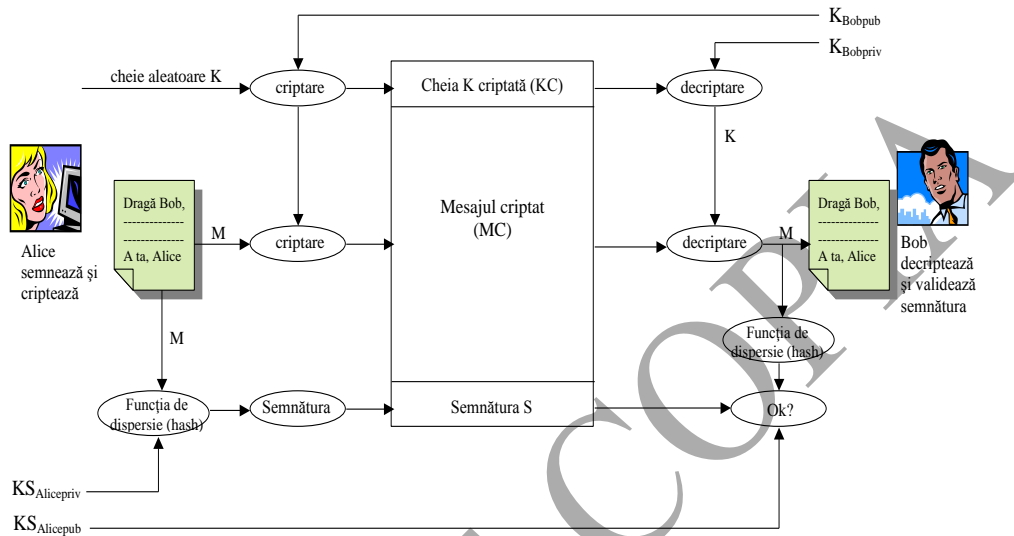


Fig. 5.6 Alice transmite către Bob un mesaj semnat și criptat. Mesajul este criptat printr-o singură cheie de criptare, iar cheia prin criptarea cu cheie publică. Mesajul este semnat cu sistemul semnăturii digitale prin cheie publică (prelucrare după Denning, D.– Op. cit., p. 332)

Să presupunem că Bob va recepționa 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 funcție criptografică prin care se va testa dacă valoarea rezumat determinată de el este aceeași 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 dorește să transmită un mesaj către Bob, mesaj care să fie semnat și criptat, procesul presupune utilizarea cheilor pentru semnătură ale lui Alice ($KS_{\text{Alicepriv}}$, KS_{Alicepub}), cheilor lui Bob de criptare a cheii ($KBobpub$) și o cheie a mesajului, K . În sinteză, iată pașii:

- Alice generează o cheie aleatoare a mesajului, K . Alice criptează mesajul M cu cheia K , obținând mesajul criptat, MC ;
- Alice criptează cheia K folosind cheia publică a lui Bob de criptare a cheii, $KBobpub$, rezultând cheia criptată, KC ;
- Alice procesează o semnătură S folosind cheia sa privată pentru semnătură, $KS_{\text{Alicepriv}}$;
- Alice transmite către Bob KC , MC și S ;
- Bob folosește cheia sa privată de criptare a cheii, $KBobpriv$, pentru a decripta KC și a obține K ;
- Bob folosește K pentru decriptarea MC și obținerea textului-clar, M ;
- Bob folosește 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, așa că Alice și Bob nu vor efectua operațiunile enunțate, 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, deși sunt mai multe oferte. Oricum e necesară obținerea 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 puteți începe dialogul pentru obținerea ID-ului digital pentru semnătură, prin click pe butonul *Get Digital ID*.

Pentru a studia cadrul legal al utilizării semnăturii electronice în România, puteți obține informațiile 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 intenția de a ajunge înapoi la (B), numai că (A), folosindu-și propria cheie privată, va face ca receptorul să fie el, reușind astfel să decripteze mesajul care era adresat lui (B).

Pentru a se evita o astfel de ciudățenie, se recurge la procesul certificării, prin care persoanele sunt legate de cheile lor publice. Documentul oferit de o *Autoritate de Certificare* acționează ca orice alt act emis de un notar și se efectuează după aceleași reguli, adică pe baza verificării identității 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 emițător dacă este necesară cheia ei publică pentru deschiderea sesiunii de transmitere a mesajelor criptate și/sau semnăturilor electronice. Certificatul conține numele subiectului, cheia lui publică, numele autorității de certificare, perioada de valabilitate a certificatului. Pentru a verifica semnătura autorității de certificare, cheia ei publică trebuie să fie verificată încrucișat 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, operațiunile pentru obținerea certificatelor digitale și validarea tranzacțiilor sunt redată în figura 5.7.



Fig. 5.7 Prezentarea unei tranzacții cu certificate digitale

5.5.5 Infrastructura cheilor publice (PKI)

Infrastructura cheilor publice (*PKI – Public Key Infrastructure*) își propune să rezolve probleme manageriale din domeniul cheilor publice, integrând semnături și certificate digitale cu o mare diversitate de alte servicii specifice comerțului electronic, prin care se solicită oferirea integrității, controlului accesului, confidențialității, autentificării și a nerepudierii tranzacțiilor electronice.

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

nerepudierea, marcarea timpului, certificarea încrucișată, aplicații 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 rețea, serverele de pe aceste rețele oferind chei publice și 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 șofer 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 unități specializate puteți obține de pe site-ul www.pki-page.org/#EU.

În SUA, majoritatea certificatelor sunt emise de Verisign, Inc., recomandată și 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) și oferă PIN-ul, după care este generat un *ID digital* și se memorează în calculatorul utilizatorului;
- *clasa 2 de certificate* cere utilizatorului să mai introducă și *Social Security Number* (codul oferit de *Internal Revenue Service*), adresa și seria carnetului de șofer;
- *clasa 3 de certificate digitale* este destinată companiilor ce publică software, oferindu-le un grad mult mai mare de securitate, dar există și o variantă pentru persoane fizice ocupate cu transferuri bancare, contracte ș.a. Este o clasă mult mai sigură.

Pentru detalii, vizitați site-ul www.verisign.com.

Oricum, realizarea unei infrastructuri a cheilor publice la nivel internațional, dar și național, este o mare problemă, nu din punct de vedere tehnic sau managerial, ci al legislației.



Dați 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 performanță 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 *forța brută* pentru a încerca toate cheile, puterea calculatoarelor necesare crește exponențial cu lungimea cheii.

O cheie de 32 de biți presupune verificarea a 2^{32} (aproximativ 10^9) pași, ceea ce se poate realiza și cu un calculator aflat la domiciliu.

Un sistem bazat pe o cheie cu 40 de biți are nevoie de 2^{40} pași, ceea ce ar însemna cam o săptămână folosind un calculator mai performant de la domiciliu.

Un sistem cu 56 de biți 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 biți sunt vulnerabile în fața multor tipuri de organizații. Cele cu 80 de biți par asigurate pentru câțiva ani, iar cele de 128 de biți sunt invulnerabile în fața atacurilor cu forță brută pentru un număr nedefinit, încă, de ani.

Totuși, 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 biți, se pare că este posibil de spart în 149×10^{12} ani, știut fiind că Universul s-a creat în urmă cu 13×10^9 ani. Nimeni nu știe însă cât de vulnerabil este un sistem în fața spărgătorilor de profesie, a criptanaliștilor. Ei se descurcă în a decripta comunicații 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.

Forța brută. Se încearcă orice combinații posibile, de regulă, secvențial, pentru aflarea algoritmului. Cu cât cheia este mai lungă, cu atât este mai dificilă aflarea ei.

Text clar cunoscut. Atacatorul cunoaște sau poate ghici textul clar pentru o parte din textul criptat. Important este să decripteze restul textului folosind aceste informații, adică să afle cheia folosită.

Text clar ales. Atacatorul este în măsură să aibă orice text dorește criptat cu cheie necunoscută. Misiunea lui este să afle cheia folosită la criptare. Se recomandă a se evita punerea la dispoziția criptanaliștilor a unui text clar și a variantei criptate.

Text clar cu selecție adaptată. Este o formă a textului clar ales, numai că selecția textului clar se schimbă în funcție de rezultatele anterioare.

Numai text criptat. Aceasta este situația în care atacatorul nu are nici o idee asupra conținutului mesajului și trebuie să „lucreze” doar cu textul criptat. În practică este deseori posibil să se intuiască bucăți din textul criptat, în special părți din antetul documentelor sau formule de final. Multe spargerii se bazează pe analiza frecvenței apariției caracterelor, dar la sistemele actuale de criptare rezultatele sunt aproape nule.

Text criptat selectat. Se selectează părți din textul criptat pentru a încerca aflarea cheii, având acces la aceleași bucăți de text clar.

Text criptat cu selecție adaptată. O formă similară celei anterioare, dar selecția porțiunilor din textul criptat pentru tentativa de decriptare va ține cont de rezultatele anterioare.

Atacul „zi-de-naștere”. De regulă, se aplică probabilității ca două mesaje diferite folosind aceeași funcție de dispersie să producă un rezumat comun al mesajului. Termenul „zi-de-naștere” 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 aceeași zi de naștere.

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 și compararea rezultatului cu ceea ce se obține „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 rețele – memorează și dă mai departe – va intercepta mesajele și versiunile modificate ale mesajului original în timp ce se află între două părți în așteptarea comunicațiilor securizate.

Criptanaliza diferențială. Se aplică sistemelor criptografice bazate pe chei private, prin urmărirea unei perechi de texte criptate care au fost obținute prin criptarea aceleiași perechi, dar de text clar, cu diferențele de rigoare, iar din analiza acestora se încearcă a se afla sistemul de criptare.

Criptanaliza liniară. Folosindu-se perechi de text clar cunoscut și textele criptate corespunzătoare, se încearcă aproximarea liniară a unei părți din cheie.

Criptanaliza diferențială liniară. Se folosesc cele două metode descrise anterior.

Factorizarea. Se folosesc metode matematice pentru determinarea factorilor primi ai numerelor mari.

Statistica. Se exploatează slăbiciunile funcțiilor de randomizare folosite la generarea cheilor.

Atac împotriva sau folosind anumite echipamente. În ultimii ani, au apărut tot mai multe echipamente mobile de criptare și, 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, radiațiile).

Erori în sistemele de criptare. Uneori, existența unor erori în sistemul de criptare poate să-i conducă pe criptanaliști la descoperirea cheilor de criptare.

Calculatoare cuantice. Calculatoarele pe bază de cuante se află în atenția multor cercetători, deoarece ele vor fi mult mai puternice decât actualele calculatoare seriale. Puterea se obține prin paralelismul inerent al mecanicii cuantice. Așa că, în loc să se efectueze sarcinile câte una pe unitate de timp, cum funcționează 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 același timp, optimiștii 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 și calculatoare paralele foarte puternice. Practic, ideea este, deocamdată, greu realizabilă. Dacă vor deveni realitate discuțiile sunt aceleași ca și la calculatoarele cuantice.

În practică, sunt multe alte tipuri de atacuri și tehnici de criptanaliză. Se consideră că descrierile anterioare ar fi suficiente pentru proiectanții sistemelor criptografice dacă ar ține cont de ele în totalitate, ceea ce este aproape imposibil.



Pe baza informațiilor din literatura de specialitate, realizați un top al celor mai dese atacuri criptografice.

Rezumat

Scopul criptografiei este de a proteja informațiile transmise fără să poată fi citite și înțelese decât de către persoanele cărora le sunt adresate. Teoretic, persoanele neautorizate le pot citi, însă, practic, citirea unei comunicații cifrate este doar o problemă de timp – efortul și 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) și criptografia prin chei asimetrice (chei publice).

Cele mai cunoscute metode de criptare sunt: substituția, transpoziția (permutarea), cifrul lui Verman, cifrul carte, codurile, ascunderea informațiilor (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 performanță 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: forța brută, text clar cunoscut, text clar ales, text clar cu selecție adaptată, numai text criptat, text criptat selectat sau cu selecție adaptată, atacul "zi-de-naștere", întâlnire-la-mijloc, om-la-mijloc, criptanaliza diferențială, liniară sau mixtă, factorizarea, statistica, atac împotriva sau folosind anumite echipamente etc.

CAPITOLUL VI

Asigurarea securității sistemelor informaționale publice și private

Cunoscută fiind importanța securității fizice, în capitolul de față vor fi tratate inițial subcomponentele ei – amplasarea centrelor de prelucrare automată a datelor, securitatea echipamentelor –, după care vor fi abordate aspecte ale securității softului și personalului. Sistemul, în integritatea sa, va avea un tratament special, într-un paragraf distinct, iar altul va prezenta responsabilitățile dintr-o organizație pe linia prelucrării automate a datelor. Ca obiective, ne dorim de la cititorii noștri:

- dobândirea de cunoștințe privind securitatea locului de amplasare a centrelor de prelucrare;
- cunoașterea modalităților de asigurare a securității echipamentelor și softului;
- familiarizarea cu măsurile ce vizează securitatea pe linia personalului;
- identificarea principalelor metode de asigurare a securității la nivelul sistemului informatic;
- crearea suportului necesar pentru aplicarea măsurilor administrative pe linia securității.

6.1 Securitatea locului de amplasare a centrelor de prelucrare a datelor

Despre măsuri speciale de asigurare a securității 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 atribuțiile responsabilului cu securitatea sistemului. De regulă, centrele de calcul se amplasează în clădiri special construite, preferându-se terenurile virane. Totuși, 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 și care dispun sau nu de sisteme de protecție speciale. De asemenea, clădirile sunt folosite și în alte scopuri, găzduind mai multe servicii ale aceleiași unități sau chiar mai multe unități, cu activități diferite, uneori chiar de ordinul sutelor, cum a fost cazul World Trade Center. În astfel de situații, apar anumite restricții, unele imperfecțiuni, 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 față de cotele de inundație trebuie să fie evident.
3. Mediul de amplasare, de asemenea, nu trebuie să fie afectat de cutremure, zgomote, vibrații, câmpuri electromagnetice (ale radarelor) sau de poluare a aerului. Zona trebuie să fie liniștită, și nu una cunoscută pentru numeroasele incidente sociale. Vecinii sunt liniștiți? Cu ce se ocupă?
4. Cum funcționează serviciile de utilități în zona de amplasare? Curentul și apa au un regim sigur de funcționare? Drumurile în ce stare sunt? Serviciile speciale de intervenție

(pompieri, salvare, poliție) sunt amplasate în apropiere? Au experiența 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 puțin 10 metri de spațiu 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 părțile de clădirile firmei, izolând-o, în acest mod, de lumea din afară.



Cum credeți că se modifică cerințele de securitate de mai sus în cazul data center-urilor moderne? Propuneți un set de cinci recomandări valabile pentru asigurarea securității amplasării centrelor de date.

6.1.2 Proiectarea centrului de calcul

După alegerea locului de amplasare, se poate trece la schițarea machetei clădirii care să găzduiască sistemul electronic de calcul. Cât ar fi de entuziaști proiectanții, îndeosebi arhitecții, uneori, în afara gustului lor deosebit pentru estetic, trebuie rugați să mai respecte și alte elemente, și anume:

1. Clădirea trebuie să fie una solidă, realizată din materiale neinflamabile. Sala calculatorului central (a serverelor) se recomandă să nu aibă ferestre și pe absolut toate părțile să fie înconjurată de alte săli ale centrului de prelucrare respectiv.
2. Numărul intrărilor și ieșirilor din clădire trebuie să fie minim, respectându-se, totuși, normele pe linie de stingere a incendiilor. Pentru introducerea în clădire a echipamentului și a mobilierului mare se poate proiecta o intrare specială, dar ea nu va fi folosită și pentru persoane. Intrarea principală a acestora trebuie să dispună și de o așa-zisă „zonă tampon”, unde să aibă loc procedurile de control și acceptare a intrării în unitate.
3. Cheile, îndeosebi cele ce înlesnesc accesarea mai multor puncte de intrare, trebuie să fie tratate cu același interes ca și lucrurile sau informațiile protejate. Toate cheile se dau numai sub semnătură persoanelor ce le primesc, întocmindu-se, în același timp, și un registru special al posesorilor de chei, care, la rândul lor, vor prezenta și autorizarea posesiei cheilor.
4. Parterul și etajul întâi, pe cât posibil, nu trebuie să aibă ferestre externe pentru a se evita intrarea prin forțarea 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 protecție.
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 și de eventualii intruși, motiv pentru care etajul unu este cel mai sigur.
6. În interiorul centrului trebuie să se efectueze o judicioasă compartimentare a spațiului, nepermițându-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 ș.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 și din motivul supravegherii continue a lor. Supravegherea zonei exterioare a clădirii și 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 și corpuri speciale de pază.

8. Un rol deosebit îl vor avea procedurile de verificare a sistemelor de alarmă, precum și 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 condițiilor de derută în sistem, astfel încât acesta să fie atacat cu ușurință de către intruși.
9. Se impune crearea unui sistem sigur de control al securității transportului unor resurse (suporturi magnetice, rapoarte, documentație ș.a.). Persoana care efectuează transportul trebuie să aibă autorizare specială.
10. Un control special se impune și pentru preîntâmpinarea deplasării neautorizate a unor componente din sistem.
11. Sistemele de asigurare a serviciilor de furnizare a apei, energiei electrice, gazului și facilitățile de comunicații trebuie să fie amplasate subteran. Canalele de acces la ele trebuie să fie, de asemenea, încuiate și supravegheate. Conductele de apă și sistemul de canalizare nu trebuie să traverseze spațiile ce găzduiesc averile informatice ale firmei, ci să le înconjoare. Dacă ocolirea nu este posibilă, se impune montarea unor ventile suplimentare.
12. Copiile de siguranță trebuie să fie păstrate în clădiri speciale, la cel puțin 100 de metri de cea a centrului de prelucrare a datelor.
13. O atenție deosebită se va acorda și tablourilor de control căldură, aer condiționat, linii telefonice și 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 și consumul de lichide și mâncare. Pentru păstrarea țigărilor, 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 și evitându-se lemnul din configurația sălii, precum și covorele și perdelele. Echipamentele, care prin funcționare produc și impurități, trebuie să fie amplasate cât mai departe de echipamentele foarte sensibile.



Cum credeți că se modifică cerințele de securitate de mai sus în cazul data center-urilor moderne? Propuneți un set de cinci recomandări valabile pentru asigurarea securității proiectării centrelor de date.

6.1.3 Protecția și securitatea mediului de lucru al calculatoarelor

Serviciile și utilitățile dintr-un centru de prelucrare automată a datelor joacă un rol foarte important în configurația sistemelor, constituind de multe ori punctele nevralgice ale acestora. Proasta funcționare a lor paralizează și cele mai performante echipamente de prelucrare automată a datelor și din această cauză se recomandă luarea unor măsuri suplimentare, dintre care amintim:

1. *Lumina.* Comutatoarele și 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 și mai riguroase figurează apelarea la acumulate 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 strictețe, conform recomandărilor producătorilor, de regulă între 19-24 grade Celsius.
3. *Sistemul de aer condiționat.* Chiar și sistemele foarte moderne funcționează optim numai în anumite condiții de temperatură și umiditate. Se recomandă un sistem propriu de aer condiționat 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 ș.a.

Una dintre recomandările anterioare se referea la evitarea construirii clădirilor din materiale ușor 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 curățenii 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 inițiate toate măsurile de pază împotriva incendiilor, cum sunt:

1. Utilizarea ușilor și pereților rezistenți la incendiu. Ele trebuie să reziste sub foc cel puțin o oră. Ușile 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 funcționeze pe bază de baterii. Sistemul de aer condiționat, dacă devine un real pericol prin funcționarea sa, trebuie să se blocheze automat, dar să se și deblocheze atunci când este necesară eliminarea fumului.
2. Se va întocmi un plan de intervenție în caz de incendiu, în care se vor cuprinde condițiile de evacuare, de stingere a incendiului și de protejare a valorilor deosebite din sistem. Personalul va fi instruit în acest sens.
3. Asigurarea cu echipamente și materiale speciale pentru intervenție în caz de incendiu, un rol aparte avându-l stingătoarele de incendii electrice și ne-electrice. Personalul trebuie să le cunoască. De regulă, pentru incendiile la instalațiile electrice se recomandă stingătoarele bazate pe bioxid de carbon, iar gazul se stinge cu apă.
4. Instalarea în toată clădirea a detectoarelor de fum și de temperaturi foarte ridicate. Ele au rol de semnalizare și depistare a momentului în care să se declanșeze 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 și stingătoarele cu apă, dar numai atunci când incendiul ia proporții și nu mai contează dacă echipamentele vor fi afectate mai mult sau mai puțin.
5. Orientarea preocupărilor și spre celelalte zone importante ale centrului, nu numai asupra sălii calculatorului. Uneori sursele de incendii sunt mai numeroase în afara sălii calculatorului.



Analizați modul în care sunt respectate măsurile de mai sus într-o organizație cunoscută de dumneavoastră.

6.2 Securitatea echipamentelor

Datorită importanței lor deosebite, componentele sistemelor electronice de calcul trebuie să beneficieze de un tratament aparte.

Se știe că o cale sigură de compromitere a securității unui sistem electronic de calcul este de natură fizică, modificându-i anumite elemente din configurație astfel încât, față de configurarea dată de utilizator, să se creeze căi de acces pentru cei rău intenționați sau să se blocheze mijloacele de asigurare a securității sistemului. În acest sens, se pot modifica circuitele electronice, se pot adăuga mici „șmecherii” (circuite cu rol special, emițătoare, microfoane), se pot realiza derivații ale canalelor de comunicație, pot fi scurt-circuitate componentele cu rol de protecție, 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 defecțiuni de fabricație, fie instalării greșite, fie datorită defectării în timpul transportului. Dar, cel mai grav, echipamentele pot „cădea” în timpul exploatării lor, devenind atât ele, cât și datele conținute în memorie inutilizabile. Uneori și 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 apăsă asupra a ceea ce s-a cumpărat și consecințele sunt și mai grave atunci când distribuitorul este un ilustru necunoscut.

Întreținerea sau depanarea sistemului sunt asigurate, de regulă, de specialiști din afară. Cu multă ușurință ei pot realiza toate operațiunile menționate anterior pentru paralizarea sistemului.

Apărarea împotriva tuturor pericolelor descrise are un rol vital în buna funcționare a sistemului. Totuși, trebuie pornit de la faptul că toate componentele sistemelor, la rândul lor, pot dispune de elemente proprii de asigurare a securității.

6.2.1 Asigurarea echipamentelor împotriva intențiilor de modificare a lor

Toate componentele sistemelor de prelucrare automată a datelor trebuie protejate, fie împotriva hoților, fie a vandalilor. Sunt unele elemente care necesită însă o grijă deosebită. De exemplu, terminalele nu sunt la fel de importante ca și calculatorul central sau serverele sistemului.

Echipamentele pot fi protejate împotriva modificării lor astfel:

- Birourile ce conțin 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 conțin imagini unice, imposibil de recreat.
- Echipamentele trebuie să fie, pe cât posibil, mai dispersate, îndeosebi în cazul lucrului cu informații speciale.
- Elementele din configurația 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 și confirmat ulterior când se solicită o operațiune la/de la perifericul respectiv. Fiecare imprimantă, terminal sau legătură din rețea trebuie să aibă definite categoriile de informații cu care pot lucra sau funcțiile din sistem ce se realizează prin intermediul lor. Numerele unice de identificare înlesnesc tratarea diferențiată 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 și 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 angajaților firmei să lucreze peste program, iar când aceasta se impune va fi sub un control riguros.

6.2.2 Controlul integrității echipamentelor

Calculatoarele pot să-și verifice singure starea în care se află celelalte componente, prin autodiagnoză, astfel încât să poată descoperi ce nu funcționează cum trebuie. Printre activitățile realizate de calculatoare vor fi verificarea modului de lucru, inclusiv urmărirea funcțiilor de realizare a securității sistemului, precum și facilitățile de control al accesului.

Autodiagnoza este utilă pentru:

- confirmarea cu precizie a identității echipamentelor, suporturilor și utilizatorilor - elementele de bază ale sistemului;
- verificarea dacă utilizatorii folosesc doar echipamentele, softul și datele la care ei au acces de drept și preîntâmpinarea accesului neautorizat;
- asigurarea că orice tentativă de acces sau utilizare neautorizată a echipamentelor, softului sau datelor este blocată și că supraveghetorii sistemului vor fi anunțați imediat.

Simpla realizare a funcțiilor de mai sus nu înseamnă neapărat și perfecțiunea sistemului de securitate, dar constituie suficiente măsuri de apărare a sistemului împotriva atacurilor rău intenționate.

Există și producători de calculatoare care asigură facilități de diagnoză de la distanță a stării sistemului, ceea ce în mod normal se realizează de către echipele de service, pentru a se asigura că totul funcționează corect și că nu se conturează posibilitatea apariției unor defecțiuni. O astfel de metodă este benefică pentru unitate, întrucât duce la reducerea costurilor și se realizează mult mai rapid decât în varianta apelării la inginerii de întreținere. Totuși, diagnoza de la distanță este destul de periculoasă pentru securitatea sistemului, intrușilor oferindu-li-se o șansă în plus să acceseze orice element din configurație, aceștia având la dispoziție o linie specializată. Așadar, aparentul cost redus poate să însemne pierderi mult mai mari.

6.2.3 Proceduri de întreținere a echipamentelor

Activitățile de întreținere și reparare a oricărui echipament pot genera o mulțime de semne de întrebare privind siguranța, securitatea și disponibilitatea datelor din sistem. Din această cauză este foarte important să se controleze accesul la echipamente și software și să se supravegheze îndeaproape specialiștii care asigură întreținerea sau repararea sistemului.

O primă măsură va consta în deschiderea unui registru de întreținere, în care să se înregistreze toate detaliile privind o astfel de activitate. Ele se vor referi la data și timpul efectuării lor, numele tehnicienilor, motivul vizitei lor, acțiunile și reparațiile 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 și în cazul diagnozei de la distanță, în timpul întreținerii sau reparării sistemului trebuie să fie scoase datele și softul de pe benzi sau pe discuri de orice tip, iar cele din memoria principală, de asemenea, salvate, reinițializându-se sistemul numai în acest scop. Specialiștilor ce efectuează întreținerea nu trebuie să li se înlesnească accesul la datele speciale ale unității, în mod deosebit la parolele acesteia.

Dacă sistemul este defect și măsurile de precauție enumerate nu mai pot fi luate, se recomandă ca specialiștii unității să fie alături de cei ce asigură întreținerea pentru a ști cu exactitate ce anume efectuează. În acest scop, ei chiar pot fi întrebați de ce efectuează operațiunile respective.

Activitățile de întreținere trebuie să aibă un plan, în totală concordanță cu planul de funcționare al întregului sistem. De regulă, producătorii specifică termenele la care să se

realizeze întreținerea fiecărei componente. Numai responsabilul sistemului poate accepta efectuarea unor operațiuni înainte de termen, precum și repararea, înlocuirea sau înnoirea unor elemente din sistem.

Se recomandă ținerea evidenței materialelor de rezervă, chiar a imprimantelor, terminalelor sau monitoarelor, iar consumabilele să fie comandate la timp pentru a nu se produce disfuncționalități în sistem.

Testarea securității sistemului trebuie să se realizeze înainte ca acesta să înceapă prelucrarea datelor reale ale unității.

Numele specialiștilor în întreținere, precum și al furnizorilor de utilități, trebuie să fie afișate la vedere pentru o contactare a lor în orice moment, de către persoanele autorizate să facă acest lucru.

Dacă inginerii de întreținere solicită scoaterea din unitate a unor componente sau a documentației firmei, în primul rând, trebuie să ne asigurăm că ele nu conțin date importante ale firmei. Este mult mai recomandat ca datele aflate pe unele suporturi să fie distruse, decât să se mizeze pe discreția specialiștilor. 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 funcționarea lui corectă în continuare, dar nimeni nu știe exact cum funcționează. Și încă ceva: depinde și de cine face „cârpeala” programului și cu ce scop. Și astfel de operațiuni se scriu în registrul de întreținere.

6.2.4 Toleranța la cădere a echipamentelor

Cel mai cunoscut este sistemul din aviație care, în cazul când o componentă se defectează, dispune de alta care să-i preia funcția. 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 siguranță s-au defectat. Toleranța la cădere a avioanelor este asigurată astfel încât să nu aibă loc prăbușirea lor.

În cazul calculatoarelor aceasta este o calitate foarte importantă, absolut vitală pentru existența sistemelor performante. Toleranța la cădere sau la defecte trebuie să contribuie la prevenirea pierderilor sau denaturării datelor și, pentru aceasta, orice apăsare de tastă trebuie să fie înregistrată undeva, astfel încât să poată fi restaurată prin anumite proceduri. Toleranța la cădere trebuie să facă în așa fel încât să permită funcționarea sigură, controlată și supravegheată, în timpul reparării, asigurându-se astfel funcționarea continuă a calculatorului care a înregistrat o defecțiune, chiar și una majoră, în timp ce se lucrează pentru îndepărtarea ei. În practică, așa-ceva este destul de greu de realizat, dar, dacă numărul componentelor cu rol vital în existența sistemului s-ar reduce și ar avea mai mulți înlocuitori, operațiunea este, totuși, posibilă.

În sensul celor spuse până acum, sunt tipuri de calculatoare care funcționează cu două unități centrale de prelucrare, în tandem, ambele prelucrând în același timp aceleași date și programe. Pe această cale, la eventuala cădere a uneia dintre ele, cealaltă va funcționa singură până când a doua va fi repusă în funcțiune. Echipamentele sunt amplasate în săli apropiate și folosesc aceleași condiții de lucru, cum ar fi: aer condiționat, linii de comunicație, tipuri de unități de bandă și de discuri, surse de energie electrică și alte utilități. 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 aplicații, funcționarea în tandem evită căderea sistemului în întregime.

Alte componente ale sistemelor electronice de calcul sunt astfel construite încât să-și exercite unele funcții în formă dublă. Un exemplu îl oferă metoda înregistrării „în oglindă” pe disc, prin care două discuri sunt scrise în același timp pentru prevenirea pierderilor de date, dacă s-ar defecta capetele de citire-scriere ale unuia.

Echipamentele folosite în condiții dificile, cum sunt cele mobile din domeniul militar, sunt amplasate în containere speciale, deosebit de rezistente la șocuri, apă și praf. Sistemul de cablare va fi protejat prin țevi metalice, iar căderile de energie vor fi suplinite de un sistem energetic propriu.

Toate măsurile luate pentru eventualele căderi trebuie să fie în deplină concordanță și cu importanța întregului sistem de prelucrare automată a datelor.

6.2.5 Contractele

Unul dintre cele mai neplăcute momente referitoare la configurația sistemului îl reprezintă lungile discuții purtate cu cei ce le-au livrat, atunci când sistemul se defectează sau nu funcționează la parametri așteptați. Sunt cunoscute suficiente mici necazuri din lumea calculatoarelor, numai că producătorii de sisteme n-au nici un interes să le popularizeze, fie din dorința de a nu-și păta reputația, fie mizând pe faptul că ele nu vor fi ușor sesizate.

Aproape că a devenit o regulă supraestimarea caracteristicilor calculatoarelor. Vanzătorii sunt, de cele mai multe ori, nesinceri sau prea încrezători în produsele ce le comercializează, imboldul venind de la producători, care își prezintă produsele ca fiind cele mai bune, în raport cu ale concurenților de pe piață.

De vină sunt și beneficiarii care, deseori, subestimează sau nu cunosc ceea ce vor. De cele mai multe ori, vor sistemele cele mai ieftine, dar își schimbă părerea când le pun în funcțiune, ajungând la concluzia că era mai bine dacă acesta ar dispune și de niște funcții 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 părțile de discuții interminabile.

Din prima fază, clientul trebuie să ofere distribuitorului de sisteme următoarele elemente:

1. O foarte clară definiție a sistemului dorit:
 - a) descrierea funcțiilor solicitate acestuia și componentele cu rol prioritar din structura sa. Dacă este nevoie de un procesor de texte, atunci trebuie cerut așa-ceva, dacă se cere un soft de birotică, trebuie menționat ca atare; oricum, nu trebuie să ne așteptăm ca un soft de un tip anume să ne onoreze toate pretențiile de prelucrare automată a datelor;
 - b) descrierea intențiilor de extindere a sistemului în viitor, îndeosebi dacă se vrea crearea unei rețele de calculatoare;
 - c) detalii privind gradul de încărcare a sistemului în perspectivă, specificându-se numărul utilizatorilor, tipul activităților de executat, cerințele rețelei, importanța ce o va avea sistemul și, de aici, cerințele pe linie de întreținere și reparare a lui.
2. Stabilirea nivelului de securitate dorit în sistem, astfel încât furnizorul să știe 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 și observațiile de pe parcurs, conversațiile telefonice, cu data corespunzătoare, cât timp au durat și cu cine s-au purtat, ce literatură s-a consultat, ce prezentări au fost făcute de către furnizor ș.a.
4. Cuantificarea, dacă este posibilă, a efectelor defectării totale a sistemului sau a nefuncționării lui la parametri promiși. Furnizorii trebuie să ia cunoștință 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 știe din timp ce trebuie să ofere sistemul și să facă promisiunea onorării tuturor cerințelor.
6. De asigurat că serviciile garantate prin contract pot fi onorate într-un timp bine determinat, stabilind cu exactitate ce misiuni revin specialiștilor, definind obligațiile

contractuale, responsabilitățile și termenele de plată. De toate aceste aspecte trebuie să se ocupe o persoană ce va fi numită în acest sens.



Analizați modul în care se asigură securitatea echipamentelor într-o organizație cunoscută de dumneavoastră.

6.3 Securitatea software-ului

Softul unui calculator cuprinde instrucțiunile sub care funcționează întregul sistem. Aceste instrucțiuni, sub formă de programe, îi vor spune calculatorului ce trebuie și ce nu trebuie să facă cu datele, cum să le păstreze, ce regim au ieșirile 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 și unele măsuri pe linia realizării securității.

6.3.1 Obiectivele securității prin software

Există trei funcții principale pe care softul trebuie să încerce a le asigura. Ele se referă mai degrabă la confidențialitatea datelor, decât la integritatea sau disponibilitatea lor.

1. *Accesul*. Softul trebuie să discearnă între utilizatorii autorizați și intruși, iar în ultimul caz să le blocheze accesul.
2. *Delimitarea*. Softul trebuie să delimiteze diversele activități ale utilizatorilor și să îi trateze după nivelul lor de autorizare la categoriile speciale de date ce urmează a fi prelucrate. Ca atare, și baza de date va fi compartimentată după reguli foarte riguroase pe linia securității sistemului.
3. *Auditarea*. Poate mai clar ar fi „proba auditării”, întrucât a treia funcție se referă la capacitatea sistemului de a reține ce persoane, cât timp, cu ce date au lucrat și ce au urmărit.

Un soft de sistem eficient trebuie să blocheze relele intenții, să prevină accesul neautorizat și să înregistreze tot ce efectuează pentru a avea ulterior forță probantă.

6.3.2 Limitele softului pentru asigurarea securității

O lungă perioadă de timp, de problemele securității sistemelor electronice de calcul s-au ocupat doar persoanele implicate în prelucrarea automată a datelor, însă de mai mult timp se simțea nevoia transferării lor în zona softului sistemelor, mutație ce a avut loc, dar căreia imediat a și început să i se aducă obiecțiuni de genul:

- softul este foarte scump. Chiar și programele destul de simple ocupă mii de linii-program, toate realizate de către om, dar cele de asigurare a securității sunt deosebit de complexe și, firește, de scumpe;
- de regulă, programele conțin și erori;
- testele de verificare a lor nu sunt perfecte;
- softul pentru securitate diminuează capacitățile și viteza de lucru a întregului sistem;
- producătorii de hard și soft nu dispun de standarde pe linia securității sistemelor;
- utilizatorii nu au cunoștințe suficient de detaliate despre hard și soft încât să poată sesiza cele mai inteligente subtilități cu intenție de fraudă incluse în softul cumpărat;

- eventualele disfuncționalități ale softului pentru securitatea sistemului oferă posibilitatea specialiștilor în întreținerea sistemului să intre în intimitatea lui, deci și să-l poată influența;
- poate lucra perfect doar „la suprafață”, el conținând aspecte esențiale compromițătoare invizibile;
- softul poate să conțină pericole deosebit de mari care nu pot fi sesizate și nici nu sunt periculoase o lungă perioadă de timp de la instalarea lui (bombele logice, caii troieni ș.a.);
- „loviturile” prin soft sunt insesizabile prin mijloacele obișnuite de percepție ale omului;
- în final, datorită curentului sistemelor deschise, a conectării într-o mare varietate de rețele și a gestionării unor baze de date masive de către mii de persoane, măsurile de realizare a securității prin software pentru aceste sisteme gigant sunt extrem de greu de realizat.

În aceste condiții, când cheltuielile sunt foarte mari, când cu mare greutate se asigură o oarecare doză de încredere în soft, apar ca fiind mai ieftine și mai eficiente alte măsuri de realizare a securității sistemelor de prelucrare automată a datelor. Chiar dacă softul joacă un rol destul de important, nicidecum nu trebuie neglijate și alte modalități. Până și furnizorii spun că virtuțile softului sunt relativ dependente de calitățile beneficiarului, dar că măsuri sigure sunt cele de încuiere a ușilor, de urmărire a personalului ș.a.

Cât timp nici cele mai importante sisteme de prelucrare automată a datelor, cum sunt cele din domeniul militar sau bancar, nu au protecție de 100%, apare ca o necesitate stringentă apelarea și la alte metode. Și încă un detaliu: cât timp hoții au demonstrat că sunt mai puternici decât producătorii softului de securitate, cum să existe o încredere mai mare în ultimii, deci și în produsele lor !?!

6.3.3 Măsuri generale de asigurare a securității softului

Practica menționează o întreagă serie de măsuri de protejare a sistemului de operare și a altor programe de la distrugerii sau acțiuni subversive, după cum urmează:

- toate activitățile de programare (modificare, scriere, utilizare etc.) trebuie să fie executate sub cele mai riguroase norme de disciplină, consemnate în scris la nivel de unitate și prin contractul de angajare. Controlul activității de programare este foarte important pentru viitorul unității;
- programele deosebit de importante și documentația aferentă trebuie să fie supuse acelorași reguli de protecție fizică așa cum au și calculatoarele pe care se rulează;
- copiile de siguranță ale programelor și datele corespunzătoare, bineînțeles că nu trebuie uitată și documentația, trebuie să fie păstrate în aceleași condiții ca și originalele;
- etapele realizării programelor trebuie să fie derulate sub un riguros control, verificate și testate în toate stadiile de realizare, pentru asigurarea încrederii în rezultatul final;
- întregul proces de elaborare a programelor trebuie să fie însoțit de documentația aferentă;
- realizarea programelor se va efectua pe calculatoare care nu execută și alte activități în același timp;
- programele trebuie să fie însoțite de numele realizatorilor lor sau ale celor ce le-au adus unele modificări;
- benzile și discurile ce conțin 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 știe”;
- o copie de bază a sistemului de operare trebuie să fie păstrată în condiții sigure de către responsabilul sistemului și 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 și rutine de securitate pentru a verifica integritatea sistemului de operare în folosință;
- nu trebuie să se permită crearea copiilor softului sistemului de operare de către personalul care utilizează sistemul, îndeosebi cel ce lucrează la distanță. În acest scop, chiar sistemul de operare trebuie să conțină măsuri de autoprotecție la intențiile de copiere;
- orice „fisură” a sistemului de operare trebuie să fie adusă la cunoștință proiectanților sistemului, producătorilor de echipamente, utilizatorilor, iar gradul de expunere la riscuri trebuie să fie adus la cunoștință conducerii firmei;
- normele interne trebuie să prevadă ca mai mult de o persoană să se ocupe de implementarea și testarea sistemului de operare, pentru reducerea riscului realizării unor activități subversive la nivel de persoană;
- inițializarea sistemului de operare și oprirea lui, de asemenea, presupun proceduri foarte riguroase de respectat. La fel se va proceda și la reîncărcarea sistemului după o defecțiune;
- registrul sistemului trebuie să consemneze absolut toate operațiunile la care acesta este supus în timpul funcționării (defecțiuni, erori, căderi, reluări, pauze, timp lung de răspuns, semnale sonore neobișnuite ș.a.);
- nu trebuie lăsat sistemul să funcționeze cu așa-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 și 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 aceluiași funcții, rutine sau programe pe calculator.



Analizați modul în care se asigură securitatea software-ului într-o organizație cunoscută de dumneavoastră.

6.4 Securitatea personalului

Atunci când punem problema personalului ne gândim îndeosebi la angajații unității, dar tot aici pot fi incluse și alte categorii din afară, capabile de orice. La nivelul anilor 2000, se înregistrau următoarele categorii de incidente sau de persoane producătoare de prejudicii:

1. *Violența*. 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 și nu banii.
3. *Delapidarea*. Angajații „șterpelesc” bani din sistemul informatic.
4. *Escrocheria*. Furnizorii de hard și soft înșeală printr-o descriere eronată a produselor pe care le comercializează.
5. *Abuzul*. Angajații, apelând la statutul de utilizatori ai sistemului, folosesc resursele acestuia pentru plăceri personale sau pentru a obține un profit.
6. *Modificarea*. Schimbarea înregistrărilor memorate.
7. *Spionajul*. Aici se încadrează spionajul industrial sau străin pentru a afla secretele de fabricație, programele sau manualele de utilizare.

8. *Violarea legislației privind exportul*. Vânzarea componentelor hard și soft deosebit de importante către potențiale țări străine ostile.
9. *Hackerii* sunt cei care trec frontierele sistemelor electronice, îndeosebi de calcul sau de telecomunicații.
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 și sistemele de apărare ale sistemelor electronice de calcul. Phreakerii și crackerii sunt subspecializări ale hackerilor, dar mult mai periculoase.
12. *Lamer* desemnează categoria rataților în piraterii, de regulă, un hacker slab. Și când sunt crackeri, neavând o „instrucție” riguroasă, se comportă lamentabil, ca orice autodidact.
13. *Wannabe* reprezintă hackerii începători. Ei vor, dar nu prea pot, întrucât au cunoștințe limitate. În schimb, dispun de un timp nelimitat și fac zgomot despre succesele înregistrate, ceea ce contribuie la prinderea lor cu ușurință. În unele materiale ei sunt cunoscuți și sub numele de *script kiddies*.
14. *Respingerea* constă în indisponibilizarea resurselor sistemului de către angajați, prin sabotaj.
15. *Folosirea frauduloasă* a calculatoarelor pentru comiterea de crime, păstrarea unor evidente a materialelor interzise sau pornografice.
16. *Violarea copyright-ului* prin difuzarea ilegală a copiilor programelor.
17. *Infrațiuni economice sau legislative*, cum sunt violarea legilor antitrust, corupție, mituire de către companiile producătoare de hard, soft, servicii.

Dintr-un studiu al cazurilor privind securitatea sistemelor informaționale, 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, procurați prin introducerea unor date fictive de către funcționarii sistemului, până la zeci de milioane de dolari, obținuți 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 piața cu astfel de componente, vândute ilegal.

În 1982, crima anului a fost din domeniul spionajului industrial, prin faptul că hoții sustrăgeau secretele de fabricație pentru a câștiga, ulterior, piața.

În 1983, escrocheria se află pe locul întâi, producătorii dezinformând cumpărătorii pe linia performanțelor produselor scoase la vânzare.

În 1984, pe primul loc s-a situat încălcarea legilor referitoare la export, scoțându-se din SUA mari cantități de calculatoare, care erau sub embargo, și erau livrate în Europa de Est și URSS.

În 1985, încălcarea copyright-ului s-a aflat pe primul loc, cu scopul copierii neautorizate și vânzării pe piață a copiilor pirat.

La nivelul anilor 1997-2002, din studiile întreprinse de Institutul de Securitate a Calculatoarelor și FBI, rezultă că s-au produs mutații importante în domeniul atacurilor sau folosirii ilegale a sistemelor de prelucrare automată a datelor, conform situației din tabelul 6.1. Pierderile înregistrate se regăsesc în tabelul 6.2. O situație similară este prezentată în tabelul 6.3, pentru perioada 2003 – 2007.

Cei chestionați au declarat că sursele de atac sunt din următoarele categorii: angajați nemulțumiți (89%), hackeri independenți (72%), corporații de pe teritoriul SUA (48%), corporații străine (29%), organizații guvernamentale străine (21%).

Tabel nr. 6.1 – Tipuri de acțiuni frauduloase în domeniul informațiilor

Tipul acțiunii frauduloase	Număr respondenți cu pierderi*						
	1997	1998	1999	2000	2001	2002	2003
Furtul datelor personale	21	20	23	22	32	26	61
Sabotarea datelor din rețea	14	25	27	28	26	28	61
Interceptarea telecomunicațiilor	8	10	10	15	16	5	-
Penetrarea sistemului din afară	22	19	28	29	42	59	88
Accesarea abuzivă a rețelei 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
Înșelătorii	4	-	-	-	-	-	-
Virusi	165	143	116	162	186	178	254
Acces neautorizat din interiorul sistemului	22	18	25	20	22	15	72
Fraudă în telecomunicații	35	32	29	19	18	16	34
Interceptarea activă a comunicațiilor	-	5	1	1	0	0	-
Furturi de laptopuri	165	162	150	174	143	134	250

* Au fost primite răspunsuri de la peste 500 de organizații

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 și raportul CSI/FBI din 2003

Tabel nr. 6.2 – Total pierderi anuale din fraudă informațională, 1997 - 2002

Tipul acțiunii frauduloase	Total pierderi anuale*					
	1997	1998	1999	2000	2001	2002
Furtul datelor personale	20048000	33545000	42496000	66708000	151230100	170827000
Sabotarea datelor din rețea	4285850	2142000	4421000	27148000	5183100	15134000
Interceptarea telecomunicațiilor	1181000	562000	765000	991200	886000	6015000
Penetrarea sistemului din afară	2911700	1637000	2885000	7104000	19066600	13055000
Accesarea abuzivă a rețelei din interior	1006750	3720000	7576000	27984740	35001650	50099000
Fraudă financiară	24892000	11239000	39706000	55996000	92935500	115753000
Respingerea serviciilor solicitate	-	2787000	3255000	8247500	4283600	18370500
Înșelătorii	512000	-	-	-	-	-
Virusi	12948150	7874000	5274000	29171700	45288150	49979000
Acces neautorizat din interiorul sistemului	3991605	50565000	3567000	22554500	6064000	4503000
Fraudă în telecomunicații	22660300	17256000	773000	4028000	9041000	346000
Interceptarea activă a comunicațiilor	-	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 organizații

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 virușilor;
- atacurile prin malware devin din ce în ce mai focalizate, adresându-se unor ținte concrete;
- utilizarea abuzivă, în interes personal, a rețelelor și sistemelor de e-mail ale organizațiilor de către angajați, pentru pornografie și descărcare ilegală de software, este problema cea mai stringentă.

Tabel nr. 6.3 – Total pierderi anuale din fraudă informațională, 2003 - 2007

Tipul acțiunii frauduloase	Total pierderi anuale*				
	2003	2004	2005	2006	2007
Furtul datelor confidențiale (în 2007 cu excepția furtului de dispozitive mobile)	-	-	-	6034000	5685000
Furtul datelor personale	70195900	11460000	30933000	-	-
Sabotarea datelor din rețea	5148500	871000	340600	260000	1056000
Penetrarea sistemului din afară	2754400	901500	841400	758000	6875000
Accesarea abuzivă a rețelei și 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
Virusi (viermi, spyware)	27382340	55053900	42787767	15691460	8391800
Acces neautorizat din interiorul sistemului	406300	4278205	-	-	1042700
Fraudă în telecomunicații	701500	3997500	242000	1262410	651000
Furturi de laptopuri sau dispozitive mobile	6830500	6734500	4107300	6642660	3881150
Phishing	-	-	-	647510	2752000
„Zombie” (bot) în interiorul organizației	-	-	-	923700	2869600
Furtul informațiilor proprietarilor prin furtul dispozitivelor mobile	-	-	-	-	2345000
Furtul informațiilor confidențiale prin furtul dispozitivelor mobile	-	-	-	-	2203000
Modificarea site-urilor Web	-	958100	115000	162500	725300
Folosirea abuzivă a rețelelor wireless	-	10159250	544700	469010	542850
Folosirea abuzivă a mesageriei instant	-	-	-	291510	-
Folosirea abuzivă a aplicațiilor Web publice	-	2747000	2227500	269500	251000
Sniffing de parole	-	-	-	161210	168100
Șantaj	-	-	-	-	160000
Atacuri exploit asupra serverului DNS	-	-	-	90100	104500
Acces neautorizat la informații	-	-	31233100	1061700	-
Ascultarea convorbirilor telefonice	76000	-	-	-	-
Interceptarea activă a convorbirilor telefonice	705000	-	-	-	-
Altele	-	-	-	885000	-
Total	201797340	141496560	130104542	52494290	66930950

* Numărul de organizații 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 organizații:

Tabel nr. 6.4 – Ponderile atacurilor în totalul incidentelor de securitate, 2004 - 2008

Tipul acțiunii frauduloase	2004	2005	2006	2007	2008
----------------------------	------	------	------	------	------

Tipul acțiunii 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 telecomunicații	10%	10%	8%	5%	5%
Acces neautorizat	37%	32%	32%	25%	29%
Virusi (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 informațiilor proprietarilor	10%	9%	9%	8%	9%
• prin furtul dispozitivelor mobile					4%
• din alte surse					5%
Folosirea abuzivă a rețelelor wireless	15%	16%	14%	17%	14%
Modificarea site-urilor Web	7%	5%	6%	10%	6%
Folosirea abuzivă a aplicațiilor Web	10%	5%	6%	9%	11%
„Zombie” (bot) în interiorul organizației				21%	20%
Atacuri asupra serverului DNS				6%	8%
Folosirea abuzivă a mesageriei instant				25%	21%
Sniffing de parole				10%	9%
Pierderea sau furtul datelor clienților				17%	17%
• de pe dispozitivele mobile					8%
• din alte surse					8%

* Au fost primite răspunsuri de la peste 500 de organizații

Sursa: Datele sunt preluate de pe site-ul Computer Security Institute, „2008 CSI Computer Crime and Security Survey”,



Extrageți câteva tendințe din tabelele de mai sus. Comentați-le.

6.4.1 Responsabilități manageriale pe linia personalului

Pe linia asigurării securității din punctul de vedere al personalului trebuie să se urmărească următoarele aspecte:

- selecția;
- verificarea prin prisma securității;
- supravegherea continuă;
- instruirea și conștientizarea.

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 știe”* face ca posesia sau cunoașterea informațiilor, indiferent de categoria din care fac parte, să fie limitată strict și să fie înlesnită doar celor care au atât autorizarea, cât și nevoia evidentă de a le ști, astfel încât să-și poată exercita corect sarcinile de serviciu. Statutul deosebit al unei persoane în firmă nu-i conferă și dreptul nelimitat de cunoaștere a informațiilor 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-și exercita sarcinile de serviciu. Controlul trebuie să fie la fel de riguros și 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 operațiuni importante. Chiar dacă o persoană răspunde de exercitarea unor atribuții de serviciu, ea va efectua activități speciale numai în prezența unei persoane autorizate. Aceasta nu înseamnă un membru al echipei de pază, ci o persoană cu cel puțin aceleași cunoștințe profesionale cu ale executantului de drept. Activitățile speciale, neexecutabile de o singură persoană vor fi prezentate ulterior. Pentru preîntâmpinarea „înțelegerilor” dintre cele două persoane, se recomandă schimbarea lor cât mai des posibil.
4. *Principiul schimbării obligațiilor de serviciu* consemnează că o persoană nu trebuie să exercite o perioadă prea lungă de timp aceleași sarcini de serviciu.

6.4.2 Măsuri pe linia securității din punct de vedere al personalului

În vederea asigurării unor măsuri deosebite pe linia securității din punct de vedere al personalului, se impune parcurgerea unor stadii:

Stadiul 1: *Identificarea locurilor de muncă cu regim special și a calităților persoanelor îndreptățite a le ocupa*

Stadiul 2: *Selecția personalului*

Operațiunea se va realiza înainte de angajare, în timpul procesului de recrutare de personal nou, dar și retroactiv.

Dacă actele la angajare sunt completate corect, unitatea poate să-și găsească suficiente elemente pentru filtrarea personalului. Documentele de angajare vor conține date medicale și informații generale despre persoană. Date suplimentare pot fi oferite de referințele obținute de la precedentul loc de muncă și apoi de la o persoană care să reprezinte o instituție credibilă (școală, justiție, poliție, armată). Dacă se consideră necesar pot fi efectuate și investigații prin firme private.

Totuși, multe elemente edificatoare se pot obține prin interviuarea solicitanților de locuri de muncă. Aspectele urmărite pot fi structurate astfel:

1. Descrierea locului de muncă anterior, funcția deținută, evoluția profesională. Se vor urmări, îndeosebi, eventualele întreruperi de activitate, altele decât concediile sau diverse motive obiective. Spitalizările și arestările vor fi urmărite cu mare atenție pentru aflarea cauzei acestora.
2. Verificarea referințelor și a diplomelor depuse la dosar. Sunt foarte dese cazurile de declarații false despre o vechime avută la unități inexistente sau diplome de la așa-zisele „școli ale vieții”. Nimic nu va fi crezut fără probe suplimentare.

Se va continua cu determinarea:

- a) *competenței*. Diplomele atașate, cu note foarte mari pe ele, nu au acoperire în calitățile profesionale ale persoanei – constatare efectuată prin probe de lucru asemănătoare ultimului loc de muncă, precum și rezolvarea unor stări imprevizibile.
- b) *punctualitatea și absenteismul* vor scoate în relief câtă încredere i se poate acorda individului.
- c) *abaterile disciplinare* vor încerca să evidențieze posibilitatea încadrării persoanei în legalitate, în normele de conduită socială (dacă a fost amendat, dacă a avut procese civile sau penale).
- d) *situația medicală* va scoate la lumină stările de instabilitate mentală, bolile cronice care pot să aibă o motivație socială sau financiară pentru solicitanții posturilor.

Calea prin care se pot obține aceste informații constă în oferirea unei polițe de asigurare de viață, 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 referințe suplimentare?
 - g) există obligații ale solicitantului față de fosta unitate?
 - h) persoana a mai fost angajată la companii private și, dacă da, când și de ce le-a părăsit?
 - i) care au fost relațiile cu foștii colegi de muncă - a fost posibilă integrarea în echipă? Era agreeat și respectat? Avea conflicte cu reprezentanții 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 existență, persoanele cunoscute, legăturile sale de familie au ceva în comun cu concurenții firmei la care cere angajarea? Pentru străini se pot solicita și actele doveditoare ale naționalității.
 4. Există unele indicii ale consumului abuziv de alcool sau droguri?
 5. Solicitantul este membru în asociații profesionale sau economice? Are puncte de vedere politice foarte puternic susținute, care? A exercitat anterior unele activități publice sau funcționărești (consultant, reprezentant sindical ș.a.) care să-i fi întrerupt preocupările profesionale sau să-l determine să fie ușor influențabil în rezolvarea unor posibile conflicte viitoare?
 6. Care îi este viața de familie? Ce activități sociale și sportive îi plac? Dau ele semne de sănătate excesivă sau chiar inexplicabilă, indică o extravaganță ieșită din comun?
 7. Comportamentul la volan, în ipostaza de conducător auto, poate să scoată în relief stări emotive sau de maturitate, controlabilitate, judecată rapidă ș.a.
 8. Dacă este posibil, se va studia situația 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 informații.
 9. Dacă a lucrat în poliție sau armată, trebuie urmărită (cu probe) cauza întreruperii acestor activități.

Literatura recomandă apelarea la companii private care să exercite astfel de activități pentru aflarea informațiilor reale despre solicitanții locurilor de muncă. De asemenea, într-o oarecare măsură, se poate folosi și detectorul de minciuni, deși 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 calitățile de care dă dovadă individul. Testul este foarte bun dacă la sfârșit se va comunica și participanților rezultatul, pentru a-și afla punctele tari sau slabe.

În final, câteva cuvinte despre referințele aduse de angajați și scrisorile de recomandare:

1. Referințele se află sub controlul candidatului la concurs, el rugând pe cineva să le formuleze, deci sunt ușor părtinitoare.
2. Obiectivele urmărite de actuala firmă, interesată să angajeze, nu se pot regăsi printre elementele referințelor. Totuși, o referință bună trebuie să scoată în relief calitățile de care poate da dovadă persoana, iar cel mai des se întâmplă când se încearcă a se scăpa de salarii slabi; o referință categoric proastă este cea care scoate în relief calitățile deosebite ale persoanelor, dar care nu au posibilitatea să fie demonstrate în mediul de lucru existent.
3. Referințele sunt scrise în „limbaje” diferite, în funcție de stilul persoanei, deseori fiind necesară interpretarea cu atenție a diverselor construcții, de genul „a încercat din greu” (eșec), „a obținut rezultate mulțumitoare” (rezervă), „a demonstrat o inteligență medie” (mai mulți colți decât idei), „în general s-a achitat de sarcinile...” (în loc de critică sau

„despre cei plecați numai de bine”). La astfel de exprimări angajările aproape că nu au motivație.

Stadiul 3: Atribuirea responsabilităților pe linia securității

După cum informațiile unui sistem fac parte din categorii diferite, la fel și 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 știe că există trei categorii de angajați:

1. *Neverificabilii* sunt acei angajați cu un statut nu prea clar, ei neputând fi verificați în detaliu prin prisma onestității, încrederii, integrității, loialității față de unitate – motiv pentru care lor nu li se poate acorda accesul la informațiile 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) și li se pot oferi anumite sarcini pe linia accesului la o parte a informațiilor speciale.
3. *Extrem de credibili*. După verificări complexe asupra trecutului unei persoane, ale familiei sale, vieții personale, moralității și rezultatelor înregistrate la vechile locuri de muncă, dacă totul este perfect, aceasta poate fi considerată de încredere și i se poate facilita accesul la cele mai intime date ale firmei. Adevărul este că încrederea și onestitatea pot fi verificate pe parcurs, și nu la data efectuării verificărilor, ceea ce înseamnă o oarecare doză de risc din partea celor ce delegă astfel de responsabilități.

În orice caz, altfel vor fi tratați angajații cu vechime în unitate și altfel cei angajați 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. responsabilitățile persoanei și sarcinile pe linia asigurării securității valorilor patrimoniale și, bineînțeles, a informațiilor, astfel încât:
 - a) să dispară orice dubiu privind persoana care trebuie să exercite o funcție anume;
 - b) să aducă la cunoștința angajaților, din faza de asociere cu unitatea, ce probleme caracterizează activitatea firmei;
 - c) să-i pregătească pentru dobândirea unor calități noi, cerute de unitatea care angajează;
2. regulamentul de ordine interioară a unității și condițiile în care încetează contractul de muncă;
3. restricții privind comportamentul persoanei în cazul încetării contractului de muncă, îndeosebi pe linia nedezvăluirii informațiilor speciale competitorilor actualei firme, respectându-se așa-zisa „clauză a confidențialității”;
4. aducerea la cunoștință a documentațiilor de specialitate, a documentelor, a situațiilor de întocmit, care trebuie să aibă aprobarea în avans a șefului său.

Angajatul trebuie să semneze contractul, ceea ce înseamnă că l-a citit, l-a înțeles, inclusiv că a luat cunoștință de problemele securității sistemului. După acest moment, de regulă, urmează o perioadă de probă, de până la trei-șase luni, după care se va face pronunțarea privind statutul definitiv al persoanei.

Stadiul 5: Instruirea și conștientizarea personalului

Pentru atingerea obiectivului acestui stadiu se stabilesc programe speciale de instruire și conștientizare pentru asigurarea încrederii în personalul unității pe linia asigurării securității sistemului de prelucrare automată a datelor. În acest scop, se pot folosi numeroase modalități de ducere la îndeplinire a obiectivului: de la cursuri cu durate și termene fixe, până la pavoazări la tot pasul a interiorului unității ș.a.

Stadiul 6: Supravegherea

Unitățile mai mari au în uz sisteme programate de evaluare a performanțelor angajaților, astfel încât să-i poată orienta profesional cât mai corect și pentru a face promovările cele mai motivate. Tot printr-un astfel de sistem se va efectua și urmărirea aspectelor referitoare la

încrederea în persoane și poziția lor față de securitatea sistemului, evitându-se incidentele nefericite din sistemele de prelucrare automată a datelor.

Cu caracter neplanificat sunt urmărirea și supravegherile zilnice ale personalului, pentru descoperirea potențialelor pericole din partea salariaților.

În caz de promovare, se vor face reevaluări ale sarcinilor pe linia securității informațiilor.

Programul de educație privind securitatea își propune să contribuie la creșterea vigilenței personalului și să declare orice vede ca fiind împotriva securității firmei, indiferent de poziția persoanei implicate în așa-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 condiții, un rol esențial revenind acordurilor dintre părți în regim post-angajare a persoanei, îndeosebi raportul fostului angajat cu concurenții firmei.

După recuperarea cheilor de acces urmează anularea parolelor de intrare în sistemele de prelucrare automată a datelor. În același timp, restul angajaților trebuie să fie anunțați că persoana respectivă nu mai are statutul de salariat al firmei, deci relațiile 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: Considerații finale

1. *Contractul angajaților.* Nu tratați oamenii ca și cum ei au fost angajați la o companie, ci ca și când ar lucra la propria lor firmă. Acordați o atenție deosebită personalului de întreținere a sistemului, personalului care efectuează curățenia, care pătrund în centrele de prelucrare automată a datelor fără să aibă supravegheri speciale. Identic se va proceda și în cazul consultanților din afară.
2. *Operatorii de la terminale* nu trebuie să fie omiși cât de periculoși pot fi pentru sistem, îndeosebi pentru faptul că pot să-și păstreze anonimul. O grijă deosebită trebuie să se acorde și personalului care lucrează la întreținerea 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 securității sistemului, efectuându-se, chiar, verificarea lor și admiterea sau nu a pătrunderii în sistem. Se recomandă ca vizita lor să aibă loc numai însoțit de un reprezentant al firmei.
4. *„Controlul extern” asupra angajaților.* Pot fi situații când persoane care nu sunt abilitate cu cunoștințe elementare de prelucrare automată a datelor să poată fi foarte periculoase pentru securitatea sistemului, fiind ghidate de cineva din afara unității asupra modului cum trebuie să procedeze.
5. *Acțiuni hotărâte.* Dacă asupra unei persoane sunt unele dubii privind securitatea, nu trebuie lăsat timpul să-și spună cuvântul, încercând să ne convingem de realitatea bănuielilor, ci trebuie acționat dintr-o dată. Parolele de acces ale persoanelor autorizate pot fi retrase de responsabilul cu securitatea sistemului fără să-i anunțe în prealabil pe cei deposedați, bineînțeles, dacă există motive de bănuială asupra loialității.
6. *Tratamentul loial în sens descendent și ascendent (pe bază de reciprocitate).* Angajatorii trebuie să-și trateze angajații corect și onest ca să se aștepte să fie tratați 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 diferită văzută de cei de sus, de aceea ei trebuie să coboare la nivelul locurilor de execuție din ateliere. Se spune că și 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 plătești, se fac că muncesc și că sunt corecți.* Încrederea personalului poate fi câștigată prin recompensarea lor la cote ridicate, scoțându-le în relief valoarea lor și câștigându-le încrederea.
9. *Nu jucați fals.* În istoria securității sistemelor, persoanele care au oferit cele mai multe „cacealmale” angajaților au fost și cele mai des furate sau spionate.
10. *Lăsați, totuși, unele porțițe de ieșire pentru situații deosebite.* Personalul nu trebuie să se teamă atât de tare de consecințele unor încălcări, din neglijență, a măsurilor de securitate. Măsurile exagerate nu aduc întotdeauna cele mai bune rezultate. Nu puneți mare preț pe anonime, dar nici nu le neglijați.
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, totuși, pe judecată și 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 intenționează să-și găsească un loc de muncă adecvat cunoștințelor acumulate de-a lungul anilor, dar și pentru firmele interesate să găsească pe cei mai buni specialiști în securitatea sistemelor, le recomandăm să consulte două site-uri foarte cunoscute pe Internet: *dice.com* și *monster.com*.



- Dacă ați face parte dintr-o comisie de selecție a candidaților pentru un post de **director de sucursală bancară, ce elemente ați folosi în interviu** lor, în așa fel încât să angajați o persoană cât mai potrivită din punctul de vedere al securității informaționale? Dați exemple de **4 informații sensibile (confidențiale sau secrete)** cu care intră în contact un **director de sucursală bancară**, justificând motivul pentru care considerați importante respectivele informații. Menționați **2 măsuri** pe care le puteți lua pentru a vă feri de divulgarea acestor informații de către proaspătul angajat.
- Reluați exemplul de mai sus pentru un **agent de vânzare**, un **contabil șef** și 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) și a mecanismelor procedurale care concură la asigurarea securității prelucrării automate a datelor.

În SUA, Centrul de Apărare a Securității Calculatoarelor al Agenției Naționale de Securitate a emis unele recomandări astfel încât să se știe 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 securității sistemelor informatice, după ce sunt supuse unor teste speciale. Astfel, au fost definite patru clase, de la D la A, și câteva subclase, cum ar fi A1 și A2. Clasa D este cea mai de jos. În cadrul claselor, numerele mai mari sugerează un sistem mai sigur.

Clasele și subclasele stabilite sunt:

D. Nesigure sau neevaluate.

C. Capabil să asigure controlul accesului discreționar.

C1. Orice sistem de operare comercial care asigură separarea fazelor de execuție ale sistemului de cele ale utilizatorilor obișnuiți.

C2. Orice sistem de operare comercial dublat de un pachet suplimentar pentru asigurarea securității.

B. Capabil să realizeze controlul obligatoriu al accesului.

B1. Toate informațiile sunt astfel etichetate încât să corespundă unei anumite categorii de securitate.

B2. Securitatea organică. Echipamentele și softul sunt concepute și 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 și aprobate ca fiind eficiente.

A1. Verificarea proiectării. De regulă, înseamnă controlul codurilor-sursă din programele de sistem care au funcții de securitate.

A2. Verificarea implementării. În acest caz sunt examinate programele de sistem executabile și se urmărește 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 condițiile lor de execuție sau a datelor prelucrate, de a modifica statutul, actual și viitor, al celorlalți utilizatori ai programului sau de a prelua controlul asupra datelor altora, ca o excepție de la regulile normale de acces.

Pentru realizarea acestor obiective, fiecare adresă de program al utilizatorului, numele programatorului, conținutul registrelor, datele utilizatorilor trebuie să fie protejate împotriva folosirilor neautorizate, în sensul neasigurării transparenței lor atunci când altui utilizator i se va aloca același spațiu de lucru.

Pentru ca un sistem informatic să fie considerat asigurat din punctul de vedere al izolării lui, trebuie să fie îndeplinite două condiții:

1. să se folosească un anumit mod de asigurare a securității prelucrării pentru a izola sistemul de inamicii săi din afară;
2. să se apeleze la strategii de apărare, prin izolarea utilizatorilor între ei și de sistemul de operare al calculatorului. Utilizatorii care prelucrează date ce aparțin categoriilor speciale trebuie să fie izolați în mod deosebit.

Sunt posibil de aplicat cel puțin șase strategii de izolare, ele putând fi mai multe. În categoria celor șase intră:

- selectarea modului de prelucrare;
- izolarea temporară;
- izolarea spațială;
- izolarea realizată prin caracteristicile arhitecturii sistemului;
- izolarea criptografică;
- restricții 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 mulți utilizatori în același timp (în mod serial sau multiprogramare), accesul direct (on-line) sau prin programare sau neprogramare influențează, în mod vădit, gradul de izolare a sistemului.

Izolarea temporară se aplică, de regulă, în cazul prelucrărilor speciale, dar poate fi folosită și în modul multiprogramare asupra terminalelor ce intră sau ies într-o/dintr-o rețea, în funcție de un calendar, care se întocmește luând în considerare categoria datelor și principiul „trebuie să știe”.

Izolarea spațială se realizează prin dedicarea componentelor de prelucrare și izolarea lor față de un alt utilizator.

Arhitectura sistemului este cea care facilitează multiprogramarea, contribuind la izolarea utilizatorilor față de sistemul de operare și între ei înșiși, asigurându-se prelucrarea datelor secrete pe niveluri de securitate.

Izolarea criptografică este folosită, în principal, pentru realizarea izolării prelucrărilor de la distanță de intrușii din afară, atunci când liniile de comunicație depășesc perimetrul de securitate. Ea poate fi folosită, de asemenea, pentru izolarea utilizatorilor din sistem, în special atunci când aceștia au niveluri diferite de responsabilitate pe linia securității.

Restricțiile de privilegiu constituie o cale de identificare distinctă a utilizatorilor-programatori de cei neprogramatori. Eficiența 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 instanță, șeful unei companii are responsabilitatea definirii informațiilor care trebuie să se afle sub control, cine să-l efectueze, prin ce persoane și în ce condiții se atribuie drepturi speciale de control și cum pot fi ele revocate. În practică, responsabilitatea se delegă spre nivelurile inferioare, spre șefii compartimentelor și administratori.

În fiecare regulă privind accesul trebuie să se reflecte două principii esențiale:

1. *Privilegiul minim*. Numai acele informații sau operațiuni de prelucrare pe care utilizatorul trebuie să le exercite și îi revin ca sarcini de serviciu vor fi lăsate la dispoziția sa, iar ele vor fi stabilite de responsabilii de drept, și nu de utilizator.
2. *Expunerea minimă*. Din momentul în care un utilizator are acces la informații 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 cunoștință de ceea ce se prelucrează, se memorează sau se transmite în altă parte. Mai mult chiar, o atenție deosebită se va acorda restricțiilor 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 modalități de genul tabelelor de autorizare, al listelor de control al accesului, al profilurilor de securitate.

Tabelele de autorizare, numite și tabele de securitate, există în formatul cod-mașină; ele sunt componente ale sistemului de operare, alături de alte programe de control, cu rol de urmărire a bunei funcționări a sistemului. Importanța lor rezidă și în faptul că au un nivel de protecție similar celor mai bine protejate programe de control.

Tabelele de autorizare se află sub directă preocupare a unor veritabili specialiști, 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 și 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 și pentru fiecare fișier de date. Ele trebuie să conțină:

- 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;
- condițiile în care se garantează accesul.

Profilurile de securitate trebuie să fie în atenția 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 responsabilitățile pe linie de securitate a sistemului;
4. identificarea tuturor fișierelor la care utilizatorul poate să aibă acces și ce anume poate să efectueze asupra lor.

Noțiunile de „proiect” și „categorie” din enunțurile de mai sus au același statut ca și utilizatorii și, deci, trebuie să aibă și ele profilul lor.

De fiecare dată când un utilizator intră în contact cu calculatorul de la un terminal conversațional sau printr-un lot de lucrări, operațiunea de certificare a identității se impune cu acuitate. Informația necesară identificării este parola.

Parolele sunt folosite pentru a permite accesul în sistemele de calcul, la fișierele și bazele de date ale acestuia. N-ar fi exclus ca ele să fie folosite în viitor și pentru accesarea înregistrărilor sau câmpurilor acestora, cu condiția de a fi eficiente și ieftine. Parolele trebuie să fie asociate cu utilizatorii, proiectele și categoriile de informații.

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 condiționare a accesului local sau de la distanță, precum și a celui intern (memorie primară, memorie virtuală, memorie secundară și suporturi externe).

De o importanță deosebită, după ce s-a autorizat accesul, este obținerea unui privilegiu de acces, prin intermediul codurilor speciale, consemnate în tabelele de autorizare.

6.5.3 Detectia amenințărilor și supravegherea sistemului

Deși pare nepotrivită, dar nu lipsită de adevăr, afirmația că fraudele din mediile informatizate ar putea fi detectate este destul de riscantă. Ca argumente sunt aduse preocupările de urmărire cu atenție a amenințărilor sistemului, analiza anumitor tendințe, cercetarea incidentelor înregistrate și auditarea.

6.5.3.1 Urmărirea amenințărilor

Toate sistemele trebuie să dispună de capacitatea de înregistrare a tentativelor de atac, într-un format intern, să le supună, apoi, unor examinări riguroase și să reconstituie informațiile principale pe baza a ceea ce s-a înregistrat în format-mașină. Cât timp este destul de greu de spus ce înseamnă amenințare și ce nu, toate operațiunile care ar putea afecta securitatea sistemului trebuie să fie înregistrate, inclusiv intrările în sesiunile de lucru, solicitările de fișiere și tranzacțiile de la terminale.

Când operațiunile principale referitoare la securitatea sistemului sunt înregistrate automat de către sistemele de prelucrare automată a datelor, registrul trebuie să fie protejat împotriva intervenției 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 directă supraveghere a responsabilului cu securitatea sistemului.

Referitor la recunoașterea potențialelor amenințări, un bun sistem trebuie să fie capabil să depisteze următoarele șase condiții:

1. terminarea anormală a unor lucrări;
2. o cădere anormală a sistemului;
3. defectarea mecanismului de asigurare a securității echipamentelor și softului;
4. tentativele de intrare în dialog cu sistemul, dar care nu sunt încununate de succes;
5. tentativele de obținere a accesului neautorizat la fișierele ce conțin date speciale;
6. tentativele de utilizare neadecvată a unor instrucțiuni sau seturi de instrucțiuni privilegiate.

Atunci când sistemul recunoaște că sunt îndeplinite condițiile de depășire a securității lui, el trebuie să fie capabil să identifice terminalul de la care se înregistrează tentativa de furt și categoria infracțiunii. De asemenea, va trebui să furnizeze identitatea utilizatorului care încearcă

să violeze sistemul de securitate, data și ora evenimentului, precum și ce fișier a fost ținta atacului.

De regulă, sunt monitorizate zece tipuri de violări ale sistemului de securitate:

1. a treia tentativă eșuată de deschidere a sesiunii de lucru a sistemului;
2. un răspuns eronat la cererea de reautentificare a utilizatorului;
3. folosirea greșită a unor instrucțiuni privilegiate;
4. tentativa de depășire a spațiului de memorie alocat utilizatorului ce a deschis sesiunea de lucru;
5. tentativa de folosire neautorizată a fișierelor cu date secrete;
6. defectarea oricărui mecanism de protecție;
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. aceeași incapacitate de a verifica tabelele de securitate ale sistemului;
10. tentativa eșuată 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 intruși, ceea ce ar însemna state de plată false, parole false și altele care să-i tenteze pe atacatori.

În același timp, din partea sistemului vor fi extrase cât mai variate tentative de înșelare a sistemului de securitate, apelându-se la echipe speciale, numite „echipe de tigri”. Oricum și acestea vor fi urmărite îndeaproape, întrucât fără să se simtă supravegheate pot fi tentate să săvârșească acte ilegale.

6.5.3.2 Analiza tendințelor

A căuta ceva ce nu este într-un loc, deși ar trebui să fie sau ceva ce este și n-ar trebui, presupune folosirea instrumentelor statistice în cazurile suspecte.

Parametrii statistici principali sunt media sau valoarea așteptată (scontată) a timpului scurs între incidente sau a capacității de utilizare a resurselor și deviația standard a oricăreia dintre mediile amintite. O informație prețioasă se obține și prin compararea mediilor în mai multe perioade de timp, dacă ele se măresc sau se micșorează ori au o comportare explicabilă în ciclu.

Datele supuse analizei pot fi obținute pe patru căi:

- registrele componentei de supraveghere a sistemului și 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 funcționalitatea sistemului, inclusiv cele privind defectarea hardului sau softului, precum și măsurile luate sau reparațiile efectuate.

În calculele de efectuat, *media* înseamnă însumarea valorilor observate și împărțirea valorii astfel obținute la numărul valorilor observate.

Deviația standard este rădăcina pătrată a sumei diferențelor la pătrat dintre medie și fiecare valoare observată, de împărțit la numărul valorilor observate minus unu.

Prin instrumentele statistice amintite pot fi descoperite cinci clase de deviații relevante de la securitatea sistemului, după cum urmează:

1. pentru activitatea sistemului ca un tot;
2. activitățile utilizatorilor;
3. activitatea unor terminale anume;
4. operațiunile cu fișierele ce conțin date secrete;
5. operațiuni care implică utilizarea programelor cu regim special.

Prin reprezentarea grafică a valorilor obținute se pot constata discrepanțe relevante privind:

1. timpul dintre două reparații ale sistemului;

2. timpul dintre două încercări eșuate de intrare în sistem;
3. timpul dintre întreruperi;
4. timpul scurs între erorile de comunicație;
5. folosirea timpului de prelucrare, măsurat în secunde, de înmulțit cu miile de cuvinte ce au fost folosite (kilo-cuvinte);
6. timpul de conectare pe lucrare ș.a.

Există sisteme capabile să-și 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 securității sistemului.

Relevant este și numărul de lucrări abandonate într-o perioadă de timp, ceea ce ar scoate în evidență fie proasta funcționare a sistemului de operare, fie o greșită utilizare a lui în intenția de a avea acces la fișierele secrete ale firmelor.

Pentru o ușoară controlabilitate a sistemului se recomandă constituirea unor așa-zise profiluri ale violatorilor sistemului. Ele sunt realizate pe utilizatori, tipuri de utilizatori (ocazionali, moderați, puternici) și lucrările foarte importante din sistem.

Profilul unui singur utilizator rezidă în evidențierea unor aspecte ce pot să conducă la ușoara descoperire a vinovatului. Ele se referă la înregistrarea codului de identificare a utilizatorului și tipul lui; numărul și tipul actelor violente; identificarea fișierelor urmărite prin actele de violență.

Tipurile utilizatorilor trebuie surprinse prin profiluri distincte, întrucât posibilitățile de a greși sunt direct proporționale 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 muncește nu greșește, deci dacă se înregistrează mai multe greșeli la un utilizator deosebit al sistemului acesta ar fi un lucru normal. Din cauza necesităților de efectuare a unor analize complexe, utilizatorii vor fi grupați pe tipuri, știindu-se cam câți aparțin fiecărui tip, iar violarea sistemului va fi urmărită prin numărul și tipul lor, precum și atacurile la securitate pe fiecare utilizator.

Este de reținut 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 eșecului. Și în acest caz, dacă se știe 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 intrușii consideră că acesta ar fi momentul propice să încerce vigilența sistemului.

Profilurile lucrărilor vor fi consemnate într-un registru special, în care se vor înregistra:

1. identificatorul utilizatorului: pentru a se putea stabili responsabilitățile;
2. kilo-cuvintele-secundă esențiale: pentru a se putea observa dacă s-au introdus coduri neautorizate;
3. timpul de execuție: pentru a ne asigura că nu au fost efectuate lucrări neautorizate;
4. numele programelor apelate: pentru a se cunoaște dacă s-au apelat numai procedurile permise și nici o altă acțiune n-a avut loc;
5. fișierele de date create și accesate, precum și numărul de citiri, scrieri sau adăugări la sfârșit în fiecare fișier: se va urmări dacă s-au accesat fișiere secrete;
6. ieșirile obținute: pentru a ne asigura că nu s-au copiat sau listat cantități mari de date din fișierele secrete.

6.5.3.3 Investigarea

Cazurile anormale care pot fi supuse investigării le cuprind pe cele de excepție, considerate ca ieșite din comun față de tendința statistică a lor. Atât numărul prea mare de violări ale sistemului, cât și cel prea mic trebuie să fie supuse investigării. În primul caz fiind semne de prea

multe tentative eșuate de depășire a sistemului de protecție, în al doilea s-ar putea trage concluzia depășirii profesioniștilor 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 informațiilor speciale ale unității;
2. pierderea sau incapacitatea de a evidenția corect orice valoare patrimonială;
3. intervenția inexplicabilă a operatorului în execuția lucrărilor;
4. prezența sau suspiciunea prezenței în sistem a unui intrus;
5. absența inexplicabilă a persoanelor cu drept de acces la informațiile speciale;
6. apariția unor nume-capcană într-o listă de persoane;
7. creșterea inexplicabilă a gradului de utilizare a sistemului, îndeosebi după program sau în regimul normal de lucru, de către utilizatori sporadici sau de la terminale inactivate o lungă perioadă de timp;
8. tentative de accesare sau solicitare a înregistrărilor, fișierelor capcană sau de folosire a parolilor expirate;
9. pierderea sau folosirea neautorizată a identificatorilor utilizatorilor, a sistemului de control al accesului sau a elementelor de recunoaștere 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 greșită a adreselor, de apariție 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 ș.a.;
13. diminuarea inexplicabilă a nivelului stocurilor;
14. creșterea inexplicabilă a frecvenței tentativelor eronate de obținere 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. apariția 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 fișierele speciale sau creșterea surprinzătoare a gradului de utilizare a unor fișiere sau conturi inactivate o lungă perioadă de timp;
20. creșterea surprinzătoare a incidentelor produse de defectarea echipamentelor, softului sau de terminarea anormală a lucrărilor, a reluărilor exagerate de execuții de programe, a restaurărilor multiple ș.a.

În plus, responsabilul cu securitatea sistemului poate să ceară informații suplimentare de la operatorii calculatoarelor, de genul:

- numele fișierelor și subrutinelor accesate de un program dat;
- lista numelor de constante și variabile ale programelor;
- datele ce ocupă spațiul memoriei primare selectate;
- listele utilizatorilor de programe și a fișierelor de date;
- exemplarele ce conțin mesaje de eroare;
- imaginea înregistrărilor bazelor de date înainte și după actualizarea lor;
- lista suspendărilor din prelucrare (erori) a unor operațiuni ce nu pot fi prelucrate pentru efectuarea actualizărilor fișierelor nomenclator;
- modificări ale bazelor de date declanșate de la un terminal conversațional;
- schimbarea locului adresei utilizatorului după ce s-au încălcat regulile de securitate;
- lista de control a comenzilor folosite în timpul execuției unei lucrări.

6.5.3.4 Aspecte generale privind controlul și auditarea sistemelor informatice

Responsabilul cu securitatea sistemului trebuie să prevadă și să construiască probe pentru auditarea sistemului pentru fiecare incident încadrat în una din următoarele categorii:

1. evidența tuturor vizitelor centrului de prelucrare automată a datelor de către persoane din afara sistemului;
2. istoricul tuturor elementelor privind controlul accesului în sistem;
3. evidența tuturor persoanelor ce activează în centrul de prelucrare automată a datelor, de la angajare până în prezent, cu drepturile avute, retrase ș.a.;
4. cronologia experiențelor deosebite ale personalului în ultimul an, îndeosebi pe linia a ceea ce a putut vedea, mânuși sau a supravegheat activitatea de contabilizare a operațiunilor informatice;
5. descrierea cronologică a tuturor incidentelor privind actele contabile;
6. păstrarea tranzacțiilor pe ultimii cinci ani despre orice persoană care a participat la derularea lor;
7. istoricul operațiunilor privind negocierile, din faza anterioară și următoare acestora, dacă valoarea este mai mare decât o valoare dată (100 dolari);
8. istoricul evoluției oricărui program al sistemului de operare, de la implementarea lui până în prezent, cu consemnarea tuturor modificărilor prin care a trecut;
9. verificarea concordanței tuturor tranzacțiilor cu orice înregistrare dintr-o serie de trei generații de fișiere (bunic, tată, fiu), în format intern;
10. istoricul evoluției oricărui program de aplicații cu rol special în sistem, de la implementare până în prezent, dar consemnând și modificările, modul de utilizare, de întreținere;
11. o listă cronologică a tuturor incidentelor în ceea ce privește violarea protecției sistemului;
12. o listă cronologică a tuturor dificultăților întâmpinate în timpul investigării oricărui atac al securității sistemului.

6.5.3.5 Acțiunile de răspuns

Toate sistemele trebuie să se bazeze pe existența unei persoane cu autorizare specială care să poată declanșa acțiuni reparatorii sau de anihilare a tentativelor de violare a sistemului. De regulă, astfel de acțiuni se numesc acțiuni de răspuns și pot fi încadrate în două categorii: acțiuni imediate și acțiuni retroactive.

Acțiunile imediate. Îndată ce responsabilul cu securitatea sistemului sau o persoană autorizată să presteze o astfel de activitate constată apariția unui atac al securității, trebuie să stopeze imediat componentele supuse acțiunii frauduloase și să rețină operațiunile ce au putut fi afectate, pentru o cercetare minuțioasă ulterioară. Imediat vor fi informate persoanele autorizate cu responsabilități pe linia securității.

Acțiunile retroactive. În cazul în care au intervenit situații clare sau numai suspiciuni de compromitere a informațiilor secrete, de pierdere a valorilor patrimoniale deosebite, de modificare a informațiilor, de folosire neautorizată a resurselor, probele reviziei și alte elemente edificatoare vor fi puse laolaltă și aduse la cunoștința celor ce răspund de securitate. Aceștia, pe baza informațiilor obținute, vor stabili amploarea pierderilor reale la nivelul firmei, persoanele cărora să li se impute valoarea pierderilor, să determine cu exactitate eficiența măsurilor de securitate, să învețe cum să fie prevenite pierderile asemănătoare în viitor, acoperirea pierderilor dacă este posibil.

Deseori se vorbește și despre efectuarea unor acțiuni speciale, care trebuie să fie declanșate când se întâlnește unul din următoarele patru tipuri de violare a securității:

1. orice îndepărtare de la regulile prescrise de deschidere a sesiunii de lucru;

2. o a treia tentativă, consecutivă, eșuată, de deschidere a sesiunii;
3. tentativa eșuată de a da răspunsul corect la acțiunea de reautentificare declanșată de sistem;
4. orice intenție a utilizatorilor de a obține accesul neautorizat la fișiere sau de a folosi instrucțiuni sau secvențe de instrucțiuni nepermise.

6.5.3.6 Infractorii tipici ai sistemelor informatice

De la început trebuie menționat că o mare parte a delincvenților își încetează misiunea prin utilizarea unor mijloace convenționale: intimidarea, anchetarea și apelarea la informatori. Cele mai importante metode de informare privind suspjecții se bazează pe supravegherea lor discretă, lucrul în comun sau asocierea. De multe ori persoanele ce se despart oferă informații prețioase despre partenerul lor de viață. Nu trebuie neglijate categoriile dintr-o unitate cărora la prima vedere nu prea li se dă prea multă importanță (curieri, personalul care se ocupă de curățenie, paznici), care, de multe ori, văd și știu foarte multe.

Deși în capitolele anterioare au fost prezentate categoriile de atacatori, în cele ce urmează se va face o scurtă descriere a patru tipuri reprezentative de delincvenți: delapidatorii, detractorii sau seducătorii, hackerii și trișorii.

Delapidatorii au devenit hoți informatizați printr-o explicație foarte simplă: înregistrările la care trebuie să ajungă și modalitățile de acoperire a faptei sunt realizabile cu ajutorul calculatorului.

De regulă, delapidatorii sunt de vârstă mijlocie, cu destulă credibilitate în firmă, câștigată, îndeosebi, printr-o prezență îndelungată în aceeași unitate. Ei sunt buni cunoscători ai măsurilor antifurt și 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 neglijați, mai ales pentru că nu ocupă o funcție mai bună în sistem.

Totul începe de la existența unor probleme personale de natură financiară, prin îmbolnăvirea unor membri ai familiei, ca urmare a unor mofturi pe care nu și le permit să și le satisfacă sau dorinței de a trăi pe picior mare. Totuși, pe ultima sută, operează bunul simț. După ce „șterpelesc” o jumătate de milion de dolari, pentru o foarte lungă perioadă de timp, se opresc.

Detractorul este un adevărat hoț informatizat și 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, locuiește într-un cartier respectabil, este căsătorit și are doi copii. S-a ocupat de „șterpeliri” timp de aproximativ 18 luni și a obținut 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 șeful echipei de programare sau de exploatare a sistemului. Motivația faptei sale poate fi una de natură egocentrică sau, în virtutea poziției 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 și 25 de ani, deși s-au descoperit și cazuri de 8 ani sau de peste 40 de ani. Este fie student, fie șomer. Are o minte sclipitoare și are soarta lupilor singuratici, fiind obsedat numai de tehnologiile de vârf, de ultimă oră. Deseori se consideră neglijat de societate, care nu-și dă seama cât de isteț este. Astfel de cazuri sunt ușor de întâlnit în mediile universitare, persoanele în cauză petrecându-și zilnic 16-18 ore în fața calculatorului sau a unui terminal, fără să mai facă nimic altceva. De cele mai multe ori sunt căzuți la examenele de matematică și 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 specialiști în domenii cheie de activitate: șefii firmelor de contabilitate, specialiști în securitatea sistemelor, ofițeri ai serviciilor secrete, oameni de afaceri cu mult succes.

Trișorul, de regulă, este femeie. De cele mai multe ori este singurul părinte al unuia sau doi copii și poate să aparțină, în mod vizibil, unor grupuri minoritare. Vârsta este între 25 și 35 de ani. Profesia este cea de responsabil introducere-date și, prin prisma acesteia, are posibilitatea să-și adauge drepturi bănești suplimentare, pe care de multe ori le împarte unor societăți caritabile. Poate să aibă și o motivație ideologică sau să acționeze sub un sindrom invers celui sub care acționa Robin Hood, luând de la bogați, dar păstrând totul pentru ea. În cele mai multe cazuri au operat pe un anumit scenariu cam doi ani și au agonisit sume ce depășesc 50000 de dolari.

Cauzele succesului unor astfel de furturi se datorează, în majoritatea lor, ineficienței controlului exercitat de către sistem, ineficienței controlului propriului personal și a unui control managerial slab.

6.5.4 Integritatea sistemelor

Integritatea sistemelor se referă, de fapt, la programe și date. Integritatea datelor este protejată prin controlul erorilor, iar a programelor, printr-un control riguros asupra tuturor activităților de programare. Un caz aparte îl poate constitui protecția programelor și funcțiilor pe linia securității.

6.5.4.1 Securitatea programelor

Controlul în detaliu al conceperii, realizării și implementării programelor calculatoarelor reprezintă problema-cheie a securității sistemului.

Conceperea programelor. Activitățile 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 șef, care are rolul de arhitect al întregii lucrări, stabilind interfețele dintre modulele programatorilor din subordine. Fiecare dintre ei răspunde de o componentă bine definită din program. Toți programatorii, inclusiv șeful, transmit ceea ce au făcut unui secretar de proiect, care colectează documentația și urmărește 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 și 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 ș.a.).

Înainte de compilarea programului trebuie să se verifice dacă există erori de logică, operațiune executată de două persoane foarte pricepute în programare. Se poate apela și la folosirea calculatoarelor pentru efectuarea acestor activități.

Realizarea programelor se înfăptuiește prin apelarea la compilatoare adecvate, în ultimul timp folosindu-se compilatoare conversaționale sau inteligente. Pentru adevărații 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 documentația programului.

Implementarea programului. În cazul îmbunătățirii unor programe deja existente, se recomandă implementarea prin funcționarea paralelă a celor două versiuni.

6.5.4.2 Protecția funcțiilor securității

Funcțiile principale de control al centrului de prelucrare automată a datelor trebuie să fie asigurate prin mecanismul de protecție. Ele, în mare parte, se referă la:

1. controlul direct al resurselor fizice (benzi, pachete de discuri, alte suporturi de date și echipamente periferice);
2. procedurile de pornire și oprire a sistemului;

3. mecanismele de supraveghere a utilizatorilor;
4. detectarea și corectarea erorilor, precum și reluarea lucrului în condiții normale;
5. generarea, coordonarea și trimiterea secvențelor de instrucțiuni (sau prelucrări);
6. cuplarea cazurilor, în vederea prelucrării lor într-o anumită ordine;
7. identificarea și verificarea utilizatorilor;
8. controlul fluxurilor de date;
9. ștergerea datelor remanente în memoria calculatorului de la un utilizator la altul sau înaintea efectuării operațiunilor de întreținere;
10. proceduri de criptare și decriptare.

Este foarte important ca securitatea să fie întreținută tot timpul și în toate condițiile, inclusiv când apar mari încărcături de date, ceea ce ar trebui să se concretizeze într-o securitate sporită. La fel trebuie pusă problema și în cazul diminuării cantității de date prelucrate sau când apar defecțiuni la echipamente sau programe, sau când se asigură întreținerea și repararea sistemului. Măsuri speciale trebuie prevăzute și pentru cazurile provocate de intervenția voită a omului asupra securității sistemului.

Un rol deosebit revine programelor de asigurare a securității, despre care s-a discutat într-un paragraf anterior.

6.5.5 Înregistrarea activităților efectuate și a măsurilor de securitate

Este foarte important să se țină evidența înregistrărilor astfel încât principiile securității prelucrării automate a datelor să poată fi puse în practică. Jurnalele asigură o înregistrare cronologică a cazurilor pe linie de securitate. Fișierele de siguranță fac posibilă reconstituirea datelor după catastrofe sau funcționări proaste ale sistemului.

Jurnalele de bord trebuie să fie ținute la zi pentru toate activitățile ce au loc sub controlul operatorului, al ofițerului cu securitatea sistemului (dacă există), al bibliotecii de suporturi și de la punctele de prelucrare.

Controlul operatorului. În jurnalul operatorului trebuie să fie înregistrate următoarele evenimente:

1. pornirea calculatorului;
2. configurația cu care s-a început lucrul;
3. inițializarea și reinițializarea sistemului;
4. execuția testelor de rutină și a programelor de întreținere;
5. momentul de început-execuție programe sau de serie de programe înlănțuite;
6. finalizarea normală sau anormală a lucrărilor;
7. disfuncționalități ale softului de sistem sau proasta funcționare a echipamentului;
8. oprirea normală sau anormală a calculatorului;
9. timpii de prelucrare pierduți;
10. mesajele de eroare afișate de calculator;
11. interogări anormale ale fișierelor cu date secrete;
12. montarea suporturilor detașabile;
13. intervenția operatorului în programele utilizatorilor sau suprascrierea de către operator a unor funcții de protecție;
14. responsabilitățile operatorului în regim activ sau inactiv;
15. prezența vizitatorilor în sala calculatorului.

Jurnalele punctelor de prelucrare și ale operațiunilor de intrare-ieșire. În continuare se va prezenta o listă a activităților 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 funcționarea sistemului;
4. momentul de lansare în execuție a lucrărilor;
5. momentul opririi execuției lucrărilor;
6. linia-destinație;
7. terminalul-destinație;
8. rutinele de comunicație;
9. calculatoarele și sistemele de operare folosite pentru execuția lucrărilor;
10. programele și subrutinele apelate și condițiile de securitate pe care le solicită;
11. fișierele de date accesate și nivelurile lor de securitate;
12. identificarea unică a lucrărilor din noianul de lucrări ale zilei sau din sistemul de clasificare pe linia securității;
13. identificarea fișierelor de date sau a programelor create sau distruse în cursul execuției unei lucrări, condițiile de securitate și mărimea lor.

Jurnalele bibliotecilor de suporturi. Bibliotecarul de suporturi trebuie să vadă data, timpul și circumstanțele în care a apărut unul din următoarele evenimente:

1. achiziția de materiale în bibliotecă;
2. ștergerea sau distrugerea suporturilor de prelucrare automată a datelor și a documentației;
3. înlocuirea documentației sau a suporturilor de date;
4. scoaterea din locul de păstrare sau arhivare a suporturilor sau documentațiilor;
5. scoaterea din bibliotecă a unor obiecte și data aducerii lor înapoi;
6. schimbări ale proprietății asupra elementelor de prelucrare automată a datelor sau documentației;
7. schimbarea încadrărilor pe linia securității suporturilor din bibliotecă sau a documentației.

Jurnalele ofițerului cu securitatea. Ofițerul 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 săvârșesc erori;
2. identificarea terminalului la care s-a înregistrat infracțiunea;
3. tipul de violare a securității;
4. data și timpul incidentului;
5. identificarea și încadrarea în nivelul de securitate adecvat a tuturor programelor speciale sau fișierelor de date expuse pericolelor externe.

Pentru a asigura securitatea sistemelor de prelucrare automată a datelor, echipamentele și programele de control trebuie să se afle în deplină siguranță, numai în acest mod putându-se continua serviciile, care sunt de cea mai mare importanță în existența sistemului. Se știe că șansele de reușită ale furturilor sau compromiterii datelor sunt deosebit de favorabile atunci când personalul de prelucrare automată a datelor este preocupat de repunerea în funcțiune a echipamentelor și programelor. Problema tinde să devină deosebit de gravă atunci când se referă la mecanismele de protecție. Uneori rezolvarea cazurilor de defectare a echipamentelor sau programelor presupune apelarea la specialiști din afară, care nu au responsabilități pe această linie, ceea ce nu este un lucru bun. În fine, trebuie să existe copii de siguranță care să fie folosite în momentul apariției unor defecțiuni la fișierele în lucru. Totul trebuie să se desfășoare astfel încât să nu ducă la oprirea sistemului.

Așadar, siguranța întregului sistem se realizează prin asigurarea funcționării normale a echipamentelor, softului și existența copiilor de siguranță. Despre toate s-a discutat în paragrafele anterioare.



- Extrageți 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 Securității Calculatoarelor al Agenției Naționale de Securitate. Aplicați factorii pe un sistem informatic dintr-o firmă cunoscută de dumneavoastră.
- Imaginați un alt profil de infractor al sistemelor informatice decât cele din subcapitolul 6.5.3.6.

6.6 Măsuri administrative pe linia securității sistemelor

Problemele referitoare la atribuirea responsabilităților pe linia prelucrării automate a datelor revin conducerii la vârf. Punerea în practică a principiilor securității sistemelor este diferită pentru sectorul public față 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 securității datelor, operațiune realizată de ofițerul responsabil cu informațiile, situat deasupra nivelului la care se efectuează prelucrarea. El are responsabilitatea securității 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 informaționale. 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 ține de componentele acestuia. Pentru rețele există un alt responsabil cu interconectarea datelor de la terminale la calculatorul central. La rândul lor, terminalele sunt supravegheate de un alt ofițer. De asemenea, pot fi unul sau mai mulți ofițeri responsabili cu aplicațiile bazate pe procesare de texte și alte tipuri de aplicații.

Actele normative pe linia securității sistemelor de prelucrare automată a datelor sunt promulgate de către Departamentul Apărării și de alte trei componente:

- Centrul de Securitate a Sistemelor de Prelucrare Automată a Datelor ale Apărării din Agenția Securității Naționale;
- Biroul Management și Bugete stabilește regulamentele departamentelor civile, în special pe linia analizei riscurilor;
- Biroul Național de Standarde emite o serie de standarde federale ale prelucrării informațiilor.

În mod normal, fiecare departament dispune de un responsabil cu securitatea sistemelor informaționale, excepție făcând locurile în care se pune problema gestionării fondurilor federale, situație 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 și băncile și alte instituții care intră în relații cu Trezoreria.

În Canada, de asemenea, de securitatea sistemelor de prelucrare automată a datelor pe linia apărării se ocupă Securitatea Apărării și Agenția de Informații Secrete. În sectorul civil, standardele sunt promulgate de către Consiliul Trezoreriei, cu avizul de specialitate al Comitetului de Avizare a Securității din cadrul Comitetului Interdepartamental pentru Probleme de Securitate și Informații Secrete. Urmărirea și rezolvarea problemelor securității datelor revine Poliției Călare Regale Canadiene.

În România,¹ securitatea informațiilor din domeniul public revine ca responsabilitate conducătorilor autorităților și instituțiilor publice. Coordonarea generală a activității și

¹ *** – Protecția informațiilor clasificate. Ghid practic, www.sri.ro/biblioteca_art_infclas.html

controlului măsurilor privind protecția informațiilor secrete de stat se realizează de către Serviciul Român de Informații. De asemenea, Ministerul Apărării Naționale, Ministerul de Interne, Ministerul Justiției, Serviciul Român de Informații Externe, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale stabilesc, pentru domeniile lor de activitate și responsabilitate, structuri și măsuri proprii pentru coordonarea și controlul activităților legate de protecția informațiilor secrete de stat. Alături de aceste organisme, Parlamentul, Administrația Prezidențială și Consiliul Suprem de Apărare a Țării stabilesc măsuri proprii privind protecția informațiilor secrete de stat, fiind asistate de către Serviciul Român de Informații.

Pentru implementarea măsurilor de securitate și organizarea activităților specifice protecției informațiilor clasificate, la fiecare autoritate sau instituție publică, agent economic sau orice altă organizație care, prin natura activității, gestionează informații clasificate, se va înființa o structură de securitate sau se vor desemna funcționari de securitate.

Implementarea unitară, la nivel național, a măsurilor de securitate națională clasificate, precum și a celor echivalente care fac obiectul tratatelor, înțelegerilor și acordurilor bilaterale sau multilaterale la care România este parte, este asigurată de către *Oficiul Registrului Național al Informațiilor Secrete de Stat*, înființat prin Ordonanța de Urgență nr. 153/7 noiembrie 2002. Acest organism își desfășoară activitatea de reglementare, autorizare, evidență și control în conformitate cu prevederile Legii 182/2002 privind protecția informațiilor clasificate, ale *Standardelor naționale de protecție a informațiilor clasificate în România* (Hotărârea de Guvern 585/2002) și ale normelor privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România (Hotărârea de Guvern 353/2002).²

6.6.2 Securitatea sistemelor informaționale din domeniul privat

În acest sector nu este o situație similară sectorului public, întrucât misiunea asigurării securității informațiilor revine contabilului șef și administratorului firmei. În cazul firmelor mai mici, de problema amintită se ocupă directorul general. Obiectivul, în toate cazurile, îl constituie reducerea pierderilor și îmbunătățirea mediului de lucru al firmei.

6.6.2.1 Obligațiile contabilului șef

Contabilul șef, ca responsabil al sectorului financiar-contabil, are datoria să realizeze corect auditul intern și trebuie să fie primul care să cunoască eventualele nereguli. Cât timp în multe cazuri el răspunde și de sistemul de prelucrare automată a datelor, el are decizia financiară pe linia procurării de noi echipamente și a organizării sistemelor de prelucrare automată a datelor.

6.6.2.2 Obligațiile secretariatului și oficiului juridic

În acest caz responsabilitățile nu sunt de aceeași importanță ca și cele enumerate anterior, dar ele se referă la:

- raporturile cu acționarii;
- perfectarea de contracte;
- procurarea patentelor, copyrighturilor, mărcilor de fabrică;
- asigurarea cadrului legal al desfășurării activităților comerciale;
- apărarea împotriva potențialilor inamici ai sistemului;
- păstrarea secretului informațiilor vehiculate în ședințele consiliului de administrație;
- plasarea polițelor de asigurare ale firmei.

² *** – Ordonanța de Urgență nr. 153 din 7 noiembrie 2002 privind organizarea și funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat, Monitorul Oficial nr. 826, 15 noiembrie 2002

6.6.2.3 Rolul vicepreședintelui cu probleme administrative

Atunci când există această funcție, responsabilul cu securitatea sistemului raportează către vicepreședinte, prin intermediul unor manageri numiți cu un astfel de obiectiv. Oricum, ideea de bază este că și securitatea sistemului se realizează pe mai multe niveluri, ca și conducerea firmelor.

6.6.2.4 Organizarea securității firmelor

De regulă, de problemele securității unui organism economico-social se ocupă o persoană numită, fie în mod direct, fie prin delegarea altei persoane care să aibă o poziție deosebit de bună în unitate, în primul rând să fie respectată.

Responsabilul cu securitatea va crea o adevărată infrastructură de asigurare a securității firmei, un rol important în îndeplinirea obiectivelor generale revenind nivelurilor inferioare, adică responsabililor de clădiri și locuri de muncă. Aceste ultime persoane vor fi responsabile cu asigurarea sistemelor de închidere, a containerelor, birourilor sau a altor mijloace de protecție a documentelor, asigurarea siguranței funcționării birourilor și întregii organizații, controlul traficului auto, controlul cheilor, sistemului ecusoanelor, al permiselor de intrare, biletelor de voie ș.a.

6.6.3 Responsabilități intra-organizaționale pe linia prelucrării automate a datelor

De problemele securității 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 și coordonatorul activităților de asigurare a securității. Ultimul este cel mai puternic implicat în problema de față.

În centrele mici, coordonarea tuturor activităților pe linia securității poate să-i revină directorului centrului, oficiului sau stației de calcul respective. *În cele puțin mai mari*, activitatea poate să-i revină unei persoane delegate de director. *Centrele mari* vor avea un administrator numit special pentru a exercita această funcție. *În centrele foarte mari*, coordonatorul securității poate fi ajutat de un administrator cu securitatea pentru controlarea activităților care presupun lucrul cu informații și un programator al securității sistemului pentru controlarea aspectelor tehnice ale locurilor de muncă.

6.6.3.1 Responsabilitățile directorului sistemului de prelucrare automată a datelor

Directorul centrului de prelucrare automată a datelor trebuie să observe dacă evaluarea pericolelor se efectuează periodic și 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 securității sistemelor. El va numi coordonatorul sistemului de securitate, care trebuie să fie un specialist în prelucrarea automată a datelor, cu suficiente cunoștințe despre securitatea sistemelor sau o persoană cu ample cunoștințe privind securitatea și suficient instruită în domeniul prelucrării automate a datelor. O altă preocupare a sa constă în întreținerea unor legături permanente cu alte unități ale căror date se prelucrează în sistemul lui.

În vederea asigurării securității la nivel de componente, directorul centrului numește 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 organizației;

- responsabilul cu integrarea sistemului, care răspunde de integrarea echipamentelor și softului;
- șeful echipei de programare a sistemului, responsabil pentru funcționarea sistemului, cu sarcini cum ar fi achiziția de noi programe pentru asigurarea funcționării corecte a acestuia;
- șeful exploatării răspunde de activitatea propriu-zisă de prelucrare automată a datelor;
- șeful controlului de calitate răspunde de calitatea prelucrării automate a datelor și a rezultatelor prelucrării;
- șeful echipei de pregătire date răspunde de pregătirea și verificarea datelor de intrare.

Fiecare responsabil, dintre cei enunțați anterior, va trebui să-și actualizeze documentația prin care consemnează procedurile necesare atingerii obiectivelor securității. Ei trebuie să-și întemeieze activitățile pe următoarele lucrări:

- consemnarea cu rol statistic a tuturor activităților de prelucrare automată a datelor, pentru detectarea excepțiilor de la regulă;
- registre/jurnale care să consemneze toate acțiunile de întreprins pentru asigurarea securității;
- descrierea tuturor evenimentelor deosebite privind securitatea;
- rezultatele la care s-a ajuns prin cercetarea cazurilor de violare a securității.

6.6.3.2 Obligațiile responsabilului cu securitatea

Coordonatorul securității este persoana de bază în domeniul securității prelucrării automate a datelor și are cel puțin șase responsabilități:

- evaluarea amenințărilor potențiale ale sistemului;
- procedurile de realizare a securității;
- contramăsuri la eventualele pericole;
- planificarea realizării copiilor de siguranță și a reconstituirii datelor pierdute;
- prevenirea incidentelor;
- instruire de specialitate.

La baza oricărei evaluări a amenințărilor care planează asupra sistemului stau identificarea și evaluarea elementelor patrimoniale, subiecte ale amenințărilor (echipamente, programe, date, documentație, furnituri de birou ș.a.).

Problema-cheie pentru asigurarea eficienței măsurilor de precauție pe linia securității constă în identificarea, prin nume, a persoanelor responsabile direct pentru fiecare element patrimonial. Ele se numesc și *persoane responsabile*, obligațiile lor fiind de a evidenția absolut toate operațiunile efectuate asupra elementelor de care răspund.

6.6.3.3 Controlul accesului la elementele patrimoniale

Pasul următor în programul de asigurare a securității constă în exercitarea controlului accesului la fiecare element patrimonial. Coordonatorul securității sistemului trebuie să-și țină la zi evidența privind:

- lista persoanelor ce dețin permise de intrare, legitimații sau ecusoane speciale;
- listele de control al cheilor, cartelelor și altor elemente de acces în unitate;
- lista parolelor, cifrurilor de intrare, codurilor secrete și a cunoscătorilor acestora;
- numele uzual, de lucru, al echipamentelor sistemului;
- numele unice ale fișierelor și ale persoanelor care le pot accesa și modifica;
- numele unice ale programelor și ale persoanelor care le pot lansa în execuție și modifica;
- profilurile utilizatorilor sistemului, cum ar fi: ce i se permite utilizatorului să facă cu fișierele și programele la care are acces;

- numele proiectului și al programatorilor lui;
- urmărirea continuă a documentelor de control al locurilor în care sunt păstrate informațiile confidențiale sau speciale ale unității;
- regulile interne referitoare la modul în care sunt păzite toate elementele patrimoniale importante.

6.6.3.4 Urmărirea respectării măsurilor de securitate

Cel puțin o dată pe săptămână, coordonatorul securității trebuie să viziteze centrul de prelucrare automată a datelor, pentru a verifica în ce mod se achită de obligații persoanele responsabile.

Cel puțin o dată pe lună, coordonatorul securității sistemului va face revizia documentației întocmite de persoanele responsabile cu asigurarea securității elementelor patrimoniale pe care le au în grijă.

Cel puțin o dată pe an, tot el, va solicita efectuarea reviziei interne a eficienței procedurilor și practicilor de securitate.

Oricând, coordonatorul securității sistemului poate propune directorului centrului să ia măsuri de prevenire a amenințărilor securității, iar acesta va include o apreciere a eficienței măsurilor pe timpul funcționării normale a sistemului, în perioadele de pauză, la inițializarea lui, la căderea lui, precum și în timpul întreținerii echipamentelor și programelor.

O atenție deosebită va fi acordată copiilor de siguranță și acțiunilor de reconstituire în caz de avarie, în toate variantele posibile ale ivirii ei. Cel puțin o dată la trei luni, coordonatorul securității va inspecta locurile în care sunt păstrate suporturile de memorie externă. De cel puțin 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 siguranță, fără să pericliteze securitatea sistemului.

La rândul lui, coordonatorul securității raportează, în detaliu, cel puțin o dată pe lună sau ori de câte ori este nevoie, către directorul centrului de prelucrare automată a datelor, absolut toate problemele pe linia securității sistemului. Raportul poate să conțină și propuneri de luare a unor măsuri suplimentare de prevenire a incidentelor.

De asemenea, coordonatorul securității sistemului este responsabil și de realizarea unor programe speciale de instruire, preocupându-se de procurarea materialelor din reviste sau alte publicații care abordează astfel de probleme. El va participa și la întâlniri cu alți specialiști din domeniu.

6.6.3.5 Principii administrative privind responsabilitățile de securitate

Pe linia securității sistemelor de prelucrare automată a datelor, în ceea ce privește componenta administrativă a personalului, există trei principii:

- principiul „niciodată singur”
- principiul exercitării limitate a unei funcții
- principiul delimitării obligațiilor de serviciu.

Principiul „niciodată singur”

În măsura în care resursele de personal ale centrului o permit și sunt în total acord cu studiile de evaluare a amenințărilor 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 acțiunilor-cheie pe linia securității și vor consemna, prin semnătură, într-un registru special, tot ceea ce se referă la:

1. eliberarea și restituirea elementelor de control al accesului sau o împuternicire a exercitării acestei activități;
2. eliberarea și restituirea suporturilor de prelucrare automată a datelor;
3. inițializarea și oprirea sistemului;
4. prelucrarea informațiilor deosebit de importante;
5. întreținerea echipamentelor și programelor;
6. testarea și acceptarea hardului;
7. modificarea hardului;
8. reconfigurarea permanentă a sistemului;
9. proiectarea și implementarea bazelor de date;
10. proiectarea, implementarea și modificarea sistemului de operare;
11. proiectarea, implementarea și modificarea programelor de aplicații;
12. proiectarea, implementarea și modificarea softului de securitate;
13. modificarea documentației;
14. modificarea planurilor privind cazurile de avarie;
15. declararea stărilor de avarie;
16. distrugerea sau ștergerea programelor sau a datelor importante;
17. reproducerea informațiilor foarte importante;
18. schimbarea procedurilor de exploatare a sistemelor de prelucrare automată a datelor;
19. recepția, eliberarea și transportul materialelor deosebit de importante.

Principiul exercitării limitate a funcției

Acest principiu prevede ca nici o persoană să nu fie lăsată în pozițiile cheie pe linia securității datelor un timp prea îndelungat, astfel încât să înceapă a crede că sarcina ce-i revine îi aparține în exclusivitate sau că puterile sale sunt veșnice.

Principiul separării obligațiilor de serviciu

Principiul de față este cel mai important. El constă în respectarea cu strictețe a regulii ca nici o persoană să nu aibă cunoștință despre funcțiile privind securitatea sistemului, să nu fie expusă la astfel de probleme și nici să nu participe la acțiuni pe această temă dacă acestea nu intră în responsabilitatea ei.

Există zece perechi de funcții 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 și programarea calculatorului;
2. pregătirea datelor și prelucrarea lor;
3. prelucrarea datelor și controlul calității prelucrării;
4. operarea la calculator și gestiunea suporturilor de memorare;
5. recepția materialelor importante și transmiterea lor;
6. reproducerea, eliberarea sau distrugerea informațiilor importante și autorizarea înfăptuirii acestora;
7. scrierea programelor de aplicații și a programelor de sistem;
8. scrierea programelor de aplicații și administrarea bazei de date;
9. proiectarea, implementarea și modificarea softului privind securitatea sistemului și exercitarea oricărei alte funcții;
10. controlul împuternicirilor de acces și exercitarea oricărei alte funcții.

Principiul separării obligațiilor de serviciu poate fi realizat pe două căi:

- prin ridicarea unor bariere fizice;
- prin instituirea unui sistem de norme interne.

Există șase *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 restricții, chiar și pentru operatorii de serviciu și personalul cu întreținerea, și se impune supravegherea activității lor;
6. materialele aruncate, care conțin informații importante, trebuie să fie depozitate într-un loc aflat în siguranță, departe de sala calculatorului.

Normele interne au caracter administrativ și se referă la:

- interdicția operatorilor calculatoarelor de a lucra și cu alte echipamente de prelucrare automată a datelor;
- operatorii nu trebuie să întocmească și nici să modifice programe;
- implementarea și păstrarea rezultatelor pe linia securității trebuie să fie activități distincte;
- controlul calității și auditarea trebuie să fie funcții separate și distincte de cele de prelucrare propriu-zisă.



- Extrageți din două fișe ale posturilor dintr-o organizație atribuțiile de securitate informațională.
- Arătați cum se aplică într-o organizație principiile administrative privind responsabilitățile de securitate.

Rezumat

Securitatea sistemelor are ca obiectiv împiedicarea pătrunderii intrușilor în sistem, transmițându-le mesaje de avertizare. Dacă împiedicarea pătrunderii nu este posibil de realizat, atunci barierele trebuie să le stopeze temporar sau să le întârzie atacul, situație când se impune să opereze, în primul rând, detectarea intenției de atac sau atacul propriu-zis.

Principalele aspecte vizate de securitatea sistemelor informaționale publice și 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 și responsabilitățile aplicabile în privința securității sistemelor sunt diferite, într-o anumită măsură, în sectorul public față de cel privat.

CAPITOLUL VII

Securitatea telecomunicațiilor

În pofida căderii *dot com*-urilor, adică a companiilor ce se ocupă îndeosebi cu comerțul electronic, viitorul nu poate fi schimbat, în sensul că o astfel de formă de comerț, bazată pe tehnologii de ultimă oră, orientate spre informații și comunicații, va avea un curs firesc. Politica statelor a fost una foarte agresivă. Investițiile în tehnologii orientate spre rețele au explodat în toată lumea. Capitolul de față își propune să treacă în revistă principalele elemente legate de interceptarea comunicațiilor, de securitatea transmisiilor, radiațiilor, securitatea tehnică și a tehnologiilor mobile, dorind ca, la finalul său, să se atingă următoarele obiective:

- stăpînirea de către cititor a principalelor concepte din domeniile menționate;
- cunoașterea principalelor pericole care afectează mediile de transmisie a datelor;
- posibilitatea de a lua măsuri care să asigure securitatea transmisiilor.

7.1 Interceptarea conversațiilor

De la începutul lor, sistemele de comunicație au fost vulnerabile în fața celor puși pe furt sau distrugerii. Furtul însemna pe atunci să vorbești fără să plătești și astfel a apărut o categorie, a *phreak*-erilor, definită mult mai târziu de la apariție, într-un mod similar hackerilor, ocupați îndeosebi de „hăcuirea” calculatoarelor. O a doua etapă a fost cea declanșată de pungași, în dorința lor de a comunica între ei fără ca poliția să le intercepteze convorbirile. Într-o nouă fază, când piața telecomunicațiilor s-a liberalizat, au început atacurile companiilor împotriva clienților altor companii sau acestea au început să se lupte între ele. Aproape întotdeauna măsurile de apărare luate erau tardive, căci apărea pe piață alt sistem de atac. Ceva similar se întâmplă acum cu Internetul, numai că vitezele actuale sunt mult mai mari.

Se desprinde concluzia că majoritatea comunicațiilor sunt vulnerabile în fața intențiilor de interceptare. Facem doar mențiunea că unele interceptări sunt îndeplinite cu multă ușurință, iar altele numai cu instrumente speciale și cu resurse considerabile.

Când atacul nu afectează conținutul comunicației, 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 și de sateliți, prin pătrunderea în rețelele de calculatoare, precum și prin utilizarea altor filtre de informații. Microfoanele parabolice pot detecta conversațiile de la o distanță de peste un kilometru, iar variantele laser interceptează discuțiile purtate chiar în spatele geamurilor închise.

De regulă, este foarte greu să știi în ce loc se efectuează supravegherea comunicației. De aceea, trebuie pornit de la premiza că orice conversație care conține informații valoroase este posibil să fie urmărită de cei interesați. Pentru contracarare pot fi luate două măsuri preventive:

- a) de evitat subiectele sensibile în discuțiile telefonice sau în transmisiile fax;
- b) dacă telefonul sau faxul trebuie să fie folosite, atunci pentru informațiile speciale se recomandă criptarea.

Pentru a se evita includerea numelui organizației unde lucrăm sau chiar al nostru pe lista neagră a căutărilor de informații speciale, se recomandă ca în fazele discuțiilor telefonice sau ale textelor transmise prin fax să nu figureze anumite tipuri de informații, cum ar fi numele organizației, numele codurilor proiectelor, denumirea produselor, numele persoanelor-cheie din organizație ș.a. Pentru a-și atinge obiectivele, agențiile specializate în căutarea informațiilor 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 și industria de apărare ale SUA folosesc STU-III (*Secure Telephone Unit*) pentru comunicarea informațiilor clasificate prin telefon, sub formă criptată.

7.1.1 Telefoanele standard

Telefonul a devenit un obiect nelipsit din viața noastră. Formelor tradiționale li s-au adăugat sistemele moderne, ale telefoniei mobile, care conturează un mediu cu totul nou pentru afaceri, diferit de comerțul sau afacerile electronice, numit comerț sau afaceri mobile.

În paragraful de față ne propunem, însă, să discutăm despre telefoanele standard și rolul lor într-un sistem de prelucrare automată a datelor. Referirea la ele o vom face prin două componente esențiale:

- 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 comunicație

Primele sisteme telefonice s-au bazat pe *perechea de fire neizolate*. Tendința este ca în configurația rețelelor locale (LAN) să se utilizeze *cablul coaxial*, deși cea mai securizată și mai performantă este *fibra optică*. În schimb, ea este mai scumpă și mai pretențioasă la instalare și întreținere.

Metoda securității liniilor se referă la tot ceea ce se întâmplă între centrala companiei telefonice și calculatorul central al unității.

Când se pune problema liniilor telefonice, un aspect important îl constituie integritatea cablului. Oriunde este posibil, o linie de comunicație, care servește un centru de prelucrare automată a datelor, trebuie să fie una directă între acesta și cea mai apropiată centrală telefonică. O astfel de legătură nu va permite amatorilor de interceptări ilegale de semnale să-și atingă scopul.

Sunt, totuși, companii telefonice în care se utilizează sistemul deschiderilor multiple, cablurile fiind orientate în mai multe casete de joncțiune, amplasate în locuri mai dosnice (subsolul clădirii, holuri necirculate ș.a.) de unde terminațiile firelor disponibile pot fi folosite oricând de compania telefonică, dar, la fel de bine, ele pot fi destul de ușor deschise de cei rău intenționați pentru a se lega la liniile la care au interes.

Când în unitate se impune utilizarea conductorilor multipli, pentru a satisface nevoile funcționale ale unității de prelucrare automată a datelor, se recomandă cablurile cu cel mai mare număr de conductori pentru a face cât mai dificilă operațiunea de selecție a liniei care îi interesează pe atacatori.

Nu se admit liniile cu circuite cuplate, deși 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 și să se realizeze și așa-zisele împământări. Ultima operațiune se efectuează pentru eliminarea nedoritelor radiații. În acest scop, un cablu care efectuează legătura dintre două calculatoare trebuie să aibă împământări la fiecare 10 metri.

Există și posibilitatea apărării împotriva „ascultătorilor” de fire, prin apelarea la așa-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 funcțiune a firului-capcană sunt foarte diversificate.

7.1.1.2 Securitatea transmisiilor prin satelit

Atunci când se inițiază o convorbire telefonică sau se intenționează transmisia unui fax, nu avem idee pe ce canal de comunicație se va desfășura acțiunea declanșată 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 și de eficiența din acel moment.

Majoritatea apelurilor pe distanțe lungi sunt realizate, fie și parțial, prin unde propagate în aer – fie prin satelit, fie între releele stațiilor terestre bazate pe microunde – iar tot ceea ce se deplasează în aer poate fi interceptat.

Tehnologiile folosite pentru monitorizarea sau interceptarea comunicațiilor prin microunde și satelit păreau complicate și necesitau imense investiții guvernamentale, însă în prezent grupurile sau persoanele ce dispun de resurse financiare rezonabile au la dispoziție 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 stație de comutare de lungă distanță. 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 stație terestră, de unde este transmis către un satelit și apoi plasat pe o stație terestră. De aici apelul merge printr-o linie terestră sau prin microunde terestre către o stație de comutare, unde are loc desprinderea de alte semnale și 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 fracțiune de secundă. Tot mai mulți sateliți sunt plasați pe orbită pentru a face față cererii crescânde de telecomunicații. Legătura satelitului cu pământul este ușor interceptată, căci nu se realizează printr-un fascicul îngust, ci printr-un semnal de microundă care se dispersează în mai multe direcții. Cu cât este mai sus satelitul, cu atât este mai extinsă aria terestră pe care se poate recepționa mesajul, deci și interceptat. Din multitudinea de sateliți, „urma” satelitului sau zona în care semnalele acestuia pot fi recepționate pe pământ înseamnă câteva mii de mile diametru. „Urma” poate fi îngustată prin coborârea orbitei satelitului sau mărirea dimensiunilor antenei-satelit, deși recepția se va efectua încă pe o zonă destul de extinsă.

Oricine posedă o antenă-satelit și ceva echipamente specializate, și se plasează în zona în care se află „urma” unui satelit, poate intercepta mesajul, așa cum recepționezi posturi TV. Iată de ce este atât de simplă interceptarea comunicațiilor derulate prin satelit, operațiune ce se poate înfăptui din clădirile ambasadelor, din clădirile deținute de persoane străine, de pe vapoarele ce poposesc în porturile mărilor de coastă sau de la baze străine.

În pofida legislației destul de clare privind interceptările, se înregistrează numeroase abateri. De exemplu, în SUA, legea federală interzice producerea, vânzarea, posesia și promovarea echipamentelor folosite pentru interceptări. Și, totuși, o firmă, *The Spy Factory*, cu un lanț de 12 magazine, a fost descoperită de FBI că deținea mii de microfoane minuscule, inclusiv transmițătoare ascunse în bilele minelor de pix, în calculatoare, în ștehere, în transformatoare, în casete minuscule ascunse în birouri, pe sub mese. Firma vindea echipamente de înregistrat ce se atașau direct la o linie telefonică și transmiteau comunicațiile într-un loc aflat la distanță, precum și echipamente pentru interceptarea apelurilor telefoanelor celulare. Cumpărătorii erau partenerii de afaceri suspicioși, concurenții și îndrăgostiții geloși.

7.1.1.3 Securitatea microundelor terestre

La început se credea că microundele terestre vor constitui mijlocul principal de transmitere a comunicațiilor pe distanțe lungi, ele traversând întreg teritoriul Statelor Unite ale Americii și, de aici, oriunde altundeva în lume. N-a fost să fie așa, căci majoritatea comunicațiilor pe distanțe lungi se efectuează prin satelit sau prin linii terestre de fibră optică, iar microundele terestre sunt folosite pentru traficul pe distanțe scurte sau între un oficiu telefonic și cea mai apropiată legătură cu un satelit sau linie terestră.

Transmișiile de microunde terestre se înfăptuiesc la nivelul releelor plasate la 15-20 km unele de altele, căci semnalele se transmit în linie dreaptă și nu urmează denivelările terestre. Cu cât frecvența este mai înaltă, cu atât distanța dintre relee este mai mică.

Ca și comunicațiile prin satelit, cele prin microunde terestre sunt foarte ușor de interceptat de către oricine dispune de un echipament adecvat, pentru că ele au un punct slab, exploatat de către cei rău intenționați, și 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 informații, se recomandă numai aparatura capabilă să le preîntâmpine sau să anihileze eventualele atacuri.

Sunt trei elemente cărora trebuie să li se acorde o importanță deosebită:

- soneria;
- piesele falsificate;
- piesele străine.

Soneria. Bobinele soneriilor din telefoanele obișnuite pot acționa ca dispozitive de captare și transmitere în linie, chiar și atunci când receptorul este pus în furcă. Pentru a ne asigura împotriva unei astfel de surse compromițătoare, se deconectează bobina în întregime și se înlocuiește cu o lampă ce se va cupla la un curent de 85 volți (de activare a soneriei clasice), transmis prin semnal la receptor. Dacă se dorește și un semnal sonor, se poate apela la o alarmă electronică acționată 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 și distrugere a lor, prin pulsuri de curenți distructivi.

Cele mai cunoscute sunt metodele de adăugare la *piesele* existente a unora *cu rol special, de captare și emisie*. Ele se pot descoperi printr-o analiză atentă a componentelor telefonului.

Tot în cazul telefoanelor se discută și despre așa-zisul *sistem muzicuță*, numit astfel deoarece se apelează la componente speciale, sub variate forme, care servesc drept aparate de ascultat în clandestinitate, în timp ce aparatul este așezat în furcă, dar operațiunea are loc nu în sistem continuu, ci sub controlul de la distanță al interceptorului neautorizat de semnale. O astfel de „muzicuță” 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. „Muzicuța” poate să dispună și 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 „muzicuță” este realizată din mai multe componente electronice, pentru cei avizați este relativ simplu de sesizat prezența lor în aparatul telefonic, dar pentru marea majoritate a utilizatorilor de telefoane ele rămân piese „veritabile” ale telefonului. Analistii de linie, la rândul lor, dispun de tehnici speciale de depistare a unor astfel de intruși.

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 și ar putea prezenta interes și pentru alții.

Pentru asigurarea unui control riguros asupra propriului personal, se recomandă apelarea la aparatură care să înregistreze data, ora și destinația apelului telefonic pornit din centrul de prelucrare automată a datelor. Nu este considerată exagerată măsura ținerii sub lacăt a aparaturii telefonice, mai ales acum, când prin e-mail se poate ieși cu ușurință ... în lume.

De asemenea, se poate ține legătura sistematic cu personalul specializat în telefonie pentru a afla cât de sigur este sistemul utilizat pentru prelucrarea datelor, dar și cât de vulnerabil este în fața potențialilor atacatori.

Pentru un plus de precauție, 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 susținută și de alte cinci argumente, după cum urmează:

1. asigurarea înregistrării complete a activităților prilejuite de stingerea incendiilor sau de alte dezastre ale naturii;
2. înregistrarea potențialelor amenințări cu bombe sau alte forme de atacare în forță a sistemului;
3. ținerea evidenței sesiunilor de teleprelucrare pentru a înlesni obținerea copiilor de siguranță și restaurarea fișierelor în cazul pierderii formei lor originale;
4. constituirea de probe în cazul utilizării neautorizate a componentelor de teleprelucrare;
5. obținerea probelor împotriva angajaților care săvârșesc acte de fraudă la adresa unității.

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, totuși, întrebarea: cum aflăm că suntem „ascultați”? Un bun „ascultător” nu face zgomot în timpul misiunii și transmite curenți foarte slabi sau, uneori, aceștia nici nu există. În concluzie, ascultarea liniei, cu scop de verificare, este fără prea mari șanse de reușită. Chiar și 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 și la înregistrarea sunetelor foarte fine produse de aparatele ce efectuează înregistrări ilegale, fie și pentru perioade foarte scurte de timp. Înregistrarea pe banda de control se va lansa prin intermediul unui comutator automat, declanșat de zgomotele sesizate în linie.

Absența tonului din aparatul telefonic este un semn de ascultare, dar profesioniștii 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, deși se știe că în realitate n-a fost așa.

O măsură de apărare împotriva ascultărilor neautorizate, chiar și când telefonul este în furcă, o constituie crearea unor sunete electrice înalte în locurile în care bănuim că intrușii ar fi interesați 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. Și multiplexoarele diminuează șansele intrușilor din liniile de comunicații.

Nu trebuie să încheiem succinta abordare a problemei de față fără să amintim de particularitățile rețelilor de transmisie a datelor și de multitudinea aspectelor specifice transmiterii de date prin radio.

7.1.2 Securitatea celularelor

Un telefon celular are trei vulnerabilități majore pe linia securității:

- vulnerabilitatea la monitorizarea conversației în timpul folosirii telefonului;
- vulnerabilitatea telefonului de a fi pe post de microfon pentru monitorizarea conversațiilor 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 alții, înregistrând convorbirile în contul nostru.

Pentru a înțelege slăbiciunile telefoanelor celulare este bine să cunoaștem câteva detalii privind modul lor de funcționare. Ele se bazează pe frecvențe radio prin aer pe două canale distincte, unul pentru comunicațiile 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 față de un „site de celulă”, transmițându-i numărul de identificare al mobilului (*MIN*, *Mobile Identification Number*) și numărul de serie electronic (*ESN*, *Electronic Serial Number*),

cunoscute sub numele generic de pereche (*pair*). Când site-ul celulei primește semnalul pereche, determină dacă solicitantul este înregistrat oficial, prin compararea perechii solicitantului cu lista abonaților 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 recepționat de un nou site-celulă, aflându-se în raza lui de acțiune.

Un telefon celular este, de fapt, un aparat radio cu emisie-recepție. Vocea noastră este transmisă prin aer ca unde radio, iar acestea nu sunt direcționale, ci dispersate în toate direcțiile, astfel încât oricine posedă un anumit tip de radio receptor poate să le intercepteze. Sunt foarte mulți radio-amatori care au site-uri web prin care se schimbă numere de telefon ale unor ținte „interesante”. Uneori persoanele oportuniste cu un astfel de hobby își vând „colecțiile”.

Dacă sistemul celular folosește 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 supravegheaților, este în folosință. Urmărirea automată, asistată de calculator, permite monitorizarea unui telefon anume 24 de ore din 24, după cum ținta se deplasează de la o celulă la alta, fără un alt efort uman.

Dacă sistemul de telefonie celulară folosește tehnologia mai nouă, digitală, supravegherea este mult mai dificilă, dar, la prețuri rezonabile, este posibil ca majoritatea radio-hobiștilor să cumpere un interpretor de date digitale care se conectează între un scanner radio și un calculator personal. Interpretorul datelor digitale citește toate datele digitale transmise între site-ul celulei și telefonul celular și oferă calculatorului aceste informații.

Este destul de simplu pentru un „ascultător” să fixeze numărul de telefon celular al țintei pentru că transmisiile sunt în dublu sens către site-ul celulei, atât timp cât telefonul este alimentat de la baterie și este pregătit să primească apeluri.

Pe piețele occidentale există un echipament numit *Celltracker* (urmăritor de celulă), cu care un „ascultător” se poate orienta spre conversațiile ce apar la un anumit telefon celular prin intermediul celui mai apropiat site-celulă. Numărul telefonului urmărit se introduce în echipament prin tastatură. Agențiile secrete, precum și cele ce supraveghează modul de respectare și punere în aplicare a legii, au la dispoziție echipamente și mai performante. De exemplu, *Law Enforcement Corp* face publicitate unui sistem care monitorizează 19 canale și urmărește trei conversații simultan.

Așa se explică ușurința cu care convorbirea dintre prințesa Diana și prietenul ei, James Gilbey, a fost înregistrată pe bandă, timp de 23 de minute. Ulterior a fost publicată, aflându-se că prietenul prințesei o alintă cu „draga mea sepie”. Nici prințul Charles n-a scăpat. El a fost înregistrat în timp ce discuta cu Camilla despre viața lor sexuală. La fel s-a întâmplat cu purtătorul de cuvânt al Casei Albe, Newt Gingrich. România nu este mai prejos. Vă amintiți de discuția dintre un membru al guvernului din perioada 1992-1996 și un senator, nu prea academică, prin care se negociau niște spații „mai umane”. Sau, în 2002, scandalul interceptării convorbirilor telefonice ale ziariștilor ieșeni. 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 și vânzarea scannerelor de celulare, specialiștii au demonstrat cum, într-un minut, cu două fire scurte de sârmă și un ciocan de lipit, un scanner legal radio se transformă într-un colector impecabil de convorbiri de pe celulare. S-a făcut chiar afirmația 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 „performanță” pe care o știu foarte puțini dintre beneficiarii telefoniei mobile. Se pare că astfel și-a găsit sfârșitul un lider rebel al unui fost stat sovietic sau așa ne explicăm de ce teroriștii nu prea apelează la telefonia celulară. Ei știu că un telefon celular poate fi transformat într-un microfon și emițător cu scopul de a asculta conversațiile din preajma lui. Noua funcție se realizează prin transmiterea către telefonul celular a unei comenzi de întreținere pe canalul de control, operațiune care aduce

telefonul mobil în „modul diagnostic”, după care orice conversație din preajma telefonului mobil poate fi monitorizată prin canalul de voce. Interesant este că utilizatorul nu-și să seama că este în modul diagnostic și că se recepționează toate sunetele din jurul lui, până când va încerca să sune pe cineva și-și va da seama că ceva nu merge. În astfel de situații, înainte ca telefonul să fie folosit pentru noi apeluri, aparatul trebuie să fie închis și 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 informații 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 hoți să monitorizeze spectrul frecvențelor radio și să-și însușească perechea de numere a telefonului celular, atunci când se face înregistrarea anonimă la un site de celulă. Clonarea este procesul prin care un hoț interceptează numărul de serie electronic, *ESN*, și numărul de identificare mobil, *MIN*, apoi programează aceste numere într-un alt telefon și-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 hoții perechii de numere a unui abonat.

ESN-ul și *MIN*-ul se pot obține foarte ușor cu un cititor de *ESN*-uri, care arată ca și 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 și memorează informațiile respective în propria-i memorie. Operațiunea este ușor 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.

Deși pare cam defetistă afirmația 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: parcuri mari, aeroporturi, supermagazine, săli de concerte, stadioane și în toate zonele foarte aglomerate ale orașelor. De puteți evita folosirea celularului în astfel de locuri, ați 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 vulnerabilități majore ale celularelor ar fi una foarte simplă: nefolosirea lor. Și, totuși, dacă le folosiți încercați să reduceți riscurile, respectând următoarele sfaturi:

- pentru că celularul se poate transforma oricând într-un microfon, fără să știm când, nu trebuie să-l purtăm cu noi în locurile în care se discută lucruri sensibile sau se face referire la informații clasificate;
- activați-vă telefonul doar în anumite momente, îndeosebi atunci când vreți să apelați pe cineva. În alte condiții, închideți-l!
- nu oferiți oricui numărul dumneavoastră de mobil. Este o mare greșală. Ca atare, nu-l puneți pe cărți de vizită, pe pagina web, pe corespondența zilnică!;
- dacă puteți, nu folosiți mobilul pentru a fi apelați de alții, căci aceasta înseamnă activarea lui continuă și, firesc, posibilitatea urmăririi continue a dumneavoastră. În acest scop se recomandă folosirea de pager pe care să primiți semnalele de la cei ce vă interesează. După primirea lor, puteți activa și folosi mobilul pentru o scurtă perioadă de timp;
- nu discutați lucruri importante prin telefonul mobil. Când sunați pe cineva, puneți-l în gardă că vorbiți de pe mobil și atenționați-l, dacă e cazul, că mobilul e vulnerabil și că trebuie să se poarte doar discuții generale, fără detalii;
- nu lăsați mobilul nesupravegheat;
- evitați folosirea telefonului mobil în locuri foarte aglomerate și în imediata lor apropiere. Aici este terenul propice pentru radio-amatorii ce folosesc scannere pentru

monitorizări aleatoare. Dacă v-au identificat și „le place” discuția, vă vor reține pentru monitorizarea permanentă;

- dacă vi se oferă de către compania telefonică un PIN (Personal Identification Number), folosiți-l o dată și nu la fiecare activare, că șansele de a fi clonat aparatul sunt mai reduse.

Există o zicere înțeleaptă care spune: Doamne, spune-mi dușmanul care mi-e prieten, căci pe ceilalți îi știu eu! Unde plasați celularul!?!



- Adaptați formele de manifestare a pericolelor în sistemele informaționale prezentate în subcapitolul 1.2.3. la tehnologiile mobile, identificând factori naturali, incidente și atacuri care afectează datele și informațiile transmise în mediul mobil .
- Câte vulnerabilități asociate Bluetooth cunoașteți? Noi începem lista cu *bluejacking*...

7.1.3 Securitatea telefoanelor portabile

Telefoanele portabile au constituit, la vremea lansării lor pe piață, o realizare deosebită, prin dispariția unicului loc de unde se putea vorbi în sistemul telefoniei fixe. Iată că și numele își pierde sensul odată cu inventarea telefonului portabil. S-au înregistrat multe satisfacții în lumea utilizatorilor fără ca ei să-și dea seama că totul se plătește. În cazul de față, comoditatea purtării unei convorbiri telefonice era eclipsată de creșterea insecurității, cât timp transmisiile pot fi recepționate de la mai mult de un kilometru distanță. Cu un telefon analogic foarte ieftin, oricine posedă un scanner radio și se află în vecinătatea unui telefon portabil poate să-și regleze scannerul pe conversația respectivă și 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 ședințele de lucru sau la conferințe. 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 condiționată de categoria informațiilor comunicate, evitându-se cele clasificate și/sau neclasificate speciale.

Din această categorie, telefoanele digitale sunt mai sigure, întrucât interceptarea pe canalul de voce a unor semnale digitale înseamnă recepționarea unui simplu zgomot. Totuși, radio-amatorii mai pretențioși 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 și 2,4 GHz. Acestea au o lățime a benzii foarte mare și nu pot fi urmărite cu aparatura obișnuită de scannare a frecvențelor radio. Doar aparatura foarte performantă poate fi folosită pentru interceptare.

Oricum, un posesor de aparat portabil poate fi dușmanul principal al altui posesor de aparat identic, prin furtul tonului și folosirea lui pentru conversații facturate titularului aparatului.

Procedura este foarte simplă. Cineva, cu un aparat portabil activat, urcă în propriul autoturism și începe să se plimbe pe o stradă unde știe că sunt mai multe portabile sau bănuiește acest lucru. Când telefonul lui primește semnalul de ton înseamnă că aparatul este compatibil cu cel din zonă în care se află și astfel poate să înceapă convorbirile în contul altuia. Și dacă cineva ridică telefonul interceptat nu-și dă seama de ceea ce se întâmplă, ci doar dacă, accidental, privește pe geam, vede că într-un autoturism cineva vorbește 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 poștei vocale (Voice Mail, V-Mail)

Una dintre performanțele deosebite ale poștei vocale constă în posibilitatea accesării de la distanță a acesteia. Nu este necesară deplasarea la birou pentru a-ți consulta poșta vocală, ci de la distanță. După lansarea apelului telefonic, prin introducerea unei parole, se pot asculta mesajele înregistrate. Din păcate aceeași operațiune poate fi efectuată și de o terță persoană.

Ghicirea parolei nu este o mare problemă, pentru că sunt prea puține persoane 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 angajaților. Alteori, când se schimbă parola, greșelile sunt comune, apelându-se la nume sau persoane sau data nașterii.

Cele mai mari amenințări vin de la foștii angajați care cunosc numărul de telefon al poștei vocale și pot intui parolele cu ușurință.

Cu câțiva ani în urmă, președintele unei companii de valori imobiliare a anunțat Serviciile Secrete ale S.U.A. că hackerii i-au atacat calculatorul care gestiona mesajele vocale. Ancheta a condus la Leslie Lynne Doucette, cunoscută și sub numele Kyrrie, care era capul unei rețele ce se ocupa de fraudele prin calculatoarele ce administrau poșta vocală din S.U.A. Asupra ei s-au găsit 481 coduri de acces, folosite de 152 hackeri.

De regulă, puștii de 13-15 ani dau lovituri mari, fie folosind sistemul pentru convorbiri la distanțe mari, fie pentru a intra în posesia unor informații 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 reieșit că jumătate dintre hackeri – mai degrabă i-am numi *phreakeri* – sunt elevi sau studenți, între 14 și 22 de ani. Cam o treime nu erau angajați, iar vârsta lor se situa între 18 și 35 de ani. Restul aveau vârste între 18 și 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 invenție 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, așa 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 recepționează un astfel de mesaj știu foarte bine ce au de făcut, casa fiind nelocuită o bună perioadă de timp. Dar insecuritatea provine și din alte cauze. Vulnerabilitatea este aproape similară celei descrise la poșta vocală. Accesul de la distanță este o înlesnire bine venită pentru posesorul telefonului cu robot dar, în același timp, el oferă impostorilor șansa să-l utilizeze. Ei pot forma numărul nostru și asculta mesajele. Singura protecție constă într-un cod scurt, presetat de producător, și care rareori este schimbat de cumpărător. Codul de folosire este cunoscut de cei ce se ocupă cu astfel de activități. Și dacă este schimbat, codul poate fi ușor spart de „profesioniști”.

Roboților telefoniei li s-a mai adăugat o a doua vulnerabilitate: lor li s-a introdus funcția ce-i permite proprietarului să sune acasă și să asculte ce se întâmplă acolo, telefonul acționând ca un microfon ce va capta fondul sonor al locuințelor. Totul este frumos, numai că realizatorii acestei performanțe tehnice nu s-au gândit că la fel poate proceda și o terță persoană care ar dori să intre în intimitatea casei noastre.

7.1.6 Interfonul casei și supraveghetorii de copii (*Baby Monitors*)

În urmă cu vreo câțiva ani mă aflam în casa unui croitor și 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 comunicații din casă se bazează pe un set de transmițătoare și cu emițătoare care apelează la energia electrică a firelor instalației din casă în două moduri: transformă curentul alternativ în curent cărauș și, în același timp, folosește firele drept antenă pentru a

transmite mesajele de la emițător la receptor. Tehnologia se numește *carrier current*, adică ar fi curentul cărăuș. Ceea ce nu știa croitorul este faptul că dialogurile lor, atât de ușor realizate, puteau fi interceptate și de alții aflați pe stradă, cu condiția să aibă un aparat similar care să funcționeze pe aceeași frecvență sau să dețină un scanner de frecvență 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 spațiilor unde sunt amplasate. Majoritatea sunt puse în priză de curent alternativ și folosesc un sistem identic celui descris anterior. Sunt și sisteme care folosesc frecvențele radio. Scopul unor astfel de aparate este acela de a alerta părinții când se întâmplă ceva în camera de joacă sau în dormitoarele copiilor, situate în diverse locuri ale casei.

Odată cu liniștea oferită părinților, ele constituie și un atentat la intimitatea casei prin vulnerabilitatea în fața celor interesați a le intercepta.

7.2 Securitatea transmisiilor

Problema securității transmisiei de date se pune în mod deosebit atunci când două sau mai multe calculatoare sau terminale conversaționale sunt interconectate într-o rețea. Acolo unde funcționează o astfel de rețea, responsabilul cu prelucrarea automată a datelor din partea unității, contabilul șef sau vicepreședintele coordonator al activității sistemului informatic trebuie să desemneze pe unul din responsabilii activității de prelucrare automată a datelor sau pe o altă persoană să răspundă de rețea, în sensul supravegherii tuturor activităților care se referă la două sau mai multe posturi de lucru în rețea.

Terminalele aflate la distanță trebuie să funcționeze în așa-zisul *mod prestabilit*. El constă în stabilirea unor reguli de folosire de către utilizatorii acestor terminale numai în limitele unui program special de aplicații, aflat sub controlul direct al sistemului de operare, și trebuie să realizeze două funcții principale: intermedierea și 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 și 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 și controlul biților de paritate.

Cel mai important lucru realizat prin funcția 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 secvență de comenzi are un răspuns sau un efect prestabilit, ceea ce ar însemna că ea nu afectează programul aplicațiilor, nici sistemul de operare și nici datele cu regim special. Accesul este autentificat la anumite puncte din aplicații, în caz contrar utilizatorul fiind dezafectat din rețea.

Controlorul de rețea trebuie să permită doar procedurile de funcționare care se încadrează într-un scenariu predeterminat dintre punctele terminale și calculatorul central. Operatorii trebuie să respecte cu strictețe modurile de lucru respective.

Fiecare calculator trebuie să poată identifica, fără ambiguități, traseul pe care se realizează la transmisie sau recepție traficul de date, cunoscându-se portul sau canalul de comunicație.

Comunicațiile terminalelor trebuie să se declanșeze sub controlul calculatorului central în momente predeterminate pentru anumite categorii de lucrări. Controlorul de rețea va realiza și va lua decizia pe linia ordinii de execuție a acestora.

Comunicațiile nu trebuie să aibă loc înainte de autentificare, componentă de bază a sistemului de securitate, apelându-se la parole, tabele de autentificare și la celelalte tehnici de asigurare a securității.

O atenție deosebită trebuie să se acorde sistemului de intrare în regim de comunicație cu calculatorul central și cu terminalele, *prin remorcare (piggybacking)*, intrusul dispunând de un

minicalculator cu care să efectueze o astfel de operațiune ilegală, având acces la ceea ce și-a propus să obțină.

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 și 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 și a transmite caracterele aflate la intersecția liniei cu coloana specificată de utilizator, realizându-se astfel autentificarea prin verificarea acelorași caractere dintr-un tabel similar al transmiiătorului.

Mesajele test. Comunicația efectivă nu trebuie să se declanșeze până când ambele capete ale liniei nu au transmis suficiente mesaje test, astfel încât controlerul să poată stabili că toate circuitele funcționează corect. O secvență de mesaje test va include suficiente erori și tentative de depășire a sistemului de securitate pentru a verifica vigența lui.

Reautentificarea. După ce comunicarea este înlesnită, reautentificarea punctelor terminale, a calculatorului central sau a ambelor se impune pentru a testa potențialii „remorcați” ai dialogului. Operațiunea 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 depășire a zonei autorizate de lucru; cererea de acces la programe și 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 lipsește de la terminal, se cere ca sistemul să testeze aceste prezențe și, în condiții date, să se închidă singur.

Securitatea comunicației. În caz de defecțiune, 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 comunicațiilor și asigurarea copiilor. Rolul lor este de a facilita analizele de trafic și de a permite reconstituirea datelor pierdute.

Alături de toate aceste mijloace și metode, există și altele cu un pronunțat caracter tehnic, cel mai important fiind sistemul verificării parității sau imparității codurilor transmise.

7.3 Securitatea radiațiilor

Toate echipamentele care funcționează pe bază de energie electrică, chiar și mașinile de spălat, produc energie electrică, emisă prin semnale electromagnetice necontrolabile, transmisibile prin aer, ca undele radio, sau de-a lungul firelor și metalelor conductibile, ca orice curent electric. Este în natura lucrurilor un astfel de fenomen și nimic nu îl poate stopa. Astfel de radiații de la calculatoare sau de la cablurile de comunicații pot fi purtătoare de informații, ce pot fi extrase de către persoane din afară, după o analiză specială.

7.3.1 Cadrul general al radiațiilor necontrolate

Protecția echipamentelor de prelucrare automată a datelor utilizate pentru informațiile speciale împotriva riscului generat de propriile lor radiații este una dintre cele mai dificile probleme puse în fața agențiilor specializate din orice parte a globului. Ele nu sunt de competența utilizatorilor finali și 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 aceleași programe, poate să-și dea seama cu ușurință cam ce activități efectuează echipamentele, fără să fie nevoie să privească la consolă sau la operator. Urechea deslușește sunetele produse de diverse echipamente. Toate acestea sunt *radiații acustice*.

Echipamentele electronice și cele electromagnetice au *radiații electrice*.

În general, complexitatea radiațiilor echipamentelor depinde de felul lor și de mediul în care se utilizează:

- echipamentele periferice, în special imprimantele și aparatura video, emit semnale puternice, fără zgomote, ce pot fi „percepute” de la distanță;
- semnalele produse de unitatea centrală de prelucrare sunt mai complexe și mai greu de descifrat. De asemenea, zonele aglomerate cu multe echipamente video și 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 radiații depinde, în mare parte, de măsurile de protecție încorporate în el în fazele de proiectare, fabricație, instalare și utilizare;
- de regulă, radiațiile de la un echipament de birou pot fi detectate de la o distanță de până la 100 de metri, deși sunt numeroase excepții, după cum o să reiasă din prezentările ulterioare.

Pentru preîntâmpinarea sau diminuarea pericolelor radiațiilor, s-au realizat echipamente speciale, despre care literatura de specialitate are următoarele păreri:

- există o prea mare preocupare pe linia promovării și, firesc, a comercializării aparaturii de distrugere a radiațiilor compromițătoare, *TEMPEST (Transient ElectroMagnetic Pulse Emanation STandardizing)*. Cu câțiva 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 afișa pe un monitor dintr-un birou aflat în centrul Londrei, operațiunea reușind îndeosebi datorită utilizării calculatorului. De fapt, povestea este ceva mai veche, întrucât cu câțiva ani în urmă, un cercetător din Olanda a demonstrat că oricine dispune de un televizor, ce conține mici modificări, ar putea citi ecranul unui calculator personal sau al unui terminal aflat la o distanță de aproximativ ... 15 Km;
- dintre cei ce susțin 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 radiațiile, ceea ce presupune un mare consum de timp și de resurse;
- pentru a obține un semnal corect și util, e nevoie ca răufăcătorii să se situeze la o distanță 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 prezența și să anunțe pe cei în drept pentru a lua măsurile necesare. Echipamentele cu gabarit redus sunt mai puțin eficiente, iar cele portabile au o utilitate foarte mică, întrucât purtătorul lor poate sesiza prin propriile organe de simț ce îl interesează, fără să mai apeleze la astfel de echipamente;
- fenomenul captării radiațiilor necontrolate nu este așa de ușor de înfăptuit, cum se întâmplă cu metodele descrise anterior. El presupune cunoștințe tehnice de înalt nivel, echipament scump, timp și șansă, dar și expunerea atacantului la un mare risc.

Totuși, ar fi o mare greșală să se desconsidere o astfel de tehnică de interceptare a informațiilor. De regulă, calculatoarele situate în zone foarte aglomerate sunt și cele mai vulnerabile la atac.

În cazul aplicațiilor militare, în care se prelucrează multe date secrete, problema interceptării radiațiilor trebuie pusă cu multă seriozitate, în toate fazele de realizare a sistemelor.

Oricum, aparatura anti-interceptare-radiații este mai mult o dorință 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 Măsurile elementare de precauție împotriva captării radiațiilor necontrolate

Există un număr substanțial de măsuri, relativ ieftine, de diminuare a pericolului răspândirii necontrolate a datelor prin radiații compromițătoare. Dintre ele amintim:

1. *Zonele sterile.* Se recomandă crearea unor zone sterile în jurul echipamentelor de prelucrare automată a datelor, în special al monitoarelor și imprimantelor, prin îndepărtarea tuturor corpurilor metalice din preajma lor. Nu se recomandă folosirea birourilor metalice, nici măcar cu picioare din metal și nici coșuri de gunoi metalice.

2. *Telefoanele.* Monitoarele sunt veritabile surse de informații, iar, pentru bunul mers al operării, alături de ele se plasează telefonul, numai că în timp ce datele se afișează pe ecran, telefonul, chiar dacă este în repaus, poate să transmită datele oriunde în afara unității. De aceea, oricând este posibil, toate componentele telefonului, inclusiv cablurile, trebuie să fie ținute la distanță de echipamentele ce prelucrează date secrete.

Dacă telefonul este, totuși, necesar:

- el trebuie amplasat la periferia zonei secrete, cu un filtru potrivit de distrugere a emanațiilor compromițătoare;
- „securitatea în timpul nefolosirii” telefonului se realizează prin deconectarea aparatului de la linie.

3. *Curenții filtranți.* Radiațiile compromițătoare pot fi diminuate prin transmiterea în cablu a unor curenți filtranți.

4. *Accesul.* Un rol important va reveni controlării accesului în unitate al persoanelor sau al prezenței vehiculelor în preajma centrului de prelucrare.

5. *Amplasarea echipamentelor în birouri.* Se va evita plasarea echipamentelor lângă ferestre, se vor poziționa monitoarele cu ecranele spre interiorul camerei pentru prevenirea observării directe a ecranului din afara ei, deși radiațiile pot fi oricum compromițătoare. Se recomandă plasarea tuturor componentelor fizice în centrul clădirii, pentru a beneficia de rolul protector al zidurilor și al altor materiale cu rol asemănător. Atenție mărită se va acorda locurilor în care se amplasează telefoanele.

6. *Echipamentele moderne.* Seturile actuale de echipamente electronice de calcul tind să dea mai puține radiații în afară decât vechile modele. Preocupările au fost concentrate spre protejarea operatorilor de a nu mai fi „bombardați” cu radiații puternice, ceea ce a dus și la diminuarea radiațiilor compromițătoare.

7. *Curățirea ecranelor.* Scurgerile de date pot avea loc doar atunci când ele sunt afișate pe ecran sau în timpul procesului de imprimare. Personalul va fi instruit să șteargă ecranul după ce nu mai are nevoie de datele afișate și, de asemenea, nu se recomandă listarea de probă de prea multe ori a documentelor ce conțin date secrete.

8. *Derutarea.* Datele importante pot fi protejate prin crearea unui val de scurgeri de informații 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 importanță, dar care vor fi interceptate de inamicii sistemului. Mai mult chiar, li se va înlesni un acces foarte ușor la ele.

7.3.3 Echipamente de testare a existenței radiațiilor de date

Practica oferă echipamente speciale pentru testarea existenței radiațiilor compromițătoare de date, dar decizia procurării lor este foarte îndrăznească din cauza prețurilor foarte mari și a dificultății procurării lor. Echipamentele veritabile funcționează prin crearea unui mediu izolant din cupru în jurul întregii configurații de echipamente ale sistemului. Dacă instalarea și exploatarea se desfășoară conform proiectului, se poate pune problema anihilării radiațiilor

compromițătoare aproape în întregime. Sunt, totuși, câteva aspecte de care trebuie să se țină 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 distanță și care nu au o protecție fizică adecvată, mai ales când prelucrează date foarte importante;
- aparatura de protecție trebuie tratată cu deosebită atenție, 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-și dea seama dacă ele funcționează la cotele maxime, ci numai unitățile specializate pot da un astfel de verdict;
- calculatoarele mari sau întregul centru de calcul poate fi plasat într-un spațiu de cupru protejat total – cușca lui Faraday – , dar acesta costă foarte mult și dă senzația unui mediu neplăcut de lucru.

7.4 Securitatea tehnică

Securitatea tehnică, ultimul domeniu din studiul securității comunicațiilor, ar fi și 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. și Canada. Ea se află în sfera de preocupare a agențiilor naționale de securitate, dar și a unor grupări care se ocupă de diverse activități interzise de legile oricărui stat, ele urmărind, în mod indirect, fie să obțină anumite avantaje materiale, fie informaționale.

Atacurile cu scop de supraveghere tehnică asupra centrelor de prelucrare automată a datelor nu au ca obiectiv primar aspectele tehnice ale activităților desfășurate în aceste locuri, ci, mai degrabă, 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 discuții mult mai importante decât sălile de consiliu sau ale executivului, sunt mult mai interesante și, deci, mai expuse pericolului de a fi supravegheate, în mod fraudulos.

Supravegherea tehnică a birourilor securității 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 acțiunilor de curățire 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 securității 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, țevilor, ușilor, ferestrelor, conductorilor electrici ș.a. Se va continua cu stabilirea locurilor de amplasare a mobilierului, rafturilor, lămpilor, diverselor aparate, tablourilor, cablurilor mobile ș.a. Orice modificare a poziției acestora trebuie să fie anunțată din timp.

Se va continua cu fotografierea camerelor din diverse unghiuri. Examinarea fizică a zonei constă în repetarea activităților anterioare și compararea lor. Vor fi urmărite îndeosebi locurile

ascunse: cărțile, dosul draperiilor, ramele tablourilor, birourile, stilourile, zona de dedesubt a meselor, scaunelor, deși imaginația intrușilor poate fi mult mai bogată. La o ambasadă vestică dintr-o țară a fostului bloc comunist s-au descoperit „corpuri străine” sub parchetul sălii.

Cercetările electrice. Partea electrică din acțiunea 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 poziții. Piese importante pot fi marcate pentru o recunoaștere ulterioară, iar bobina de inducție va fi scoasă și înlocuită conform discuțiilor de la „securitatea liniilor de comunicație”.

Similar se va proceda cu întregul sistem de comunicație prin telefon, radio, televiziune, aparate de înregistrat ș.a. Se vor desface și cerceta dozele electrice, de telefon, prizele și 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 și de un aparat de măsură. În structura lui se află un oscilator de frecvențe radio și o antenă pe bază de ferite. Lumina se aprinde dacă radiațiile 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 configurația normală a sălii sau clădirii. Se efectuează câteva cercetări cu detectorul asupra pereților, podelei, tavanului și se marchează punctele în care se aprinde lampa sau aparatul sesizează prezența corpurilor metalice. În pasul următor, se repetă cercetarea și se marchează locurile unde lumina nu s-a aprins mai înainte.

Din arsenalul securității tehnice arma de apărare principală este *detectorul de „muzicuțe”*. 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 și circuitele de control se află într-o geantă de umăr. Aparatul detectează prezența tuturor diodelor semiconductoare dintr-o cameră, bineînțeles și a celor care fac parte din configurația normală a aparatelor întrebuintate. Puterea lui trece de multe ori de limita fizică a zidurilor camerei.

Detectia radiațiilor. Detectia radiațiilor continuă seria căutărilor în locurile în care s-au constatat unele aspecte ciudate în urma cercetărilor fizice și electrice. Echipamentele de transmisie în spațiul liber sunt folosite de profesioniștii ascultărilor neautorizate și pot fi activate sau dezactivate de la distanță.

Detectorul de muzicuțe va sesiza pe cele ce nu sunt activate, iar detectorul de radiații va afla sursa de radiații.

O problemă importantă, în acest caz, se referă la *cunoașterea modului în care pot fi activate microfoanele secrete sau emițătoarele*.

Unele emițătoare ale amatorilor acționează 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 funcționa cu succes.

În acțiunea de cercetare, nu se recomandă provocarea activării microfoanelor secrete prin fluierături, astfel încât prezența lor să fie sesizată. Echipele însărcinate cu o astfel de misiune trebuie să lucreze în liniște, fără ca ascultătorii neautorizați să-și dea seama că s-a făcut simțită prezența microfonului secret. Dimpotrivă, după localizarea microfonului intrus se pot întinde curse sau emite informații false.

Înregistrarea pe bandă a discuțiilor de afaceri poate fi declanșată tot prin elemente străine, care să stabilească momentul în care să înceapă să funcționeze. În afara microfoanelor/emițătoarelor străine introduse în aparatura din cameră sunt cunoscute și activatoarele de înregistrări, aflate în preșurile de la uși, în pernele fotoliilor sau în saltelele paturilor. În ultimul caz, reglajul este stabilit să declanșeze înregistrarea când în pat se constată greutatea medie a două persoane.

Instrumentul principal de detectare a radiațiilor 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 aglomerație maximă, cu comutatoarele aparatelor din cameră activate și neactivate.

Există și alte aparate pentru descoperirea microfoanelor/emițătoarelor secrete, de regulă, create pentru liniștea utilizatorilor obișnuiți, dar instituțiile și locurile ce se știu urmărite cu orice preț, 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 țevi sau pe conducte, pe care se lipește urechea pentru a asculta discuțiile.

Șarpele este un tub gol în interior, plasat alături de țevile instalațiilor electrice care face legătura între camera ascultată și locul de ascultare.

Țeapa este o vergea lungă ce asigură cuplarea acustică între camera ascultată și microfonul intrus. Literatura citează cazul țepeii 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 obișnuită de captare a sunetelor poate fi folosită și la captarea electrică a emanațiilor de date. În Vietnam grotelile dealurilor erau folosite ca o ureche mărită.

Pușca de vânătoare este o variantă a antenei acustice, care folosește 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 și casele se vor schimba de o persoană de serviciu, care este angajată la firmă, dar „cumpărată” de cei interesați. 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 „muzicuță”

Microfoane și fire. Cele mai obișnuite 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 țesătura covorului.

Pioneza este un cilindru de cauciuc cu capul având funcția 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 și un diametru de 3 mm, transparent, cu un minuscul microfon la un cap și 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 mașinii. Microfoanele se plasează în interiorul portbagajului și de la ele sunt fire mascate ce duc spre aparatul de înregistrat. Șoferul părăsea mașina în timpul discuțiilor, dar, fiind omul serviciilor secrete nu uita să-și regleze sistemul de lucru.

Emițătoarele în spațiul liber. Emițătoarele clandestine se vând la prețuri foarte mici, câteva zeci de dolari, și sunt cunoscute sub numele de „doică electronică”. Un emițător foarte cunoscut, de dimensiunea unui timbru poștal, este cel numit „păianjenul Hong Kong”.

De regulă, amatorii în „trasul cu urechea” folosesc emițătoare de frecvență asemănătoare stațiilor radio sau TV. Rezultatul operațiunii depinde și de receptor, care, de regulă, nu poate fi plasat mai departe de câteva sute de metri.

Emițătoarele funcționează pe bază de baterii, deci misiunea lor încetează când bateriile se consumă, fiind nevoie de sprijinul oferit de „cineva” pentru a le înlocui. Emițătoarele, de regulă, se amplasează în aparatura-gazdă, de unde își iau și energia necesară.

Sunt preferate instalările de emițătoare în locul aparaturii de înregistrare, întrucât atunci când persoana este prinsă nu se pot cunoaște și cele mai recente date captate. Emițătorul funcționează pe bază de cristale și operează în frecvența de 30-50 megahertzi. Sunt și excepții de la regulă. Uneori numai aceste dispozitive asigură succesul sigur al intrușilor, celelalte fiind ușor detectabile.

Intrușii echipamentelor. În timp, cele mai multe tentative de implantare a dispozitivelor străine în echipamentele celor spionați s-au orientat spre dispozitivele de criptare. Într-un caz, dispozitivul de criptare s-a aflat în *bobina de inducție* și avea rolul de a stabili ce taste au fost apășate pentru introducerea textului în clar de la tastatura mașinii de criptat.

În alt caz, după ce dispozitivul a fost luat pentru o „reparație” de o oră, s-a constatat că avea instalat în el un emițător radio. Acesta a fost introdus într-un condensator și 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 ținta a cât mai multe acțiuni 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 biți + 1 de paritate) emițătoare, făcându-le dificil de utilizat de către intruși.

În afara elementelor descrise până acum mai sunt și altele care au un pronunțat caracter tehnic, ele depășind cadrul materialului de față.

Rezumat

Pentru a demonstra vulnerabilitatea sistemelor de comunicație în fața persoanelor rău-intenționate, sunt prezentate posibilitățile de interceptare a comunicațiilor și alte vulnerabilități care apar în cazul telefoanelor standard, celulelor, telefoanelor portabile, poștei vocale, robotului telefonic, pagerelor, interfoanelor și al baby monitors.

Transmișiile, radiațiile și supravegherea tehnică sunt analizate separat, în termenii vulnerabilităților și măsurilor de asigurare a securității.

CAPITOLUL VIII

Aspecte juridice privind protecția și securitatea sistemelor informaționale²¹

Domeniul atât de sinuos al protecției și securității informațiilor, sistemelor informaționale și al tuturor componentelor specifice nu se limitează doar la politicile și măsurile care pot fi stabilite la nivelul organizațiilor, ci trebuie să abordeze și 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 informațiile, prelucrarea și transmiterea lor. Obiectivele capitolului sunt:

- cunoașterea principalelor reglementări juridice privind protecția și securitatea informațiilor existente în România;
- dobândirea de informații despre principalele aspecte ce caracterizează copyright-ul, mărcile înregistrare și licențele.

8.1 Legislația în România

La nivelul României, în ultimii ani, au început să apară din ce în ce mai multe reglementări legislative privind protecția și securitatea informațiilor. Lucrurile s-au schimbat odată cu proliferarea și pe teritoriul țării a tehnologiilor informaționale și de comunicații, care au eliminat barierele de timp, spațiu și localizare a prelucrării, stocării și transmiterii informațiilor. Chiar dacă sunt încă multe lacune în această privință, se poate spune că este un început bun pentru trecerea României la societatea informațională și a cunoașterii.

Printre cele mai importante legi care reglementează, direct sau indirect, protejarea informațiilor, mecanismele de prelucrare, stocare și transmitere, se pot enumera:

- Legea 51/1991 *privind siguranța națională a României*;
- Legea 182/2002 *privind protecția informațiilor clasificate*, însoțită de Hotărârea de Guvern 585/2002 pentru aprobarea *Standardelor naționale de protecție a informațiilor clasificate în România*;
- Hotărârea de Guvern 781/2002 *privind protecția informațiilor secrete de serviciu*;
- Ordonanța de Guvern 34/2002 *privind accesul la rețelele de telecomunicații electronice și la infrastructura asociată, precum și interconectarea acestora*;
- Legea 544/2001 *privind liberul acces la informația de interes public*;
- Legea 677/2001 *privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date*;
- Legea 682/2001 *privind ratificarea Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal*, adoptată la Strasbourg la 28 ianuarie 1981;
- Ordinul Avocatului Poporului 52/2002 *privind aprobarea cerințelor minime de securitate a prelucrărilor de date cu caracter personal*;
- Ordinul Avocatului Poporului 75/2002 *privind stabilirea unor măsuri și proceduri specifice care să asigure un nivel satisfăcător de protecție a drepturilor persoanelor ale căror date cu caracter personal fac obiectul prelucrărilor*;

²¹ Capitol realizat, în cea mai mare parte, de prof. dr. Gabriela Meșniță de la Universitatea „Al. I. Cuza” Iași, Facultatea de Economie și Administrarea Afacerilor și revizuit pentru noua ediție de lect. dr. Daniela Popescu

- Legea 506/2004 privind *prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice*;
- Legea 102/2005 privind *înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal*;
- Legea 161/2003 privind *unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției*, care conține componenta de prevenire și combatere a *criminalității informatice*, în Titlul III;
- Legea 64/2004 pentru *ratificarea Convenției Consiliului Europei privind criminalitatea informatică*, adoptată la Budapesta la 23 noiembrie 2001;
- Ordonanța 130/2000 privind *protecția consumatorilor la încheierea și executarea contractelor la distanță*, aprobată cu modificări prin Legea 51/2003;
- Legea 365/2002 *privind comerțul electronic*, modificată și completată prin Legea 121/2006;
- Legea 455/2001 *privind semnătura electronică*, împreună cu Norma tehnică și metodologică din 13 decembrie 2001 pentru aplicarea ei;
- Legea 451/2004 *privind marca temporală*;
- Legea 589/2004 privind *regimul juridic al activității electronice notariale*, împreună cu Ordinul Ministrului Comunicațiilor și Tehnologiei Informației pentru aprobarea normelor tehnice și metodologice pentru aplicarea ei, nr. 221/2005;
- Hotărârea de Guvern 557/2006 *privind stabilirea datei de la care se pun în circulație pașapoartele electronice, precum și a formei și conținutului acestora*;
- Ordinul Ministerului Finanțelor Publice 875/2001 pentru aprobarea *Regulamentului privind operațiunile cu titluri de stat emise în formă dematerializată*;
- Ordonanța de Guvern 24/2002 *privind încasarea prin mijloace electronice a impozitelor și taxelor locale*;
- Ordinul Ministerului Comunicațiilor și Tehnologiei Informației 218/2004 privind procedura de avizare a *instrumentelor de plată cu acces la distanță, de tipul aplicațiilor Internet-banking, home-banking sau mobile-banking*;
- Regulamentul Băncii Naționale a României 6/octombrie 2006 privind *emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente*;
- Legea 8/1996 privind dreptul de autor și drepturile conexe, care conține informații privind *drepturile autorilor programelor de calculator*;
- Ordonanța de Urgență 123/2005 pentru modificarea și completarea Legii 8/1996 *privind dreptul de autor și drepturile conexe*, care aduce câteva precizări suplimentare privind *distribuirea pe Internet a bazelor de date și a programelor de calculator*. Actele normative privind dreptul de autor sunt prezentate în paragraful 8.2.2.3.

Legea 51/1991 privind siguranța națională a României

Una dintre primele legi care face referire la securitatea informațiilor pe teritoriul României a fost *Legea privind siguranța națională a României*, din 1991.

Printre principalele aspecte pe care le abordează sunt și cele care se referă la organismele naționale care au în atribuții activitatea de informații privind realizarea siguranței naționale, și anume:

- Serviciul Român de Informații, care este organul specializat în materie de informații din interiorul țării;
- Serviciul de Informații Externe, care urmărește obținerea informațiilor din străinătate referitoare la siguranța națională;

- Serviciul de Protecție și Pază, organ specializat în asigurarea protecției demnitarilor români și străini pe timpul prezenței lor în România, precum și în asigurarea pazei sediilor de lucru și reședințelor acestora.

Legea stabilește că *activitățile ce sunt legate de informații* necesare realizării siguranței naționale *au caracter secret*, stabilindu-se categoriile de persoane și organisme cărora li se pot comunica aceste informații (președintele Senatului, al Camerei Deputaților, comisiile permanente pentru apărare publică, miniștrii și șefii departamentelor ministeriale, prefectii, primarul general al Capitalei, conducătorii consiliilor județene, organele de urmărire penală).

Divulgarea, prin orice mijloace, a datelor și informațiilor secrete care pot aduce prejudicii intereselor naționale, indiferent de modul în care au fost obținute, este interzisă și se pedepsește potrivit prevederilor legale.

Pentru obținerea unor informații din această categorie este necesară autorizarea efectuării unor astfel de acțiuni de către procurorul general al României. În categoria actelor ce pot fi autorizate intră:

- interceptarea comunicațiilor;
- căutarea unor informații, documente sau înscrisuri pentru obținerea cărora este necesar accesul într-un loc, la un obiect sau deschiderea unui obiect;
- ridicarea și repunerea la loc a unui obiect sau document, examinarea lui, extragerea informațiilor pe care acesta le conține, cât și înregistrarea, copierea sau obținerea de extrase prin orice procedee;
- instalarea de obiecte, întreținerea și ridicarea acestora din locurile în care au fost depuse.

Cererea de autorizare trebuie să fie formulată în scris și să conțină următoarele informații:

- date sau indicii din care să rezulte existența unei amenințări la adresa siguranței naționale, prevăzute în lege, pentru a cărei prevenire, descoperire sau contracarare este necesară emiterea mandatului;
- categoriile de activități pentru care trebuie emis mandatul;
- identitatea persoanei ale cărei comunicații trebuie interceptate, dacă este cunoscută, sau a persoanei care deține informațiile, documentele sau obiectele ce trebuie obținute;
- descrierea generală, dacă și când este posibil, a locului în care urmează a fi executate activitățile autorizate;
- durata de valabilitate a mandatului solicitat.

Dacă cererea de eliberare a mandatului a fost aprobată, acesta trebuie să conțină:

- aprobarea pentru categoriile de comunicații care pot fi interceptate, categoriile de informații, documente sau obiecte care pot fi obținute;
- identitatea persoanei, dacă este cunoscută, ale cărei comunicații trebuie interceptate sau care se află în posesia datelor, informațiilor, documentelor sau obiectelor ce trebuie obținute;
- organul împuternicit cu executarea;
- descrierea generală a locului în care urmează a fi executat mandatul;
- durata de valabilitate a mandatului, care nu poate depăși 6 luni.

În lege se specifică faptul că mijloacele de obținere a informațiilor necesare siguranței naționale nu trebuie să lezeze drepturile sau libertățile cetățenilor, viața particulară, onoarea sau reputația lor, ori să îi supună la îngrădiri ilegale. Inițierea, organizarea sau constituirea pe teritoriul României a unor structuri informative care pot atinge siguranța națională, sprijinirea acestora sau aderarea la ele, deținerea, confecționarea sau folosirea ilegală de mijloace specifice de interceptare a comunicațiilor, precum și culegerea și transmiterea de informații cu caracter secret ori confidențial, prin orice mijloace, în afara cadrului legal, se pedepsesc potrivit prevederilor în vigoare. Informațiile privind viața particulară, onoarea sau reputația persoanelor,

cunoscute incidental în cadrul obținerii datelor necesare siguranței naționale, nu pot fi făcute publice.

Legea prevede că documentele organelor de informații și ale celor cu atribuții în domeniul siguranței naționale se păstrează în arhivele acestora și nu pot fi consultate decât în condițiile legii.

Legea 182/2002 privind protecția informațiilor clasificate

Scopul legii îl reprezintă protecția informațiilor clasificate și a surselor confidențiale ce asigură acest tip de informații. Protejarea lor se face prin instituirea sistemului național de protecție a informațiilor.

Principalele obiective ale protecției informațiilor clasificate sunt:

- protejarea informațiilor clasificate împotriva acțiunilor de spionaj, compromitere sau acces neautorizat, alterării sau modificării conținutului acestora, precum și împotriva sabotajelor ori distrugerilor neautorizate;
- realizarea securității sistemelor informatice și de transmitere a informațiilor clasificate.

Protecția informațiilor clasificate vizează:

- protecția juridică;
- protecția prin măsuri procedurale;
- protecția fizică;
- protecția personalului care are acces la informațiile clasificate ori este desemnat să asigure securitatea acestora;
- protecția surselor generatoare de informații.

În lege sunt abordate definițiile principalilor termeni care operează în domeniul protejării informațiilor clasificate, și anume:

- *informații* – orice documente, date, obiecte sau activități, indiferent de suport, formă, mod de exprimare sau de punere în circulație;
- *informații clasificate* – informațiile, datele, documentele de interes pentru securitatea națională, care, datorită nivelurilor de importanță și consecințelor care s-ar produce ca urmare a dezvăluirii sau diseminării neautorizate, trebuie să fie protejate;
- *clasele de secretizare* sunt secrete de stat și secrete de serviciu;
- *informații secrete de stat* – informațiile care privesc securitatea națională, prin a căror divulgare se pot prejudicia siguranța națională și apărarea țării;
- *informații secrete de serviciu* – informațiile a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat;
- *nivelurile de secretizare* se atribuie informațiilor clasificate din clasa secrete de stat și sunt:
 - *strict secret de importanță deosebită* – informațiile a căror divulgare neautorizată este de natură să producă daune de o gravitate excepțională securității naționale;
 - *strict secrete* – informațiile a căror divulgare neautorizată este de natură să producă daune grave securității naționale;
 - *secrete* – informațiile a căror divulgare neautorizată este de natură să producă daune securității naționale;
- *protecție juridică* – ansamblul normelor constituționale și al celorlalte dispoziții legale în vigoare, care reglementează protejarea informațiilor clasificate;
- *protecție prin măsuri procedurale* – ansamblul reglementărilor prin care emitenții și deținătorii de informații clasificate stabilesc măsurile interne de lucru și de ordine interioară destinate realizării protecției informațiilor;
- *protecție fizică* – ansamblul activităților de pază, securitate și apărare, prin măsuri și dispozitive de control fizic și prin mijloace tehnice, a informațiilor clasificate;

- *protecția personalului* – ansamblul verificărilor și măsurilor destinate persoanelor cu atribuții de serviciu în legătură cu informațiile clasificate, pentru a preveni și înlătura riscurile de securitate pentru protecția informațiilor clasificate;
- *certificate de securitate* – documentele care atestă verificarea și acreditarea persoanei de a deține, de a avea acces și de a lucra cu informații clasificate.

În lege, la art. 17 este prezentată lista informațiilor secrete de stat, iar în art. 19 cine sunt cei împuterniciți să atribuie unul dintre nivelurile de secretizare a informațiilor cu prilejul elaborării lor.

Legat de *informațiile secrete de stat*, în lege sunt stipulate următoarele reglementări:

- *instituțiile deținătoare de informații secrete de stat* poartă răspunderea *elaborării și aplicării măsurilor procedurale de protecție fizică și protecție* a personalului care are acces la informațiile din această categorie;
- *documentele* cuprinzând informații secrete de stat *vor purta pe fiecare pagină nivelul de secretizare*, precum și *mențiunea „personal”*, când sunt destinate unor persoane determinate;
- *autoritățile publice* care elaborează ori lucrează cu informații secrete vor întocmi un *ghid pe baza căruia se va realiza o clasificare corectă și uniformă a informațiilor secrete de stat*, în strictă conformitate cu legea;
- *persoanele autorizate* care copiază, extrag sau reproduc în rezumat conținutul unor documente secrete vor aplica pe noul document rezultat mențiunile aflate pe documentul original;
- *declasificarea ori trecerea la un nivel inferior* de clasificare este realizată de *persoanele sau autoritățile publice competente* să aprobe clasificarea și nivelul de secretizare a informațiilor respective;
- protecția informațiilor nedestinate publicității transmise României de alte state sau de organizații internaționale, precum și accesul la informațiile acestora *se realizează în condițiile stabilite prin tratatele internaționale sau înțelegerile la care România este parte*;
- *accesul la informații secrete de stat* este permis numai în baza unei autorizații scrise, eliberate de conducătorul persoanei juridice care deține astfel de informații, după notificarea prealabilă la Oficiul Registrului Național al Informațiilor Secrete de Stat.

În ceea ce privește *informațiile secrete de serviciu*, legea prevede:

- informațiile secrete de serviciu *se stabilesc de conducătorul persoanei juridice*, pe baza normelor prevăzute prin hotărâre a Guvernului;
- informațiile secrete de serviciu *vor purta pe fiecare pagină și mențiunea „personal”*, când sunt destinate strict unor persoane anume determinate;
- *dispozițiile privind accesul* la informațiile secrete de stat se aplică în mod corespunzător și în domeniul informațiilor secrete de serviciu;
- *neglijența în păstrarea informațiilor secrete de serviciu* atrage, potrivit legii penale, răspunderea persoanelor vinovate;
- *se interzice clasificarea ca secrete de serviciu a informațiilor* care, prin natura sau conținutul lor, sunt *destinate să asigure informarea cetățenilor asupra unor probleme de interes public sau personal*, pentru favorizarea ori acoperirea eludării legii sau obstrucționarea justiției.

Legea stabilește următoarele *obligații și răspunderi* privind încălcarea prevederilor asupra informațiilor secrete de stat:

- persoanele fizice cărora le-au fost încredințate informații clasificate sunt obligate să asigure protecția acestora, potrivit legii, și să respecte prevederile programelor de prevenire a scurgerii de informații clasificate;

- obligațiile persoanelor fizice se mențin și după încetarea raporturilor de muncă, de serviciu sau profesionale, pe întreaga perioadă a menținerii clasificării informației;
- persoana care urmează să desfășoare o activitate sau să fie încadrată într-un loc de muncă ce presupune accesul la informații clasificate va prezenta conducătorului unității un angajament scris de păstrare a secretului;
- autoritățile publice, precum și celelalte persoane juridice care dețin sau cărora le-au fost încredințate informații secrete de stat sau informații secrete de serviciu vor asigura fondurile necesare în vederea îndeplinirii obligațiilor care le revin, precum și luării măsurilor necesare privitoare la protecția acestor informații;
- răspunderea privind protecția informațiilor clasificate revine conducătorului autorității sau instituției publice ori altei persoane juridice deținătoare de informații, după caz;
- informațiile secrete de stat se transmit, se transportă și se stochează în condițiile stabilite de lege;
- este interzisă transmiterea informațiilor secrete de stat prin cablu sau eter, fără a se folosi mijloace specifice cifrului de stat sau alte elemente criptografice stabilite de autoritățile publice competente;
- încălcarea normelor privind protecția informațiilor clasificate atrage răspunderea disciplinară, contravențională, civilă sau penală, după caz;
- persoanele încadrate în serviciile de informații și siguranță sau ale armatei, aflate în serviciul relațiilor externe, precum și cele special însărcinate cu protecția informațiilor secrete de stat, vinovate de deconspirări voluntare ori de acte de neglijență care au favorizat divulgarea ori scurgerea informațiilor secrete, își pierd irevocabil calitatea.

Legea trebuie să fie aplicată având în vedere și reglementările stabilite prin *Standardele naționale de protecție a informațiilor clasificate*, aprobate prin *Hotărârea de Guvern 585/2002*. Standardele oferă garanții de securitate pentru informațiile naționale clasificate și pentru cele echivalente care fac obiectul acordurilor internaționale la care România este parte.

Hotărârea de Guvern 781/2002 privind protecția informațiilor secrete de serviciu

Aplicarea Hotărârii se face pe baza *Standardele naționale de protecție a informațiilor clasificate*, aprobate prin *Hotărârea de Guvern 585/2002*. Prin prevederile hotărârii, protecția informațiilor secrete de serviciu se aplică în ceea ce privește:

- clasificarea, declasificarea și măsurile minime de protecție;
- regulile generale de evidență, întocmire, păstrare, procesare, multiplicare, manipulare, transport, transmitere și distrugere;
- obligațiile și răspunderile ce revin conducătorilor autorităților și instituțiilor publice, agenților economici și altor persoane juridice;
- accesul cetățenilor străini, al cetățenilor români care au și cetățenia altui stat, precum și al persoanelor apatride la informații clasificate și în locurile în care se desfășoară activități, se expun obiecte sau se execută lucrări din această categorie;
- exercitarea controlului asupra măsurilor de protecție

În Hotărâre sunt prezentate *regulile de marcare, utilizare și accesare a informațiilor 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”;
- informațiile secrete de serviciu constituite în dosare, precum și cele legate în volume distincte se marchează pe copertă și pe pagina de titlu;
- evidența documentelor secrete de serviciu se ține separat de cea a documentelor secrete de stat și nesecrete, în registrul special destinat acestui scop;

- se interzice scoaterea din incinta unității deținătoare a informațiilor secrete de serviciu fără aprobarea conducătorului acesteia;
- funcțiile care presupun accesul la informații secrete de serviciu se stabilesc de către conducătorii unităților deținătoare;
- accesul personalului la informațiile secrete de serviciu este permis numai în baza autorizației scrise (pentru care este stabilit un model cadru de formulare), emisă de conducătorul unității;
- evidența autorizațiilor de acces la informații secrete de serviciu se ține centralizat de structura/funcționarul de securitate în Registrul pentru evidența autorizațiilor de acces la informații secrete de serviciu;
- sancțiunile contravenționale prevăzute în Hotărârea Guvernului nr. 585/2002 se aplică și în cazul nerespectării normelor ce privesc protecția informațiilor secrete de serviciu.

Legea 544/2001 privind liberul acces la informația de interes public

Potrivit legii, *informația de interes public* reprezintă orice informație care privește activitățile sau care rezultă din activitățile unei autorități publice sau instituții publice, indiferent de suportul, forma sau modul de exprimare a acesteia. Accesul la informație se realizează cu ajutorul compartimentelor specializate sau de informare și relații cu publicul sau prin persoanele desemnate cu atribuții în acest domeniu.

Prin *autoritate sau instituție publică* se înțelege orice autoritate sau instituție publică, precum și orice regie autonomă care utilizează resurse financiare publice și care își desfășoară activitatea pe teritoriul României, potrivit Constituției.

În conformitate cu prevederile legii, *sunt considerate informații publice*:

- actele normative privind organizarea și funcționarea autorităților sau instituțiilor publice;
- structura organizatorică, atribuțiile departamentelor, programul de funcționare și audiențe al instituțiilor;
- numele persoanelor din conducerea autorității sau instituției publice;
- coordonatele de contact;
- sursele financiare, bugetul și bilanțul contabil;
- programele și strategiile proprii;
- lista documentelor de interes public;
- lista categoriilor de documente obținute și/sau gestionate potrivit legii;
- modalitățile de contestare a deciziei autorității sau instituției publice, dacă persoana se consideră vătămată în privința dreptului de acces la informațiile de interes public;
- informațiile care favorizează sau ascund încălcarea legii de către o autoritate sau instituție publică nu pot fi incluse în categoria informațiilor clasificate și se constituie în informații de interes public;
- informațiile privind datele personale ale cetățeanului dacă afectează capacitatea de exercitare a unei funcții publice.

Nu intră în categoria informațiilor la care să aibă acces liber cetățenii următoarele:

- informațiile din domeniul apărării naționale, siguranței și ordinii publice, dacă fac parte din categoria informațiilor clasificate;
- informațiile privind deliberările autorităților sau cele care privesc interesele economice sau politice ale României, dacă fac parte din categoria informațiilor clasificate;
- informațiile privind activitățile comerciale sau financiare dacă publicitatea lor aduce atingere principiului concurenței loiale;
- informațiile cu privire la datele personale, potrivit legii;
- informațiile privind procedurile din timpul anchetelor penale sau disciplinare, dacă se periclitează rezultatul anchetei;

- informațiile privind procedurile judiciare, dacă aduce atingere asigurării unui proces echitabil ori interesului legitim al oricărei părți implicate în proces;
- informațiile a căror publicare prejudiciază măsurile de protecție a tinerilor.

Accesul la informațiile publice se realizează prin:

- afișare la sediul autorității sau al instituției publice;
- publicare în Monitorul Oficial al României;
- mijlocele de informare în masă;
- publicații proprii sau pe pagina de Internet a autorității sau instituției publice;
- consultare la sediul autorității sau instituției publice, în spații special amenajate.

**Legea 677/ 2001 privind protecția persoanelor
cu privire la prelucrarea datelor cu caracter personal
și libera circulație a acestor date**

Legea are ca scop garantarea și protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viața intimă, familială și privată, cu privire la prelucrarea datelor cu caracter personal și se aplică prelucrărilor de date cu caracter personal efectuate prin mijloace automate, precum și prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau sunt destinate să fie incluse în astfel de sisteme.

Legea se aplică:

- prelucrărilor de date efectuate în cadrul activităților desfășurate de operatori stabiliți în România;
- prelucrărilor de date efectuate în cadrul activităților desfășurate de misiunile diplomatice sau de oficiile consulare ale României;
- prelucrărilor de date efectuate în cadrul activităților desfășurate de operatori care nu sunt stabiliți în România, prin utilizarea de mijloace de orice natură situate pe teritoriul României, cu excepția 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 situații de excepție, fără acordul ei cu respectarea următoarelor reguli:

- datele personale sunt prelucrate cu bună-credință și în conformitate cu dispozițiile legale;
- datele personale sunt colectate în scopuri determinate, explicite și legitime;
- prelucrarea ulterioară a datelor personale se face în scopuri statistice, de cercetare istorică sau științifică, inclusiv a celor ce privesc efectuarea de notificări către autoritatea de supraveghere, precum și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute în normele ce reglementează activitatea statistică, cercetarea istorică sau științifică;
- datele sunt adecvate, pertinente și neexcesive prin raportare la scopul pentru care sunt colectate și prelucrate;
- datele sunt exacte, eventual actualizate. În situația datelor inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate, ele trebuie să fie șterse 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 menționată se face cu respectarea garanțiilor 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;
- apartenența sindicală;
- starea de sănătate sau viața sexuală.

Sunt supuse unor *reguli speciale de prelucrare* o serie de date cu caracter personal care au o semnificație deosebită pentru persoanele la care fac referire, respectiv:

- prelucrarea datelor cu caracter personal având funcție de identificare (cod numeric personal);
- prelucrarea datelor cu caracter personal privind starea de sănătate;
- prelucrarea datelor cu caracter personal referitoare la fapte penale sau contravenții (cele care fac referire la săvârșirea de infracțiuni ori la condamnări penale, măsuri de siguranță sau sancțiuni administrative ori contravenționale aplicate persoanei vizate).

Persoana vizată de prelucrarea datelor cu caracter personal trebuie să-și cunoască drepturile pe care le poate exercita, și anume:

- *dreptul de a fi informată* cu privire la identitatea operatorului, scopul prelucrării datelor, destinatarii sau categoriile de destinatari ai datelor și alte informații a căror furnizare este impusă prin dispoziția autorității de supraveghere, ținând 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, informații referitoare la scopurile prelucrării, categoriile de date avute în vedere și 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 și a oricărei informații disponibile cu privire la originea datelor, a informațiilor privind principiile de funcționare a mecanismului prin care se efectuează prelucrarea automată a datelor ș.a.;
- *dreptul de intervenție asupra datelor*, adică rectificarea, actualizarea, blocarea, ștergerea sau transformarea în date anonime a celor a căror prelucrare nu este conformă cu legea, în special a datelor incomplete sau inexacte;
- *dreptul de opoziție*, prin care persoana vizată are dreptul de a se opune, din motive întemeiate și legitime legate de situația sa particulară, ca datele care o vizează să facă obiectul unei prelucrări, cu excepția cazurilor în care există dispoziții legale contrare. De asemenea, persoana vizată are dreptul de a se opune, în mod gratuit și fără nici o justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, în numele operatorului sau al unui terț, sau să fie dezvăluite unor terți 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 privința persoanei, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalității sale, cum ar fi competența profesională, credibilitatea, comportamentul sau alte asemenea aspecte. De asemenea, persoana poate solicita reevaluarea oricărei alte decizii luate în privința sa, care o afectează în mod semnificativ, dacă decizia a fost adoptată exclusiv pe baza unei prelucrări de date care întrunește condițiile enumerate anterior;
- *dreptul de a se adresa justiției*, prin care orice persoană care a suferit un prejudiciu în urma prelucrării unei date cu caracter personal, efectuată ilegal, se poate adresa instanței competente.

Legea are prevederi exprese privind *confidențialitatea și securitatea prelucrărilor*. Astfel, orice persoană care acționează 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 instrucțiunilor operatorului, cu excepția cazului în care acționează în temeiul unei obligații legale.

De asemenea, operatorul este obligat să aplice măsurile tehnice și 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 rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

Pe lângă asigurarea confidențialității și securității prelucrărilor, legea stabilește *condițiile și categoriile de date cu caracter personal care pot fi transferate peste granițele țării.*

Legea 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției

Legea face parte din pachetul legislativ anticorupție aprobat de Guvern în anul 2003. Una din componentele importante pe linia securității sistemelor informaționale o constituie cea cuprinsă în *Titlul III al legii* cu privire la *prevenirea și combaterea criminalității informatice*, prin măsuri specifice de prevenire, descoperire și sancționare a infracțiunilor săvârșite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului și protecția datelor personale.

Potrivit legii, *autoritățile și instituțiile publice cu competențe în domeniu, în cooperare cu furnizorii de servicii, organizațiile neguvernamentale și alți reprezentanți ai societății civile* desfășoară următoarele activități:

- promovează politici, practici, măsuri, proceduri și standarde minime de securitate a sistemelor informatice;
- organizează campanii de informare privind criminalitatea informatică și riscurile la care sunt expuși utilizatorii sistemelor informatice.

De asemenea, *Ministerul Justiției, Ministerul de Interne, Ministerul Comunicațiilor și Tehnologiilor Informației, Serviciul Român de Informații și Serviciul de Informații Externe* au ca responsabilități:

- organizarea și actualizarea continuă a bazei de date privind criminalitatea informatică;
- efectuarea de studii periodice în scopul identificării cauzelor care determină și a condițiilor ce favorizează criminalitatea informatică;
- desfășurarea de programe speciale de pregătire și perfecționare a personalului cu atribuții în prevenirea și combaterea criminalității informatice.

În condițiile legii, sunt considerate *infracțiuni împotriva confidențialității și integrității datelor și sistemelor informatice* următoarele fapte:

- accesul, fără drept, la un sistem informatic;
- interceptarea neautorizată a unei transmisii de date care nu este publică și 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 conține date care nu sunt publice;
- modificarea, ștergerea sau deteriorarea datelor sau restricționarea 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 funcționării unui sistem informatic prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor sau prin restricționarea accesului la aceste date;
- producerea, vinderea, importarea, distribuirea sau punerea la dispoziție, sub orice altă formă, fără autorizare, a unui dispozitiv sau program informatic conceput sau adaptat în scopul săvârșirii de infracțiuni prezentate la punctele anterioare;

- producerea, vinderea, importarea, distribuirea sau punerea la dispoziție, sub orice altă formă, în mod neautorizat, a unei parole, cod de acces sau alte asemenea date care permit accesul total sau parțial la un sistem informatic, cu scopul săvârșirii de infracțiuni prezentate la punctele anterioare;
- tentativa producerii uneia din infracțiunile anterioare.

În ceea ce privește *infracțiunile informatice*, legea face referire la următoarele fapte:

- introducerea, modificarea sau ștergerea fără autorizare a datelor ori restricționarea accesului la aceste date, rezultând date necorespunzătoare adevărului, cu scopul producerii unei consecințe juridice;
- cauzarea unui prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ștergerea de date, prin restricționarea accesului la aceste date sau prin împiedicarea în orice mod a funcționării unui sistem informatic cu scopul obținerii unui beneficiu material pentru sine sau pentru altul;
- tentativa uneia din infracțiunile informatice precedente.

Legea 455/2001 privind semnătura electronică

Legea stabilește regimul juridic al semnăturii electronice și al înscrisurilor în formă electronică, precum și condițiile furnizării de servicii de certificare a semnăturilor electronice.

Într-o primă parte, legea oferă toate definițiile necesare înțelegerii și aplicării prevederilor legale privind:

- *datele în formă electronică* – reprezentări ale informației într-o formă convențională adecvată creării, prelucrării, trimiterii, primirii sau stocării acesteia prin mijloace electronice;
- *înscrisurile în formă electronică* – o colecție de date în formă electronică între care există relații logice și funcționale și care redau litere, cifre sau orice alte caractere cu semnificație inteligibilă, destinate a fi citite prin intermediul unui program informatic sau al altui procedeu similar;
- *semnătura electronică* – date în formă electronică, care sunt atașate sau logic asociate cu alte date în formă electronică și care servesc ca metodă de identificare;
- *semnatarul* – o persoană care deține un dispozitiv de creare a semnăturii electronice și care acționează fie în nume propriu, fie ca reprezentant al unui terț;
- *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 și/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 și/sau hardware configurate pentru a implementa datele de verificare a semnăturii electronice;
- *certificat* – o colecție de date în formă electronică ce atestă legătura dintre datele de verificare a semnăturii electronice și 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 și 6, înscrisul în formă electronică este asimilat, în ceea ce privește condițiile și efectele sale, cu înscrisul sub semnătură privată, având același efect ca actul autentic între cei care l-au subscris și între cei care le reprezintă drepturile. De asemenea, conform art. 7, în situația în care forma scrisă este cerută ca o condiție de probă sau de validitate a unui act juridic, un înscris în formă electronică îndeplinește această cerință dacă i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat și generată prin intermediul unui dispozitiv securizat de creare a semnăturii.

Legea stabilește condițiile de furnizare a serviciilor de certificare, obligația furnizorilor de a comunica autorității de reglementare și supraveghere specializată în domeniu toate informațiile referitoare la procedurile de securitate și de certificare utilizate, precum și orice intenție de modificare a lor, cu precizarea datei și orei la care modificarea intră în vigoare.

Furnizorul de servicii de certificare va asigura accesul la toate informațiile necesare utilizării corecte și în condiții de siguranță a serviciilor sale.

Persoanele fizice care prestează, conform legii, în nume propriu servicii de certificare, precum și personalul angajat al furnizorului de servicii de certificare, persoană fizică sau juridică, sunt obligate să păstreze secretul informațiilor încredințate în cadrul activității lor profesionale, cu excepția celor în legătură cu care titularul certificatului acceptă să fie publicate sau comunicate terților.

Autoritatea de reglementare și supraveghere specializată în domeniu și furnizorii de servicii de certificare au obligația să respecte dispozițiile legale privitoare la prelucrarea datelor cu caracter personal.

Furnizorii de servicii de certificare au obligația de a crea și de a menține un registru electronic de evidență a certificatelor eliberate, care trebuie să fie disponibil permanent pentru consultare, inclusiv în regim on-line.

De asemenea, sunt stipulate:

- mențiunile pe care trebuie să le conțină certificatul la eliberare;
- condițiile 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 desfășurării activităților legate de certificarea semnăturilor electronice;
- condițiile în care poate fi suspendată și încetează validitatea certificatelor eliberate;
- responsabilitățile autorității de reglementare și supraveghere;
- omologarea dispozitivelor securizate de creare și verificare a semnăturii electronice;
- modalitatea de recunoaștere a certificatelor eliberate de furnizorii de servicii de certificare străini;
- răspunderea furnizorilor de servicii;
- obligațiile titularilor de certificate;
- contravențiile și sancțiunile.

Legea 451/2004 privind marca temporală

Prin legea sus-menționată se stabilesc regimul juridic al mărcii temporale și condițiile de furnizare a serviciilor de marcă temporală.

În înțelesul legii, *marca temporală* este o colecție de date în formă electronică, atașată 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 marcă temporală. Mai precis, ea este un set de tehnici care permite oricărei persoane să identifice în mod exact momentul emiterii și semnării unui document electronic și care asigură asupra faptului că nimeni, nici măcar autorul documentului, nu a intervenit cu modificări după marcarea temporală a acestuia.

Alți termeni definiți de lege sunt:

- *amprenta atașată unui document electronic*, adică acea informație cu ajutorul căreia documentul poate fi identificat în mod unic, dar care nu permite deducerea conținutului documentului respectiv;
- *certificatul asociat mărcii temporale*, adică informația cuprinsă în marca temporală prezentabilă în formă inteligibilă și care conține cel puțin numele furnizorului de servicii de marcă temporală, numărul de ordine din registrul furnizorului și informația reprezentând momentul de timp;
- *baza de timp*, ca sistem unitar de referință temporală la care se raportează toți furnizorii de servicii de marcă temporală.

Marca temporală este formată din cel puțin următoarele elemente:

- *amprenta atașată documentului electronic supus marcării*;
- *data și momentul de timp* aferente documentului supus marcării, exprimate în timp universal;
- *informații care identifică în mod unic furnizorul* de servicii de marcă temporală;
- *numărul de ordine din registrul furnizorului* de servicii de marcă temporală.

Informațiile verificate la furnizorul de servicii de marcă temporală sunt:

- elementele de identificare ale certificatului relativ la cheia ce verifică marca;
- identificarea algoritmului utilizat pentru generarea amprenteii.

Marca temporală poate să conțină și elementele de identificare a solicitantului mărcii temporale.

Din punct de vedere tehnic, marcarea digitală este bazată pe semnături electronice și funcții hash. Cu ajutorul unei funcții hash se obține amprenta datelor originale, prin atașarea unui șir de biți individual fiecărui set de date în parte. Dacă datele sunt modificate, se modifică automat și amprenta care le-a fost atașată. Amprenta este trimisă furnizorului de servicii de marcă temporală, care îi atașează o dată și un moment din timp și calculează o nouă funcție hash. Rezultatul este criptat cu cheia privată a furnizorului de servicii și trimis solicitantului mărcii temporale. Cum datele originale nu pot fi extrase din amprenta trimisă autorității de marcă, ca urmare a modului de lucru într-o singură direcție a funcției hash, metoda asigură confidențialitatea lor.

Marca temporală garantează asupra faptului că documentul nu a fost creat sau modificat după data și ora cuprinse în amprenta digitală. Cel care dorește să verifice aplică din nou funcția hash datelor originale, atașează rezultatului marca temporală primită de la furnizorul de servicii de marcă și calculează un nou hash al șirului concatenat. Obține astfel un prim hash (A). Apoi, este decriptată, cu cheia publică a furnizorului, marca temporală emisă de acesta. Rezultatul obținut (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 *cerințe 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 marcă temporală au obligația de a crea și de a menține un registru electronic operativ de evidență 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 desfășurării activităților legate de marcarea temporală. Pe lângă acestea, furnizorii de servicii de marcă temporală mai au următoarele *obligații*:

- să mențină înregistrări ale mărcilor temporale emise pe o perioadă de 10 ani;

- să păstreze documentația aferentă algoritmilor și procedurilor de generare a mărcilor temporale emise;
- să asigure posibilitatea obținerii și 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 își întemeiază conduita pe efectele juridice ale respectivelor mărci temporale.

Legea 589/2004 privind regimul juridic al activității electronice notariale

Legea stabilește *regimul juridic al actelor notariale în formă electronică*, venind în completarea legilor privind semnătura electronică și marcare temporală.

Potrivit articolului 2, actele notariale în formă electronică instrumentate de notarul public trebuie să îndeplinească, sub sancțiunea nulității absolute, următoarele *condiții*:

- 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 conține informații privind biroul notarial, stabilite prin reglementări de către autoritatea de reglementare și supraveghere specializată în domeniu;
- să îndeplinească toate condițiile de fond prevăzute de lege privind operațiunea juridică pe care o consemnează.

Actele notariale în formă electronică au același regim juridic ca și actele notariale pe suport de hârtie. Valabilitatea în străinătate a actului notarial în formă electronică este stabilită prin convenții internaționale la care România este parte. Documentele în formă electronică provenind de la autoritățile 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 condițiile prevăzute la articolul 2 și atestarea locului unde s-au încheiat acestea;
- primirea și păstrarea în arhiva electronică a documentelor ce îndeplinesc condițiile prevăzute la articolul 2;
- legalizarea traducerilor în formă electronică;
- eliberarea de duplicate.

Pentru ca notarii publici să fie autorizați să efectueze acte notariale în formă electronică, ei trebuie să îndeplinească un set de condiții, dintre care majoritatea se referă la necesitatea de a *garanta securitatea serviciilor oferite de ei*. Astfel, utilizarea unui sistem informatic omologat este obligatorie, ca și emiterea de mărci temporale și semnături electronice pentru documentele întocmite. Legea obligă și la:

- angajarea, în cabinetul notarial, de personal cu cunoștințe de specialitate în domeniul tehnologiei semnăturii electronice și o practică suficientă în ceea ce privește procedurile de securitate corespunzătoare;
- adoptarea de măsuri de securitate împotriva falsificării actelor notariale în formă electronică;
- garantarea confidențialității în cursul procesului de generare și arhivare a acestora;
- păstrarea tuturor informațiilor 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 și primite de birourile notarilor publici, Camerele notarilor publici și Uniunea Națională a Notarilor Publici din România;
- utilizarea de sisteme omologate pentru arhivarea actelor notariale în formă electronică.

O autoritate de reglementare și supraveghere specializată va urmări modul în care furnizorii de servicii electronice notariale respectă cerințele de securitate stabilite prin lege.

În Ordinul ministrului privind normele tehnice și metodologice de aplicare a legii activității electronice notariale, sunt precizate, în mod concret, condițiile pe care trebuie să le îndeplinească notarul pentru a obține autorizația privind activitatea electronică. Prezentăm, din întregul set de cerințe, pe cele legate strict de sistemul informatic:

- asigurarea securității fizice;
- protecția antivirus;
- asigurarea unui mecanism de autentificare a utilizatorilor;
- asigurarea confidențialității și integrității comunicațiilor, a datelor recepționate, transmise și stocate,
- menținerea unei arhive electronice locale;
- menținerea unui registru automatizat de audit care va cuprinde evenimentele legate de utilizarea și administrarea sistemului informatic - aceste informații vor fi păstrate pentru o perioadă de cel puțin 10 ani și în arhiva de siguranță;
- accesul (eventual pe baze contractuale) la servicii calificate de arhivare electronică de siguranță, unde va fi păstrată o copie a fiecărui act electronic notarial efectuat, o copie a registrului electronic al notarului, precum și o copie a registrului de audit menționat la punctul anterior.

Hotărârea de Guvern 557/2006 privind stabilirea datei de la care se pun în circulație pașapoartele electronice, precum și a formei și conținutului acestora

Hotărârea de Guvern stabilește ca dată de punere în circulație a pașapoartelor electronice 1 ianuarie 2007. Pașaportul electronic este definit ca pașaportul diplomatic, pașaportul de serviciu sau pașaportul simplu, *în care se include un mediu de stocare electronică a datelor biometrice ale persoanei*. În înțelesul dat de Hotărâre, datele biometrice sunt *imaginea facială, impresiunea digitală, precum și orice alte date ale persoanei care pot fi introduse în mediul de stocare electronică*.

Responsabilitatea alegerii, prin licitație publică, a unui furnizor care să asigure confecționarea pașapoartelor electronice și a întregii infrastructuri aferente este atribuită Regiei Autonome „Administrația Patrimoniului Protocolului de Stat”, în colaborare cu Ministerul Administrației și Internelor și cu Ministerul Afacerilor Externe.

În anexele la Hotărâre, sunt precizate forma și conținutul pentru pașaportul electronic diplomatic, pașaportul electronic de serviciu și pașaportul electronic simplu. Acesta din urmă, de exemplu, pe lângă elementele fizice ale pașaportului „tradițional”, va conține fotografia titularului engravată laser și fotografia în umbră realizată prin perforație cu laser, ca și datele informatizate citibile optic și mediul de stocare electronică a datelor biometrice ale persoanei.

Ordinul Ministerului Finanțelor Publice 875/2001 pentru aprobarea Regulamentului privind operațiunile cu titluri de stat emise în formă dematerializată

Prin acest Ordin sunt specificate doar regulile specifice emisiunilor de titluri, fără să fie specificate obligațiile de asigurare a securității și protecției informațiilor ce decurg din utilizarea mediilor electronice de emisiune și decontare.

Singurele elemente la care se face trimitere în textul Ordinului și care au legătura cu dematerializarea emisiunii de titluri de stat sunt cele referitoare la condițiile minime pe care trebuie să le îndeplinească intermediarii pe piața primară sau secundară, respectiv:

- *dotări tehnice specifice activităților de tranzacționare*: echipamente informatice, echipament de suport informațional (Reuters, Telerate etc.), echipamente de comunicații specifice (linii telefonice, fax, telex, SWIFT etc.);

- *dotări tehnice specifice activității de custodie*: sisteme informatizate de evidență, gestiune și control, sisteme de baze de date securizate, sisteme de stocare și arhivare a informațiilor.

Ordinul Ministerului Comunicațiilor și Tehnologiei Informației 218/ 2004 privind procedura de avizare a instrumentelor de plată cu acces la distanță, de tipul aplicațiilor Internet-banking, home-banking sau mobile-banking

Ordinul se aplică *băncilor*, persoane juridice române, precum și sucursalelor din România ale băncilor, persoane juridice străine, și are ca obiect stabilirea procedurii privind eliberarea avizului Ministerului Comunicațiilor și Tehnologiei Informației asupra instrumentelor de plată cu acces la distanță tip Internet-banking, home-banking sau mobile-banking.

În primă fază, sunt prezentate *definițiile* pe care le dă Ordinul principalilor termeni din domeniu:

- *instrument de plată cu acces la distanță* - soluție informatică ce permite deținătorului să aibă acces la distanță la fondurile aflate în contul său, în scopul obținerii de informații privind situația conturilor și operațiunilor efectuate, efectuării de plăți sau transferuri de fonduri către un beneficiar, prin intermediul unei aplicații informatice, al unei metode de autentificare și al unui mediu de comunicație;
- *emitent* - banca autorizată de Banca Națională a României să emită instrumente de plată electronică și care pune la dispoziție deținătorului un instrument de plată electronică cu acces la distanță, pe baza unui contract încheiat cu acesta;
- *deținător* - persoana fizică sau juridică care, în baza contractului încheiat cu emitentul, deține un mecanism de autentificare în utilizarea instrumentului de plată cu acces la distanță;
- *utilizator* - deținătorul instrumentului de plată cu acces la distanță sau o persoană fizică recunoscută și acceptată de către deținător ca având acces la drepturile sale conferite de către emitent;
- *instrument de plată la distanță tip Internet-banking* - acel instrument de plată cu acces la distanță care se bazează pe tehnologia Internet (world wide web) și pe sistemele informatice ale emitentului;
- *instrument de plată la distanță tip home-banking* - acel instrument de plată cu acces la distanță care se bazează pe o aplicație software a emitentului instalată la sediul deținătorului, pe o stație de lucru individuală sau în rețea;
- *instrument de plată la distanță tip mobile-banking* - acel instrument de plată cu acces la distanță care presupune utilizarea unui echipament mobil (telefon, PDA - Personal Digital Assistant etc.) și a unor servicii oferite de către operatorii de telecomunicații;
- *plan de securitate* - document ce descrie totalitatea măsurilor tehnice și administrative care sunt luate de către emitent pentru utilizarea în condiții de siguranță a instrumentului de plată cu acces la distanță.

În articolul 3, se precizează că vor fi avizate pentru oferirea de instrumente de plată cu acces la distanță băncile al căror sistem informatic îndeplinește unele *cerințe minime de securitate*, referitoare la:

- confidențialitatea și integritatea comunicațiilor;
- confidențialitatea și nonrepudierea tranzacțiilor;
- confidențialitatea și integritatea datelor;
- autenticitatea părților care participă la tranzacții;
- protecția datelor cu caracter personal;
- păstrarea secretului bancar;
- trasabilitatea tranzacțiilor;
- continuitatea serviciilor oferite clienților;
- împiedicarea, detectarea și monitorizarea accesului neautorizat în sistem;

- restaurarea informațiilor gestionate de sistem în cazul unor calamități naturale, evenimente imprevizibile;
- gestionarea și administrarea sistemului informatic;
- orice alte activități sau măsuri tehnice întreprinse pentru exploatarea în siguranță a sistemului.

Articolul 4 stipulează că măsurile tehnice și organizatorice întreprinse pentru îndeplinirea cerințelor enumerate la articolul 3 vor fi în concordanță cu progresul tehnologic și cu riscurile potențiale.

Pe lângă alte documente necesare, pentru obținerea avizului, banca va trebui să prezinte:

- planul de securitate al sistemului informatic, semnat de către emitent, cuprinzând totalitatea măsurilor tehnice și organizatorice prevăzute pentru asigurarea cerințelor cuprinse la articolul 3 – structura planului este descrisă ulterior în Ordin;
- certificări din punct de vedere al securității asupra soluției informatice sau produselor conținute în aceasta, emise de organizații naționale sau internaționale recunoscute, acolo unde există;
- opinia de audit asupra planului de securitate și a soluției informatice prin intermediul căreia este oferit instrumentul de plată cu acces la distanță;
- o declarație în care este exprimată independența auditorului față de sistemul informatic auditat.

Regulamentul Băncii Naționale a României 6/2006 privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente

Regulamentul are ca *obiect* stabilirea principiilor privind emiterea și utilizarea instrumentelor de plată electronică pe teritoriul României, monitorizarea activității cu aceste instrumente, și a condițiilor care trebuie îndeplinite de bănci și de alți participanți la desfășurarea activității de plăți cu instrumente de plată electronică, indiferent de moneda în care sunt emise/denominate acestea.

După prezentarea principalilor termeni utilizați în decontările cu ajutorul instrumentelor electronice, a caracteristicilor generale ale cardurilor, condițiilor de desfășurare a tranzacțiilor, sunt prezentate toate drepturile, obligațiile și responsabilitățile emitentului instrumentului de plată și a băncilor acceptate, precum și ale deținătorului. Dintre acestea au fost selectate cele considerate importante pe linia protecției și securității tranzacțiilor și informațiilor implicate, după cum urmează:

- *emitentul va asigura și va răspunde pentru elemente de siguranță și de personalizare ale instrumentului de plată electronică, accesibile sau nu simțurilor ori cunoașterii comune, care să prevină falsificarea sau alterarea informației necesare și suficiente în efectuarea de plăți prin intermediul instrumentului de plată electronică, precum și limitarea efectelor cauzate de pierderea, furtul și distrugerea acestora, în scopul evitării producerii unor prejudicii și afectării încrederii în sistemele de plăți care operează cu instrumente de plată electronică;*
- *emitentul este responsabil pentru confecționarea materială a cardului și pentru informația necesară și suficientă pe care acesta trebuie să o conțină;*
- *emitenții și instituțiile acceptante au obligația să asigure liniile și echipamentele de comunicații și procesare, dispozitivele prin intermediul cărora se inițiază, se înregistrează, se controlează și se transmit informații și date aferente tranzacțiilor inițiate, precum și terminalele și locațiile unde acestea sunt amplasate, astfel încât acestea să prezinte un grad adecvat de siguranță operațională, în vederea prevenirii accesului neautorizat la acestea și protejării confidențialității, autenticității și integrității informațiilor și datelor în timpul procesării, stocării și arhivării datelor, inclusiv asigurarea unei utilizări facile a terminalelor;*

- *amplasarea terminalelor* trebuie să se facă în locuri care să asigure *siguranța* deținătorilor/utilizatorilor cardului sau ai instrumentului de plată de tip monedă electronică, *confidențialitatea* operațiunilor efectuate la acestea și *accesul tuturor deținătorilor/utilizatorilor*;
- *informațiile și datele transmise* băncii acceptante și, respectiv, emitentului în momentul plății *nu trebuie să prejudicieze* sub nici o formă *confidențialitatea operațiunii*;
- *informațiile* trebuie să se *limiteze strict* la cele *conținute*, de regulă, de *instrumentele de plată fără numerar pe suport hârtie*, respectiv *cecurile și ordinele de plată*;
- dacă *emitentul solicită autorizarea pentru un instrument de plată cu acces la distanță*, de tipul aplicațiilor *Internet-banking* sau *home-banking*, cererea va fi însoțită de toate avizele/certificările primite de la producătorul programului informatic aflat la baza aplicației, privind *nivelul de securitate al transmisiilor de date și protocolul de răspuns utilizat* în cazul apariției unor disfuncționalități în cadrul sistemului, precum și de avizul Ministerului Comunicațiilor și Tehnologiei Informației sau al altor entități indicate de acesta;
- prin organizarea activității lor de informare *emitentul și banca acceptantă răspund de identificarea, evaluarea și limitarea* producerii *efectelor fraudelor și activităților cu potențial de risc*;
- *emitentul va face dovada că informațiile și datele* obținute pe parcursul desfășurării *tranzacțiilor cu carduri nu sunt utilizate, schimbate, transmise sau vândute* decât în conformitate cu contractul încheiat între emitent și deținător sau comerciantul acceptant, pentru raportările către Banca Națională a României și către Oficiul Național de Prevenire și Combatere a Spălării Banilor sau în alte scopuri, conform legislației în vigoare.

Potrivit Regulamentului, este considerată *activitate frauduloasă* una din următoarele situații:

- utilizarea unui card pierdut;
- furtul cardului;
- emiterea și nerecepționarea cardului de către deținător;
- completarea unei cereri de eliberare a cardului în mod eronat sau fraudulos;
- utilizarea în cadrul tranzacțiilor a unui card contrafăcut;
- folosirea frauduloasă a cardului de către o persoană neautorizată;
- folosirea frauduloasă a numărului de cont al cardului în cadrul unei tranzacții;
- o altă fraudă identificată de banca acceptantă și efectuată la comerciantul acceptant.



Imaginați un caz de încălcare al unei legi dintre cele de mai sus. Imaginați un proces pe marginea respectivului caz, prezentând succint argumentele apărării și acuzării.

8.2 Protecția prin patente, copyright și mărci înregistrate

Alături de legislația ce se referă efectiv la protejarea datelor și informațiilor din sistemele de prelucrare automată a datelor, se va urmări și cadrul legal prin care sunt asigurate drepturile pentru protecția intelectuală.

Astfel, în majoritatea țărilor, legile privind protejarea proprietății intelectuale (patentele, copyright-ul și mărcile înregistrate), împreună cu legile privind secretul comercial, legea contractelor, sunt aplicate pentru a asigura și protecția software-ului, în general.

Patentele au rolul de a proteja conceptele industriale încorporate la realizarea soft-ului, în timp ce copyright-ul urmărește protejarea codului sursă sau a codului obiect care stă la baza produselor obținute. Marca de înregistrare pentru produsele informatice protejează „numele” sub care este realizat produsul, iar înregistrarea mărcii va preveni utilizarea însemnului de către alți producători pentru bunuri sau servicii similare.

S-a constatat că, în ultima perioadă, costul unui sistem este format, în proporție de aproape 2/3, din prețul mediu de achiziționare și instalare a soft-ului. Situația a fost mult amplificată de invadarea pieței calculatoarelor de către microcalculatoarele personale. Una din cele mai importante probleme ale pătrunderii soft-ului pe piață o constituie faptul că programele trebuie să fie accesibile cumpărătorilor diferitelor tipuri de echipamente și cărora trebuie să li se asigure o întreținere corespunzătoare. Din această cauză, dificultatea producătorului de soft, care realizează produse în serie mare și care sunt lansate pe diferite piețe, 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 piața 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 obținute de firme din vânzarea acestora, cu efecte vizibile asupra capacității de finanțare a activităților de cercetare și de investiții. De asemenea, publicul trebuie să știe faptul că prețul 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 discuțiilor, s-a stabilit că pentru industria informatică, care se confruntă cu dificultăți practice în includerea programelor informatice în categoria invențiilor, nu se justifică o abordare restrictivă a subiectelor ce pot fi puse sub jurisdicția patentelor.

Reglementările clarifică problemele legate de înscrierea sau nu cu drept de patent a combinației calculator-program. Astfel, un program informatic sau o înregistrare efectuată pe un suport nu sunt brevetabile prin conținutul lor. Pe de altă parte, dacă subiectul revendicat aduce contribuții noi, el nu poate fi exclus din categoria celor supuse patentului. De exemplu, noile programe de control al echipamentelor, al producției sau al proceselor ar putea fi privite ca potențiale 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 invențiile care pot lua forma unui program specific unui calculator. Potrivit acestora, furnizarea și încărcarea unor programe pentru care nu s-a obținut dreptul de folosire și care au dreptul de protecție 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 funcții 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, deși probează un anumit grad de noutate, să nu facă față testelor de probare a conținutului lor, atât timp cât pentru realizarea lor s-au folosit

algoritmi și 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 și primele programe de calcul tabelar au dreptul de a obține patentul.

Dintr-un anumit punct de vedere se consideră că patentele pentru invenții ce se bazează pe programe informatice sunt mai puțin valoroase decât în cazul altor produse. În cazul microprocesoarelor, acest lucru este în mod evident neadevărat, dacă invenția se concretizează într-un microprocesor care poate să facă față tuturor testelor ce se aplică unei invenții oarecare.

În cazul programelor este necesară dezvăluirea mai multor informații 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 și problema dificultății descoperirii încălcărilor legii privind programele informatice față de alte domenii de activitate, în care procesul realizării invențiilor poate fi supus unui control riguros prin intermediul patentelor (procesele chimice, domeniul telecomunicațiilor, 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 situație, un patent poate fi încălcat de către o persoană care concepe, la o perioadă de timp mai îndelungată, o invenție asemănătoare sau folosește idei și/sau elemente ale invenției originale, revendicându-și un drept de brevet pentru lucrarea sa.

De asemenea, programele mai pot fi protejate prin asigurarea distribuirii numai a codului-obiect și păstrarea secretului comercial de către distribuitori.

La respingerea includerii programelor informatice în categoria subiectelor de patente, s-a adus ca argument și perioada mare de timp care se scurge între momentul formulării cererii și cel al obținerii patentului, dacă se ține seama de rapiditatea schimbărilor din acest domeniu. Critica nu a fost lansată sistemului de patente, ci modului de derulare a procedurilor de obținere a acestora.

8.2.2 Copyright-ul

Copyright-ul își 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 și invenția”, guvernul britanic a propus câteva amendamente acestei legi.

Copyright-ul, ca nume, sugerează un drept de copiere, dar în mod normal el este înțeles 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 și înregistrarea unor date pentru obținerea 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 corporație înregistrată care își desfășoară activitatea pe teritoriul britanic și pe baza legilor engleze. Publicarea lucrării ce se constituie subiect de copyright nu este esențială pentru obținerea acestuia. Data publicării va afecta, totuși, termenul de copyright, care, în mod normal, este de 50 de ani de la sfârșitul 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 față de cel al patentelor, care se acordă pentru o perioadă de 20 de ani, sau de perioada nedeterminată a secretului comercial sau al confidențialității datelor, care, în cele mai multe cazuri, se stinge când subiectul ce a stat la baza confidențialității a fost făcut public.

Copyright-ul se aplică lucrărilor originale din domeniul literar, dramaturgiei, artei plastice. Drepturi speciale se acordă filmelor cinematografice, înregistrărilor audio și reclamelor. De asemenea, lucrările din industria informatică sunt asimilate lucrărilor literare și artistice. Astfel de lucrări sunt subiecte de copyright numai dacă își dovedesc originalitatea. Totuși, gradul de

originalitate cerut este nesemnificativ și este legat mai mult de creație decât de conceptul de noutate, cum este în cazul patentelor.

Protecția în cazul copyright-ului este acordată pentru conținutul formal sau expresia lucrării și nu pentru ideile pe care se bazează. Acest lucru este în contrast cu Legea Patentelor, în care protecția este acordată pentru conținutul de fond al invenției și nu pentru conținutul formal.

8.2.2.1 Copyright-ul și software-ul

La nivelul majorității țărilor dezvoltate s-au constituit organizații și instituții speciale care se ocupă de respectarea legislației privind copyright-ul. De exemplu, în Anglia de aplicarea prevederilor legale privind copyright-ul se ocupă Federația 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 justiție în cazul în care se dovedește încălcarea lui. De aceea, este deosebit de important ca proprietarii soft-ului să se asigure că și-au înregistrat produsele lor sub copyright;
- când soft-ul este realizat de către salariați ai firmei, care sunt și acționarii săi, ei pot obține, în mod automat, dreptul de copyright. Această regulă nu poate fi aplicată și simplilor salariați sau programatorilor angajați temporar;
- documentația originală, obținută în timpul realizării programului, trebuie să fie datată pentru a putea demonstra perioada în care a fost elaborat programul și pentru a proteja materialele literare legate de produs. Copyright-ul poate fi obținut chiar și pe baza acestei documentații, care poate să asigure posibilitatea de stabilire a unui drept de copyright firmei producătoare, cât și posibilitatea de a scoate în evidență faptul că produsul a fost realizat fără a încălca dreptul de copyright al altor produse;
- aducerea la cunoștința distribuitorilor și utilizatorilor programului că este un produs aflat în proprietatea cuiva. Acest lucru se poate realiza prin includerea unui marcaj nu numai pe documentație și manuale, ci chiar în program. Una din cele mai folosite notații este formată din simbolul © însoțit de numele proprietarului și anul primei publicări, în concordanță cu cerințele Convenției 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 și notația (C), sau poate fi scris efectiv cuvântul **Copyright**;
- detectarea și 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 aceeași 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, și care cu greu să poată fi identificate;
- stabilirea în contractele încheiate cu salariații a unor clauze prin care aceștia se obligă să respecte confidențialitatea informațiilor față de alți producători de produse similare sau față de clienți.

8.2.2.2 Marcarea copyright-ului

Există două convenții internaționale privind copyright-ul, respectiv Convenția BERNE și Convenția Universală a Copyright-ului, care au efecte în teritoriile țărilor semnatare ale acestora.

Protecția oferită în fiecare țară depinde de legea proprie a copyright-ului, iar convențiile stabilesc numai drepturile reciproce care se respectă între țările semnatare.

Legat de modul de marcarea a copyright-ului nu sunt cerințe stricte, dar potrivit prevederilor UCC, drepturile reciproce pot fi respectate dacă se folosește notația standard:

© *Proprietarul lucrării, anul primei apariții*

Simbolul poate să apară fie pe prima pagină a publicației, fie la sfârșitul paginii de titlu.

Problema care apare la introducerea notației nu se referă la publicații sau alte materiale, ci la includerea ei în cadrul software-ului. Se recomandă ca o notație să fie înregistrată astfel încât să fie vizibilă pentru utilizatori, iar o altă notație să fie citibilă numai pentru calculator. În acest sens, Oficiul Copyright din SUA a promulgat câteva recomandări pentru plasarea corespunzătoare a notației copyright. Astfel, pentru lucrările reproduse prin copii pe diferite suporturi de memorare, de pe care notația nu poate fi vizualizată decât cu ajutorul echipamentului, pot fi folosite următoarele metode de poziționare a simbolului:

- un simbol care să fie perceptibil la listare, fie în titlu, fie la sfârșitul lucrării;
- un simbol care să fie afișat 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, cartuș, 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-mașină, cu ajutorul translaatoarelor (asamblatoare, compilatoare), fiind considerat un comentariu al programului ar putea fi omis de la translare. De aceea, este necesar ca notația 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 notației copyright-ului, care să apară în format alfa-numeric ce va conține cele trei elemente ale notației (simbolul de copyright, numele autorului și anul primei apariții).

8.2.2.3 Protecția copyright-ului în România

În România prima lege care reglementează drepturile de autor și cele conexe a fost *Legea nr. 8/1996 privind dreptul de autor și drepturile conexe*, completată ulterior cu *Legea nr. 329 din 14 iulie 2006 privind aprobarea Ordonanței de Urgență 123 din 1 septembrie 2005 pentru modificarea și completarea Legii nr. 8/1996 privind dreptul de autor și drepturile conexe*.

Conform legii modificate și 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 creație, modul sau forma concretă de exprimare și independent de valoarea și destinația lor. În articolul 8, în categoria operelor derivate create plecând de la una sau mai multe opere preexistente sunt menționate și bazele de date – „care, prin alegerea ori dispunerea materialului, constituie creații intelectuale”.

Potrivit articolului 13 din Capitolul IV – *Conținutul dreptului de autor*, utilizarea unei opere dă naștere la *drepturi patrimoniale*, distincte și exclusive, ale autorului de a autoriza sau de a interzice:

- a) reproducerea operei;
- b) distribuirea operei;
- c) importul în vederea comercializării pe piața internă a copiilor realizate, cu conștientizarea 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 dispoziția publicului, astfel încât să poată fi accesată în orice loc și 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 vieții autorului, iar după moartea sa se transmit prin moștenire, potrivit legislației civile, pe o perioadă de 70 de ani.

În secțiunea IV *Contractul de închiriere*, articolul 63, se prevede că prin contractul de închiriere a unei opere, autorul se angajează să permită folosința, pe timp determinat, cel puțin 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 excepția dreptului de difuzare, dacă nu s-a convenit altfel.

Legea are un capitol distinct privind programele de calculator, unde sunt reglementate aspectele legate de protecția programelor, stabilind categoriile ce intră sub incidența legii, respectiv programele de aplicație și sistemele de operare, exprimate în orice fel de limbaj, fie în cod-sursă sau cod-obiect, materialul de concepție pregătit, precum și manualele.

Autorii programelor beneficiază de drepturile generale ale oricărui autor de opere, așa cum sunt stabilite în partea I a legii și enumerate mai sus, cu accentuare asupra dreptului exclusiv de a realiza și autoriza reproducerea, traducerea, difuzarea originalului sau copiilor unui program. O atenție 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 mulți angajați în exercitarea atribuțiilor de serviciu ori după instrucțiunile celui care angajează, aparțin *angajatorului*.

Legea oferă și detalii privind drepturile utilizatorilor programelor legate de realizarea arhivelor, copiilor de siguranță, testarea funcționării programului cu ocazia încărcării lui în sistem pentru care există autorizarea din partea autorului. Toate aceste acțiuni 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, prejudiciați 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 obținerea informațiilor necesare interoperabilității unui program pentru calculator cu alte programe, dacă sunt îndeplinite o serie de condiții:

a) actele de reproducere și de traducere sunt îndeplinite de o persoană care deține dreptul de utilizare a unei copii a programului sau de o persoană care îndeplinește aceste acțiuni în numele celei dintâi, fiind abilitată în acest scop;

b) informațiile necesare interoperabilității nu sunt ușor și rapid accesibile persoanelor prevăzute la litera a);

c) actele prevăzute la litera a) sunt limitate la părțile de program necesare interoperabilității.

Art. 79 specifică faptul că informațiile obținute prin aplicarea art. 78:

a) nu pot fi utilizate în alte scopuri decât la realizarea interoperabilității programului pentru calculator, creat independent;

b) nu pot fi comunicate altor persoane, în afara cazului în care comunicarea se dovedește necesară interoperabilității 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 fabricanților bazelor de date*.

Articolul 122 definește 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 și în mod individual accesibile prin mijloace electronice sau printr-o altă modalitate.

Prin fabricantul unei baze de date se înțelege persoana fizică sau juridică ce a făcut o investiție substanțială cantitativă și calitativă în vederea obținerii, verificării sau prezentării conținutului unei baze de date. Acestuia îi revine dreptul patrimonial exclusiv de a autoriza și de a interzice extragerea și/sau reutilizarea totalității bazei de date sau a unei părți substanțiale din aceasta, evaluată calitativ sau cantitativ. Fabricantul nu mai poate împiedica extragerea și/sau

reutilizarea normală, parțială sau totală a bazei de date dacă a pus-o, prin orice modalitate, la dispoziția publicului.

În același timp, însă, utilizatorul legitim al unei baze de date, care este pusă la dispoziția 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 prestații conținute în această bază de date.

Utilizatorului legitim al unei baze de date, care este pusă la dispoziția publicului prin orice modalitate, îi este permis, fără autorizarea fabricantului bazei de date, să extragă sau să reutilizeze o parte substanțială a conținutului acesteia în cazul în care utilizarea este:

- a) privată, iar baza de date neelectronică;
- b) pentru învățământ sau pentru cercetare științifică, cu condiția indicării sursei și în măsura justificată de scopul necomercial urmărit;
- c) în scopul apărării ordinii publice și a siguranței naționale ori în cadrul unor proceduri administrative sau jurisdicționale.

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 substanțială, evaluată calitativ sau cantitativ, a conținutului unei baze de date, constând, în special, în adăugări, suprimări sau schimbări succesive și pentru care se poate considera că s-a efectuat o nouă investiție substanțială, evaluată calitativ sau cantitativ, permite atribuirea unei durate de protecție proprii bazei de date rezultate din această investiție.

8.2.3 Protejarea mărcilor înregistrate

Un ajutor deosebit pentru piața calculatoarelor îl poate constitui alegerea unui nume edificator pentru produsul lansat. Un nume ușor de reținut și remarcabil poate fi mai mult decât o simplă receptare a produsului. El poate identifica programul cu un comerciant și poate asigura cumpărătorul sau licențiatul că i se oferă programul care să-i satisfacă cerințele așteptate. Din acest motiv, un nume poate determina obținerea unei imense valori comerciale, iar cel care-l distribuie va căuta să-și protejeze *good-will*-ul asociat acestui nume.

Cea mai eficientă metodă de protejare a unui nume atașat unui program constă în înregistrarea lui ca o marcă. Aceasta asigură recunoașterea statutară a mărcii ca proprietate atribuibilă și transmisibilă.

Ca formă a proprietății industriale, mărcile înregistrate au un mare avantaj față de brevete și copyright: pot fi obținute 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, consultațiile profesionale și serviciile de cercetare tehnică. În octombrie 1986 a luat ființă Serviciul de Înregistrare a Mărcilor.

8.2.4 Licențele

Deși, adesea, nu suntem conștienți de importanța acestui fapt, licențele sunt o parte a vieții noastre de zi cu zi. Aproape toți dintre noi avem o licență de conducere sau pentru TV. Fără îndoială că majoritatea produselor pe care le avem în casă (alimente, jocuri, mașini de uz casnic etc.) au o etichetă ce conține următoarele cuvinte „produs sub licență” (Manufactured under Licence) sau o frază similară. Este clar că licența nu se aplică numai calculatoarelor și soft-ului.

Licența are rolul de a asigura producătorul că nici o altă firmă nu va putea realiza produsele sale sub alt nume fără a obține acordul său, printr-un contract specific acestui gen de operațiuni.

Unele licențe derivă din legislația specifică unor activități pe care guvernele doresc să le controleze și/sau să-și asigure un venit din ele. De exemplu, licența TV își are originea în prevederile Legii telegrafiei din 1949 (Wireless Telegraphy Act). Altele se bazează pe legislația privind drepturile de proprietate intelectuală (IPR - Intellectual Property Rights).

Industria informatică poate fi considerată o industrie internațională; soft-ul poate fi transmis foarte ușor și rapid în întreaga lume, fie prin intermediul suporturilor de memorare, fie prin liniile de comunicații existente.

Problemele comerciale privind protecția unui program apar ori de câte ori este transferat peste granițele țării în care a fost realizat.

Legislația privind proprietatea intelectuală are un grad diferit de uniformitate în lume, dar care poate fi influențat prin convențiile internaționale. Totuși, uniformitatea legislativă în acest domeniu este mult mai mare față de legile specifice altor domenii.

Majoritatea țărilor industrializate recunosc că persoanei care cheltuie timp și bani pentru a realiza un program informatic trebuie să îi fie asigurată o anumită protecție împotriva utilizării neautorizate a programului său. Deși, așa cum am menționat anterior, legile nu oferă același nivel de protecție, efectele lor asupra informațiilor confidențiale, secretelor comerciale, concurenței nelociale sunt aproape aceleași.

De multe ori, se consideră mai eficientă asigurarea protecției prin licență a anumitor informații sau programe, decât prin păstrarea secretului lor de către o persoană sau un grup restrâns de persoane.

În general, prin legislația existentă, părților interesate într-un contract de licență li se oferă libertatea de a-și stabili termenii contractelor în funcție de necesitățile lor. Cu toate acestea, sistemul legal al țărilor tinde să stabilească anumite limite care să permită încadrarea termenilor contractuali într-o serie de norme economice și sociale.

Prevederile legislative privind tranzacțiile de bunuri și servicii, inclusiv comercializarea produselor informatice, se referă la condițiile de desfășurare a acestora, la calitatea produselor și la modul de etichetare a bunurilor, conform standardelor naționale și internaționale. Cu toate aceste măsuri, se întâlnesc numeroase cazuri de contrafacere a programelor prin copierea ambalajului și a etichetelor unui program original, astfel încât clientul este înclinat să creadă că a cumpărat un produs original.

În Marea Britanie, ca și în alte țări, există suficiente măsuri de contracarare a unor astfel de acțiuni, pe baza legilor comerciale.

8.2.4.1 Tipuri de licențe

Pot fi delimitate *cinci principale categorii de licențe*:

1. transferul drepturilor de licență;
2. licența simplă;
3. sistemul de închiriere sau leasing al programelor;
4. licența pe locul de utilizare a produsului (site licences);
5. licența liberă (free licences).

Transferul drepturilor de licență

În acest caz, proprietarul soft-ului transferă toate drepturile de licență unor persoane sau unei firme. Adesea, transferul se extinde și asupra proprietății asociate soft-ului, respectiv asupra copiilor, manualelor și a dreptului de a continua dezvoltarea și 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. Aceleași cerințe pot fi solicitate și de către programatorii angajați doar temporar de firmă, sau de o firmă care s-a angajat să realizeze un soft în numele alteia.

Trebuie însă reținut că în cazul în care prin contractul de transfer al licenței nu a fost inclusă o clauză ce prevede expres dreptul producătorului de a utiliza programul în cauză și în

realizarea altor aplicații, 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 și domeniile de activitate în care soft-ul poate fi utilizat.

Licența simplă

În această categorie de licențe, producătorul (sau agentul/distribuitorul său) vinde utilizatorului o copie a programului, dar își păstrează toate drepturile de proprietate.

Scopul licenței în acest caz poate fi explicat prin două aspecte.

În primul rând, operațiunile 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 și cazurile în care pot fi folosite copiile programelor. Astfel, unii consideră că ar fi normal ca pe baza unei copii cumpărate ei să-și poată realiza atâtea copii de câte au nevoie, mai ales în cazurile în care dispun de un sistem bazat pe o rețea 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 discuție, însă, în ceea ce privește publicarea manualelor tehnice.

Unii furnizori practică o politică fermă în ceea ce privește 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 defecțiuni ale mediului de lucru, utilizatorul va trebui să solicite furnizorului înlocuirea programului cu o altă copie. Pentru a-și asigura securitatea programului împotriva copierilor neautorizate, producătorii au inclus în programe unele sisteme anticopiere, deloc atractive pentru utilizatori.

Dezavantajul acestui tip de licență îl constituie faptul că utilizatorul s-ar putea trezi în situația de a nu-și mai putea actualiza soft-ul sau să-l înlocuiască în cazul defecțiunilor, 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, față de cea pasivă a altor produse, de exemplu a înregistrărilor audio.

Un utilizator urmărește să cumpere un program care să-i asigure o serie de facilități, care ar putea fi puse la dispoziție de un procesor de texte, un program grafic sau un program de contabilitate. Aceste facilități pot fi folosite în trei contexte diferite:

- în scop personal;
- pentru a realiza o activitate care nu este legată în mod special de facilitățile 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 și apelează la un furnizor pentru a-i pune la dispoziție una din componentele necesare, și 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 licențe o constituie faptul că furnizorul unui produs nu poate avea o legătură directă cu ultimul cumpărător, care poate avea și el o rețea de desfacere. De aici rezultă, în mod evident, necesitatea de a se stabili o legătură contractuală între producător și utilizatorul final, care implicit este considerat un contract de licență.

Marcajul licenței, care este mult mai detaliat decât notația copyright-ului, este inclus în ambalajul de plastic transparent al dischetelor, CD-urilor pe care programul este înregistrat. O etichetă exterioară atenționează cumpărătorul să nu rupă învelișul de plastic până nu a citit cu atenție și a acceptat condițiile de licență.

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 asistența și actualizarea permanentă a programelor. Condițiile de licență 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 licență pot să apară modificări ale aplicației și 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 convențional, licența este specificată pentru un utilizator și un calculator anume. Este necesar să fie stabilită perioada pentru care s-a încheiat contractul și dacă la sfârșitul acestei perioade furnizorul dorește să vândă produsul său. Uneori intervin dificultăți ca urmare a faptului că utilizatorul nu dorește să preia toate programele incluse în contractul de închiriere sau urmărește să-l descompună în mai multe subcomponente, care vor funcționa cu funcții bine stabilite.

Forma contractelor de licență 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 obținerea licenței, drepturile care se acordă utilizatorului produsului închiriat în ceea ce privește realizarea copiilor de siguranță, modificarea programului, utilizarea lui pentru obținerea unor produse similare din punct de vedere al funcționării sau în cadrul unor sisteme care nu sunt supuse licenței, în caz de urgență sau în cazurile în care pot fi necesare pentru derularea eficientă a diferitelor operațiuni.

Licența pe un loc de utilizare (site licences)

Unii licențiatori sunt dispuși să ofere unui utilizator o licență în termeni deosebit de favorabili în ceea ce privește copiile ce pot fi realizate pe baza programului ce constituie obiectul contractului de licență. În alte cazuri, se acordă substanțiale reduceri de prețuri dacă utilizatorul acceptă o singură copie a programului, cu condiția ca modificările sau actualizările ulterioare să fie suportate de el, astfel că pentru producător/distribuitor costurile administrative se reduc simțitor. Avantajul acestei licențe pentru cel care o acceptă constă în posibilitatea de a stabili fără acordul proprietarului momentul în care poate să-și modifice sistemul, pentru a-și asigura compatibilitatea cu noile programe achiziționate.

Licența acordată pentru mai multe copii ale unui program capătă noi semnificații în următoarele condiții:

- folosirea unor calculatoare similare (PC-uri sau stații de lucru) într-o singură unitate, în loc de un mainframe, care ar fi putut să ofere aceleași facilități de lucru;
- creșterea capacității și complexității sistemelor distribuite și a rețelelor.

Unii utilizatori sunt mai interesați în reducerea costului soft-ului, în timp ce alții urmăresc să obțină libertate în utilizarea programelor, astfel încât să-și asigure fără probleme continuitatea licenței și păstrarea înregistrării.

Licența liberă (free licences)

Sunt unele surse care asigură obținerea programelor fără a mai apela la licențe, cum sunt bibliotecile de programe, magazinele de calculatoare, grupurile de utilizatori, revistele și unele firme distribuitoare. Aceste programe sunt considerate de interes public sau sunt unele care prin prețul lor asigură acoperirea oricărui tip de pierdere. Nici un program de acest tip nu-l scutește 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 preț ce nu va include și o valoare a licenței, dar cumpărătorul va trebui să facă dovada existenței unui mediu de lucru adecvat și a timpului necesar introducerii instrucțiunilor de la tastatura sistemului său.

Programele sunt realizate, de cele mai multe ori, pe suporturi disponibile oricărui sistem de prelucrare a datelor, cu prețuri care acoperă și eventualele pierderi datorate de copierea neautorizată, precum și un drept de autor.

Acest tip de licență nu garantează și faptul că programul va funcționa pe orice tip de calculator sau că se vor obține rezultatele care sunt așteptate de utilizator.

8.2.4.2 Aspecte generale ale licențelor

Toate componentele dreptului de proprietate intelectuală, mai ales cele referitoare la produsele din domeniul informatic, sunt influențate de o serie de factori, dintre care mai importanți 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 dorința sau nevoia de utilizare a calculatoarelor de la copii de vârstă școlară, până la bunicile lor, care-și păstrează rețetele pe calculator. Este de presupus că nici nepoții și nici bunicile nu au vreo cunoștință despre drepturile de proprietate intelectuală și ce presupun ele. În consecință, ei nu-și vor da seama că folosind copii ale unor programe sau jocuri comit o ilegalitate privind încălcarea copyright-ului sau a altor forme de protecție. Ca urmare, industria informatică a reacționat în consecință, dar fiecare firmă în felul ei (unele dintre ele invadând piața calculatoarelor, altele încercând să-și asigure un grad cât mai ridicat de protecție a produselor lor).

La nivel general s-a căzut de acord că este necesară asigurarea securității privind sistemele informatice. Astfel, în Marea Britanie a fost introdus un amendament al Legii Copyright-ului și s-a creat, în 1984, Federația Împotriva Furtului de Software (*FAST - Federation Against Software Theft*), cu rol în educarea publicului, în general, și a utilizatorilor de calculatoare, în particular, în asigurarea protecției programelor prin lege și încurajarea respectării drepturilor legale ale producătorilor de soft.

Se crede, totuși, că prin activitățile 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 fațetele generale ale aspectelor proprietății intelectuale. Cum pot fi constrânși studenții să plătească drepturile de autor proprietarilor programelor, când profesorii lor folosesc sute de copii xerografiate din materiale cu drept de copyright, pentru uzul școlar? În al doilea rând, este destul de puțin probabil ca prin educație să se elimine pirateria „profesională”, deși potențialii cumpărători de produse de acest gen încep să devină mult mai circumspecți.

Mărimea pieței

Majoritatea piraților de soft și a imitatorilor sunt interesați în obținerea unui profit cât mai rapid și mai mare, prin producerea de copii ale unui produs și exploatarea altora. Extinderea pieței, care trebuie să satisfacă cerințele diferitelor tipuri de utilizatori, determină o creștere a cererii și, în consecință, o sporire a ofertei de produse, astfel că a devenit un domeniu deosebit de atrăgător și profitabil pentru producătorii-pirați, care și-au mutat domeniul de acțiune de la producerea de copii imitate ale casetelor audio la cel al produselor informatice.

În general, piratul nu dorește să se implice în acordarea vreunui sprijin cumpărătorilor programelor sale. El nu are adesea nici o pregătire tehnică sau informatică, esențială în oferirea unor astfel de servicii. Programele, de cele mai multe ori, nu sunt funcționale din cauza conversiilor neglijente sau a tehnicilor neadecvate de copiere, ceea ce determină din partea utilizatorilor depunerea de plângeri către diferitele magazine care-și oferă serviciile de întreținere. Dacă programul este contrafăcut, plângerile pot ajunge și la firmele producătoare, dar fără nici un rezultat.

Unii distribuitori de copii nelicențiate ale programelor originale, care sunt capabili să schimbe pachete de hard/soft pentru a crește rata profitului, pot să-și stopeze activitatea imediat ce simt că furnizorii lor au descoperit ceva. Este greu de înțeles 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 depistați.

Un alt exemplu de copiere cu „grijă” este cel în care utilizatorul obține o copie licențiată pentru un program general, cum este un procesor de texte sau un program de calcul tabelar, cu intenția ascunsă de a-l folosi pe un alt calculator decât pe cel căruia i s-a acordat dreptul de utilizare. Un caz similar apare și când el cumpără calculatoare similare cu cel pentru care i s-a acordat dreptul de utilizare a programului și cade în tentația de folosi atâtea copii ale programului câte are nevoie. Problemele apar nu numai la nivelul PC-urilor, ci și la nivelul mainframe-urilor, care necesită programe mai complexe. Deși au fost prinși de nenumărate ori în astfel de situații, utilizatorii refuză să accepte că ar fi făcut ceva ilegal.

Costul echipamentelor

Problema pachetelor de aplicații este legată de asigurarea continuității lor, de cele mai multe ori privind programele de salarii, de contabilitate etc. Programele achiziționate asigură utilizatorului o bază substanțială de pornire, deoarece aproape toate programele rulate în cadrul firmelor sunt rezultatul unei improvizații, prin adăugarea de noi facilități și prin simplificarea modului de utilizare a programelor existente.

Prețul programelor originale a fost determinat în cea mai mare măsură, în ultimul timp, în concordanță cu prețul echipamentului pe care se intenționează a se instala. Dar este puțin probabil că un utilizator va fi dispus să plătească un preț pentru o aplicație 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 și copii pirat. Iată și unul din motivele scăderii continue a costului echipamentelor în comparație cu creșterea gradului lor de performanță, mai ales ca urmare a presiunii exercitate de furnizorii de soft.

Sistemele distribuite și rețelele de calculatoare

Așa cum se știe, rețelele sunt definite, din punct de vedere al scopului lor, ca unități de prelucrare interconectate între ele, astfel încât să fie posibil transferul informațiilor. Un program, în acest caz, poate fi considerat ca fiind un grup de informații, transmisibil în sistemul rețea prin modul lui de realizare. Din această cauză, un program poate fi disponibil pentru întreaga rețea sau numai pentru un anumit număr de terminale.

Din punctul de vedere al acordării licențelor pot fi identificate mai multe tipuri de rețele, și anume:

- o rețea 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 rețea. Sistemul este folosit doar de salariații firmei sau de alte persoane care au autorizarea necesară utilizării lui. Pentru astfel de cazuri poate fi obținută o licență de loc (site licence) pentru programele care vor fi instalate în toată rețeaua prin achiziție sau prin închiriere. În aceste cazuri, termenii de încheiere a contractului de licență trebuie să se bazeze pe un anumit grad de încredere între licențiator și licențiat;
- un alt tip de rețea poate fi definit ca un sistem bazat pe subscrieri sau abonamente. Un exemplu tipic îl constituie bazele de date comerciale, ce conțin informații și programe protejate prin patente, informații despre o serie de decizii legale, proiecte, clienți etc. Oricine poate plăti un operator care să-i descopere parola sau instrucțiunile de utilizare a acestui sistem și de acces la baza de date prin intermediul liniilor telefonice sau a unui terminal. În general, programele în astfel de rețele sunt foarte bine protejate și nu pot fi accesate foarte ușor nici chiar de către abonat;

- o altă categorie de rețea este caracterizată printr-un grad mare de acces, adesea fiind folosită de către organizații mari, cum sunt universitățile, pentru a încuraja schimbul de informații. Sistemul poate fi destul de vulnerabil la un nivel minim de securitate a soft-ului, ca urmare a dorinței de a simplifica accesul utilizatorilor începători. Un potențial spărgător poate obține destul de ușor accesul prin simple tehnici de pătrundere în sistem sau prin descoperirea parolelor de la un terminal;
- sistemele mari de rețele sunt caracterizate de transferul datelor și/sau programelor între calculatoare situate în diferite țări. În aceste condiții pot să apară numeroase probleme legate de nivelurile diferite de protecție pe care le asigură țările. Legile privind licențele nu sunt uniforme; de aceea este necesar să se realizeze contracte de licențe separate în funcție de țara în care urmează a fi folosite programele.

Un alt domeniu al legislației se referă la nivelul de securitate națională garantat, libertatea de circulație a informațiilor și confidențialitatea datelor.

De asemenea, nu trebuie uitați nici factorii politici și economici, care pot influența foarte mult cadrul legal al protecției diferitelor componente informatice.

Proiectarea și producția asistată de calculator

Câteva dintre argumentele care au stat la baza asigurării protecției proprietății intelectuale a programelor și a ieșirilor obținute în urma prelucrării datelor și a utilizării programelor s-au bazat pe conceptul că prin sistem se asigură doar procesul de prelucrare a datelor de intrare pentru a obține informațiile de ieșire. Cu toate acestea, ieșirile dintr-un sistem de proiectare asistată de calculator reprezintă, direct sau indirect, proiectul unui obiect fizic. De multe ori, calculatoarele și programele folosite sunt o parte integrantă a procesului de producție.

Noua generație de sisteme de producție încearcă să integreze un grup cât mai mare de funcții de producție, ca și în cazul sistemelor care înglobează protocoalele standard ale rețelelor care asigură schimbul de informații între diferite unități.

De multe ori copierea ilegală este considerată de către producători drept o vânzare pierdută. Experiența zilnică arată că principalul motiv al efectuării de copii ilegale de către diferite persoane, altele decât „piratii profesioniști”, îl constituie comoditatea sau indiferența față 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 siguranță, va consulta cartea într-o librărie sau o bibliotecă și își va face câteva notițe. În acest caz nu se va cumpăra nici o copie a întregului document, ceea ce va determina o posibilă pierdere de profit față de cazul în care materialul ar fi fost cumpărat. Majoritatea editurilor au devenit conștiente de acest fenomen și au luat o serie de măsuri de înregistrare a unei mențiuni prin care se specifică că sunt autorizate doar copiile făcute în scopuri non-profit.

8.2.5 Măsuri tehnice de protecție a licenței software-ului

Din studiile efectuate, s-a ajuns la concluzia că măsurile privind protecția 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, pirătării sau utilizării neautorizate a produselor-program. Aceste măsuri, denumite măsuri tehnice de protecție, sprijină protecția oferită de copyright sau de alte drepturi de proprietate intelectuală producătorilor de soft sau editorilor de materiale privind soft-ul realizat.

Licența privind programele specifică ce clienți pot utiliza sau nu programul aflat sub licență. Principalele restricții 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 siguranță 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 configurație 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 documentații asociate.

Măsurile tehnice de protecție 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 licența necesară.

În perioada de început a utilizării microcalculatoarelor au fost foarte puține cazuri de încălcare a drepturilor producătorilor de soft. Acest lucru se datora mai ales faptului că multe programe specifice mainframe-urilor și minicalculatoarelor dispuneau de caracteristici care ofereau, în mod automat, un anumit nivel de protecție. Unele programe au fost realizate pentru a satisface cerințele unui singur client sau pentru o mică piață specializată, în care numărul clienților era destul de redus. În aceste cazuri, era puțin probabil ca un client autorizat să realizeze copii ale programului pentru un alt utilizator. Dacă, totuși, se întâmpla acest lucru, el putea fi foarte ușor descoperit de către producător, datorită numărului mic de utilizatori al unui astfel de program.

Aproape toate produsele-program standard necesită servicii de întreținere 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 deține codul-sursă al programului. De obicei, producătorii consideră codul-sursă ca fiind o informație confidențială a firmei producătoare. Deci, fără acces la codul-sursă, utilizatorul nu poate depista defecțiunea din program care generează erorile și nu va ști ce instrucțiuni 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 achiziționat de la persoane neautorizate (firme sau alți utilizatori). De cele mai multe ori, însă, utilizatorii caută să-și înregistreze sub licență programele achiziționate.

Aceste modalități de asigurare a protecției soft-ului sunt considerate ca metode implicite de protejare. Nu este cazul și pentru programele specifice microcalculatoarelor.

Ca urmare a exploziei calculatoarelor pe piața produselor informatice, copiile produselor program sunt identice pentru a putea fi folosite de miile de utilizatori pe configurații hard și sisteme de operare similare.

Toate sistemele de operare au făcută o copie de către operatorul de sistem, cu scopul de a asigura funcționalitatea 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 și alte servicii specifice miilor de utilizatori din țară și de pretutindeni. Mai concret, ei, în mod normal, oferă și sprijină aceste servicii prin intermediul unui lanț de distribuitori, care pot realiza copii ilicite și pot distribui soft în propriul lor folos. În majoritatea cazurilor, clienții nu intră în contact direct cu producătorul, ci cu intermediarii acestuia.

Mulți producători încearcă să-și verifice distribuitorii prin interzicerea realizării de copii ale programelor. În plus, ei oferă, pentru fiecare produs, o fișă de înregistrare ce va fi completată de către cumpărător, căruia i se cere să o returneze completată producătorului și nu distribuitorului, ca o condiție de a obține 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 clienții uită să trimită fișele, în timp ce alții nu primesc din start o astfel de fișă. Distribuitorul ar putea să reproducă produsul împreună cu documentația asociată, producătorul neavând o evidență a tranzacțiilor ilegale care au fost efectuate și nici a drepturilor lui de autor ce i s-ar fi convenit pentru produsele astfel vândute. Din punctul de vedere al unor producători, este mult mai eficient să se prevină sau să se depisteze acțiunile de copiere ilegală folosind metode de protecție tehnică proiectate cu scopul de a preveni copierea sau utilizarea neautorizată a produselor lor.

Alți producători au încercat să împiedice astfel de activități fără a interveni efectiv în program, ci prin realizarea unor manuale de utilizare și 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 protecție:

1. *măsuri pentru depistarea copierii și utilizării neautorizate a programelor*, care constau în includerea notației copyright-ului sau a altor observații în cadrul programului. Aceste notații vor fi afișate în momentul folosirii programului, astfel că operatorul va fi atenționat asupra dreptului de copyright al furnizorului și/sau a numelui cumpărătorilor autorizați 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 protecție, cum ar fi formatarea non-standard a discurilor și nesincronizarea biților. 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 deține un program specific de reîncărcare, înlocuind temporar sistemul de operare al clientului, în timpul operațiunii 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 conține 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. Prezența dispozitivului sau a unui număr va fi verificată permanent, iar în cazul în care acesta lipsește programul se va opri prin blocare.

Deși multe firme au inclus în strategiile lor și măsuri tehnice de protecție, ele afirmă că se confruntă în continuare cu pierderea de venituri din reproducerea neautorizată sau pirateria soft-ului.

Din studiile efectuate în Marea Britanie și SUA s-a ajuns la o serie de concluzii care converg spre a considera că problemele industriei informatice, în ceea ce privește asigurarea protecției drepturilor de proprietate intelectuală, sunt mult mai grave decât cele din alte sectoare industriale. Deși perceperea importanței problemelor este diferită de la o firmă la alta, se pare că majoritatea companiilor producătoare de soft sunt interesate și încearcă, pe cât le este posibil, să prevină și să descopere activitățile de copiere sau utilizare neautorizată a programelor sau pe cele de piraterie. Există, însă, unele firme care își motivează imposibilitatea de a face față pierderilor cauzate de concurență pe seama unor astfel de activități. Deci, pentru astfel de firme activitățile ilegale pot constitui o scuză destul de plauzibilă în fața publicului în ceea ce privește incapacitatea lor de a obține profit pentru produsele lor.



Dați exemple de încălcări ale dreptului de autor, mărcii înregistrate, patentelor și licențelor cu care v-ați întâlnit în viața reală sau în literatură.

Rezumat

Capitolul de față a avut rolul de a oferi informații privind reglementările legislative existente în România pe linia securității informațiilor, sistemelor informatice și spațiului 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, licențele și modalitățile de protejare a acestora.

ANU SE COPIA

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 Architecture: 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 informaționale contabile: cadru general*, Editura Polirom, Iași, 2001.
25. **Năstase, D.** – „Necunoscutele” ale izvoarelor istoriei românești, Extras din Anuarul Institutului „A. D. Xenopol”, XXX, Ed. Academiei Române, Iași, 1993.
26. **Oprea, D.** – *Premisele și consecințele informatizării contabilității*, Editura Graphix, Iași, 1995.
27. **Oprea, D.** – „Particularități ale securității sistemelor informatice bazate pe partajarea resurselor”, în *Tribuna Economică*, 13, 1995.

28. **Oprea, D.** – „Vulnerabilitatea securității 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.** – „Protecția fizică a sistemelor informatice”, I-IV, în *Tribuna Economică*, 39-42, 1995.
31. **Oprea, D.** – „Securitatea comunicațiilor”, I-II, în *Tribuna Economică*, 40, 43, 1996.
32. **Oprea, D.** – „Security Particularities of Information Systems”, in *Contributi allo studio della transizione dell'agricoltura rumena verso il mercator: aspetti strutturali, 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 și proiectarea sistemelor informaționale economice*, Editura Polirom, Iași, 1999.
36. **Oprea, D.** – *Managementul proiectelor: teorie și cazuri practice*, Editura Sedcom Libris, Iași, 2001.
37. **Oprea, D., Airinei, D., Fotache, M. (coord.)** – *Sisteme informaționale pentru afaceri*, Editura Polirom, Iași, 2002.
38. **Oprea, D., Meșniță, G.** – *Sisteme informaționale pentru manageri*, Editura Polirom, Iași, 2002.
39. **Patriciu, V.V., Pietroșanu-Ene, M., Bica, I., Cristea, C.** – *Securitatea informatică în Unix și Internet*, Editura Tehnică, București, 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 Falsifying Banknotes”, in *Optical Security and Counterfeit Deterrence Techniques 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. **Schwartz, 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 Architecture: 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.

Referințe 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: www.counterpane.com
55. Cyber Crime ... and Punishment? Archaic Laws Threaten Global Information: www.mcconnellinternational.com
56. Dice-Tech Jobs. 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.com
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. Protecția informațiilor clasificate: www.sri.ro/biblioteca_art_infclas.html
75. Rău, P. – Infracționalitatea 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 informațiilor în firmă*, Traducere Nicolae Ionescu Cruțan, 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

Cărți 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

ANU SE COPIA

**MINISTERUL EDUCAȚIEI AL REPUBLICII MOLDOVA
UNIVERSITATEA DE STUDII EUROPENE DIN MOLDOVA
FACULTATEA DE DREPT**

**NOTE DE CURS
DREPT INFORMAȚIONAL
(Ciclul I)**

**AUTOR:
Victoria Mihalaș
mg. în drept, lector. univ.**

*Aprobat la ședința Catedrei Drept public
din: 20.05.2013, proces-verbal Nr. 10*

*Examinat de Consiliul facultății de Drept USEM
la 24.05.2013, proces-verbal Nr. 5*

*Aprobat la ședința Senatului USEM
din: 01.07.2013, proces-verbal Nr. 9*

CHIȘINĂU – 2013

TEMA 1. Considerații generale privind Dreptul informațional

1. Bazele teoretice ale informației.
2. Premisele constituirii dreptului informațional
 - a) Informația și materia
 - b) Informația și statul
 - c) Informația și societatea. Societatea informațională

1. Bazele teoretice ale informației.

Însăși cuvântul „informație” este cunoscut din antichitate și provine de la cuvântul latin „informatio”, ce înseamnă explicare sau comunicare. Actualmente informația nu poate fi definită atât de simplu și se utilizează diferite definiții a noțiunii de informație.

Definiție: Informația este o reflectare a lumii reale sau inventate și prezentate prin intermediul simbolurilor și semnelor. Această definiție este prea filozofică și în prezent se folosesc definiții cu un sens mai îngust.

Definiție: Informația reprezintă cunoștințe care pot fi păstrate, prelucrate și transmise.

Noțiunea de informație este legată de obiectul sau fenomenul real sau inventat și elimină nedeterminarea acestuia reflectându-i esența în măsura necesară pentru realizarea scopului. Conform art.3 al Legii „Cu privire la informatizare și la resursele informaționale de stat”, nr.467-XV din 21.11.2003, informația reprezintă cunoștințe despre persoane, subiecte, fapte, evenimente, fenomene, procese, obiecte, situații și idei.

Totodată informația are o anumită formă: articol, mesaj, comunicare, film, pictură, desen tehnic, cântec, model matematic, semnal electronic, undă electromagnetică. Informația permanent se găsește în circulație și trece următoarele etape:

- 1) Perceperea informației
- 2) Prelucrarea informației
- 3) Transmiterea informației
- 4) Prezentarea informației

Perceperea informației – este un proces ce constă în acumularea cunoștințelor despre proprietățile, structura și interacțiunea obiectelor sau fenomenelor.

Prelucrarea informației – este un proces ce constă în analiza și sinteza informațiilor.

Transmisia informației – este un proces ce constă în transportarea informației de la un emițător către un receptor.

Prezentarea informației – este un proces ce constă în demonstrarea prin semne convenționale a caracteristicilor calitative și cantitative ale informației.

Informația poate fi caracterizată prin următorii parametri:

- Autenticitatea;
- Plinătatea;
- Actualitatea;
- Claritatea.

Definiție: Informația este autentică dacă ea reflectă corect fenomenul sau obiectul dat și duce la luarea unor decizii corecte.

Definiție: Informația neautentică se numește dezinformație.

Definiție: Informația este deplină dacă ea este suficientă pentru rezolvarea unor probleme.

Definiție: Informația este actuală dacă ea este disponibilă în timpul și locul potrivit.

Definiție: Informația este clară dacă ea este înțeleasă de consumator.

2. **Premisele constituirii dreptului informațional**

- a) Informația și materia
- b) Informația și statul
- c) Informația și societatea. Societatea informațională

Trăim o perioadă de mari îndrăzneli, de mari victorii ale genului uman. Nimeni nu mai este nedumerit în fața unor așa titluri ca: „Omul și planeta”, „Omul și cosmosul”, „Omul și informația”. Relația „societate-informație” este indisolubilă. Schimbul de informații reprezintă o categorie esențială în existența societății. Cea ce a fost diferit de la o etapă la alta a fost conținutul și intensitatea transferului de informații. Pe măsură ce informația s-a diversificat și mesajele au devenit mai complicate, mai determinate, mai numeroase în procesul de transfer s-au produs specializări, au intervenit forme noi de organizare și memorizare. În lumea contemporană, odată cu creșterea rolului științei în dezvoltarea societății, câmpul informației științifice s-a extins, ocupând un loc vast în sfera comunicării.

Mișcarea informațiilor în societate poate fi controlată și organizată, ajungându-se la ora actuală la rețele mari, la structuri informaționale. Stadiile societății sînt stadii ale procesului de informație. Savanții demonstrează că progresul societății este strîns legat de procesul informațional.

În Declarația Universală a Drepturilor Omului, articolul 19, se indică că „Orice om are dreptul la libertatea opiniilor și exprimării; ceea ce implică dreptul de a nu fi intimidat pentru opiniile sale și acela de a căuta, de a primi și de a răspîndi, fără considerații de frontieră, informații și idei prin orice mijloc de exprimare”. În contextul epocii contemporane abilitățile și modalitățile cele mai eficiente de a fi informat reprezintă un deziderat cu valoare socială prioritară. Problemele care vizează informația devin tot mai pregnant momente de referință în diverse rapoarte politice, economice, culturale ce tratează problemele globale ale umanității.

În conformitate cu Declarația de intenții semnată la Liublana în 2002, Decretul Președintelui Republicii Moldova Privind edificarea societății informaționale în Republica Moldova, Hotărârea Guvernului Republicii Moldova Despre aprobarea Politicii de edificare a societății informaționale în Republica Moldova din 2004, Republica Moldova și-a asumat responsabilitatea edificării societății informaționale, bazată pe principiile consfințite în Statutul ONU, în Declarația Universală a Drepturilor Omului și în Carta edificării societății informaționale globale de la Okinawa în 2000, orientată spre interesele cetățenilor întregii societăți. Edificarea societății informaționale „una din prioritățile naționale” (4) se bazează pe implementarea largă a tehnologiilor informaționale și de comunicații. Trecerea la societatea informațională constituie „unul din obiectivele strategice pentru următorii ani precum și una din etapele de tranziție pentru integrarea țării în Uniunea Europeană” (5). Acestea au servit drept bază conceptuală pentru elaborarea și aprobarea prin Hotărîrea Guvernului Republicii Moldova a Strategiei Naționale de edificare a societății informaționale – „Moldova Electronică” și planului de acțiuni.

Prin transpunerea în viață a Strategiei, RM va realiza „dreptul la comunicare și informare ca drept fundamental al cetățeanului, va asigura accesul universal la informații și cunoștințe tuturor categoriilor sociale”. Societatea informațională este o formă nouă a civilizației umane în care accesul egal și universal la informație în corelație cu o infrastructură informațională și de comunicare dezvoltată contribuie la dezvoltarea social-economică durabilă. În societatea informațională cunoștințele sînt recunoscute ca un factor esențial al dezvoltării. Societatea informațională este caracterizată prin sporirea rolului informației și cunoașterii, crearea unui spațiu informațional global capabil să asigure comunicarea informațională eficientă dintre membrii societății, accesul lor la resursele informaționale mondiale. Contribuția și rolul bibliotecii în edificarea societății informaționale sînt indispensabile în următoarele arii:

- infrastructura informațională
- accesul la informații

- capacitatea de edificare
- identitatea și diversitatea culturală
- diversitatea lingvistică și conținutul local.

Informația devine resursă publică de dezvoltare, gradul de utilizare a ei este comparabil cu cele ale utilizării resurselor tradiționale: energie, materie primă etc. Orice realizare nouă își are rădăcina în realizările anterioare, orice specialist pentru a se ridica pe o treaptă superioară se sprijină pe munca predecesorilor.

I. Newton spunea „dacă am văzut ceva mai departe decât alții, e din cauza că am stat pe umerii unor giganți”. Comunicarea științifică a evoluat în funcție de necesitatea materială a oamenilor de a acumula cunoștințe. În procesul acesta au fost parcurse mai multe etape succesive:

1. Prima revoluție informațională - înseamnă din punct de vedere istoric crearea limbajului articulat care a permis realizarea comunicării prin schimbul direct de informații dintre oameni.

2. A doua revoluție informațională – este marcată prin apariția scrisului și a permis posibilitatea de transfer informațional de la o generație la alta. Ca suport al scrisului s-au folosit diverse materiale: roci, argilă, fildeș, papirus, pergamentul, lemnul și hîrtia (China, 105). Scrisul a apărut simultan în mai multe părți ale lumii. Cea mai veche formă de scris este pictografia. Ea constă nu în desenul literelor ci în desenul obiectelor. Fiecare imagine reprezenta un cuvînt. (Exemplu: o broască, o pasăre, un șobolan și o săgeată). Scrisul pictografic a evoluat spre scrisul ideografic. Locul desenelor a fost preluat de ideograme ce se bazau pe judecăți. (exemplu: apa era reprezentată printr-o linie ondulată).

3. A treia revoluție informațională – a fost marcată de realizarea tiparului cu litere mobile din metal de J. Gutenberg. Prima carte tipărită de Gutenberg a fost Biblia (1450-1456). Toate cărțile tipărite între 1455 și 1500 se numesc incunabule (scutec de copil și leagăn).

4. A patra revoluție informațională - este marcată prin creșterea fără precedent a fluxului de informație științifică determinată de amplificarea și diversificarea surselor și mijloacelor de comunicare în masă. Analiza relației nou create între informația științifică și savantul, cercetătorul lumii contemporane, chemat să o amplifice, conferă cu adevărat „științei informării” un rol determinant în progresul unei societăți. . Cu vre-o câteva decenii în urmă majoritatea științelor erau separate prin granițe precise. Informarea specialistului se realiza cu mult mai ușor.

Obiectivele de referință

- să definească informația ca materie și să stabilească interacțiunea dintre informație și societate;
- să identifice premisele edificării societății informaționale în Republica Moldova;
- să argumenteze necesitatea edificării societății informaționale în Republica Moldova.

Subiectul 2. Obiectul de studiu și metodele dreptului informațional

1. Fundamentele obiective ale constituirii dreptului informațional.
2. Obiectul de studiu al dreptului informațional.
3. Baza metodologică a dreptului informațional.
4. Noțiunea și sistemul dreptului informațional.

1. Fundamentele obiective ale constituirii dreptului informațional.

Relațiile sociale sunt într-o continuă evoluție, astfel apar noi relații sociale care trebuiesc reglementate de lege. Unele din ele se încadrează în obiectul ramurilor de drept existente, devenind reglementate fie prin modificarea unor acte normative din domeniu, fie prin adoptarea unui act normativ nou, iar altele, pentru că reprezintă o categorie de relații sociale distinctă, necesită adoptarea unui cadru normativ complex și complet. În felul acesta se creează noi ramuri de drept. De altfel, criteriile principale de deosebire a ramurilor de drept îl reprezintă obiectul și metoda de reglementare.

Țin să evidențiez că nu crearea oficială a unei ramuri noi de drept este premisă pentru apariția unui obiect distinct de reglementare, ci anume aceste relații care au trăsături comune, care reprezintă o categorie distinctă și care necesită o reglementare amplă, sunt premisa pentru apariția unei noi ramuri de drept, aceste relații reprezentând obiectul de reglementare al ramurii de drept respective.

În ceea ce privește dreptul informațional, ca premisă pentru apariția acestei ramuri de drept a fost dezvoltarea progresivă a societății informaționale, relațiile din cadrul acestui domeniu presupunând necesitatea de a fi reglementate, acestea reprezentând obiectul de reglementare a dreptului informațional.

2. Obiectul de studiu al dreptului informațional.

Obiectul de reglementare a dreptului reprezintă acele relații sociale care sunt reglementate de normele juridice.

Obiectul de reglementare a dreptului informațional reprezintă relațiile sociale care apar în rezultatul colectării, stocării prelucrării sau difuzării informației și care sunt reglementate de normele juridice de drept informațional.

O mare parte din relațiile sociale astăzi sunt reglementate de normele juridice. Rămân nereglementate relațiile unde nu este considerată necesară intervenția statului pentru a le reglementa, pentru a stabili anumite limite, interdicții, pentru a prescrie un anumit comportament sau pentru a permite subiecților de drept să aleagă comportamentul lor, uneori prezentând câteva variante alternative.

3. Baza metodologică a dreptului informațional.

Prin prisma art.4 din Constituția Republicii Moldova, normele Declarației au devenit obligatorii pentru autoritățile de stat, demnitari și funcționari publici. Statul și-a asumat responsabilitatea de a nu atenta la drepturile și libertățile consfințite în Declarație, de a apăra persoana de eventualele abuzuri ale reprezentanților săi, desemnați la guvernare.

Un om poate fi cu adevărat liber atunci când, după Franklin Roosevelt, dispune de:

Libertatea cuvântului,

Libertatea conștiinței,

Libertatea de privațiunile material,

Libertatea de povara fricii.

Libertatea poate fi obținută dacă omul este informat și își cunoaște drepturile și libertățile, căile de obținere ale lor.

Legea Supremă a Republicii Moldova a stabilit un nou cadru constituțional în domeniul drepturilor omului, în general, și în domeniul libertăților mass-media și accesului la informație, în special. Constituanta legislativă a corelat normele constituționale în acest domeniu atât cu transformările democratice survenite în societate, cât și cu exigențele tratatelor internaționale la care Republica Moldova a devenit parte. Astfel, art. 32-34 din Constituție referitoare la libertatea opiniei și a exprimării, libertatea creației și dreptul la informație au fost corelate cu art. 19 din Declarația Universală a Drepturilor Omului, precum și cu art.19 din Pactul Internațional cu privire la drepturile civile și politice, care erau în vigoare pentru Republica Moldova la momentul adoptării Constituției.

4. Noțiunea și sistemul dreptului informațional.

Astăzi, sistemul integrat al resurselor informaționale de stat din cadrul Sistemului Național Informațional al Republicii Moldova reprezintă una din condițiile de bază pentru edificarea societății informaționale, un mecanism real pentru consolidarea unui stat de drept, care asigură calitatea procesului decizional, reprezintă “inima” prestării serviciilor informaționale de diverse nivele și tipuri, vectorul principal al stabilității social-economice, platforma pentru egalitate în educație și cultură, baza pentru securitatea statală și apărarea drepturilor omului.

Asigurarea accesului la resursele informaționale are loc prin următoarele mijloace:

- Accesarea datelor din registre prin intermediul tehnologiilor Web – SIC “Acces-Web”
- Vizualizarea datelor din registre prin intermediul dispozitivelor de tip Pocket PC și tehnologiilor GPRS – SIC AccesMobile
- Mecanisme standardizate de obținere a datelor din registrele informaționale bazate pe Web-Service – Interfața Unică de Obiecte (Common Object Interface).
- Acces public prin intermediul rețelei Internet - „Verifică Datele”.
- Acces la datele statistice din registre prin intermediul tehnologiilor Web – SIA „Statistica”

În conformitate cu art.23 al Legii “Cu privire la informatizare și la resursele informaționale de stat” nr.467 din 21.11.2003, Ministerul Tehnologiei Informației și Comunicațiilor îndeplinește, în numele Guvernului, funcția de posesor al resurselor informaționale de bază.

În conformitate cu art.12 al Legii cu privire la registre nr. 71 din 22.03.2007 și Hotărârii Guvernului nr.625 din 22.05.2008, Guvernul Republicii Moldova a atribuit ÎS “CRIS “Registru” funcțiile de deținător și administrator al resurselor informaționale de stat de bază, care sunt:

Registrul de Stat al Populației

Registrul de Stat al Unităților de Drept

Sistemul Informațional Național Geografic (SING)

Toate celelalte resurse și registre de stat fac parte la categoria „Resurse și Registre Informaționale de Stat departamentale”:

Registrul de stat al transportului (RST)

Registrul de stat al conducătorilor auto (RSCA)

Registrul resurselor și sistemelor informaționale de stat

Prestarea serviciilor informaționale prin intermediul SIC „Acces -web”

Accesul la informația din resursele informaționale de stat se efectuează în bază de contract, prin utilizarea software-ului specializat - Sistemul informațional de căutare (SIC) “ACCES-Web”:

- persoana fizică (*inclusiv cetățeni străini, cu domiciliul în Republica Moldova*) - numele, prenumele, patronimicul, data nașterii, numărul, seria, valabilitatea documentului de identificare al persoanei, numărul de identificare de stat – IDNP, imaginea grafică, etc.;
- persoana juridică - denumirea întreprinderii, adresa juridică, numărul de înregistrare, genurile de activitate, filialele și reprezentanțele, informația cu privire la reorganizarea întreprinderii, datele de identificare ale conducătorului sau fondatorilor etc.;
- unitatea de transport – caracteristicile tehnice ale autovehiculului, (*tipul UT, marca/modelul, culoarea, numărul de stat de înregistrare*), datele agregatelor (*numărul caroseriei, motorului, șasiului, codul VIN*), numărul și seria documentului de înmatriculare, posesorul, etc.

Obiectivele de referință

- să definească obiectul și metodele de studiere ale Dreptului Informațional;
- să delimiteze sfera de reglementare a Dreptului Informațional și să stabilească locul Dreptului Informațional în sistemul de drept al Republicii Moldova;
- să determine condițiile de apariție a dreptului informațional;
- să stabilească fundamentele și modul de organizare a societății informaționale ca cadru de existență a dreptului informațional;

TEMA 3. Izvoarele dreptului informațional și sistemul legislației informaționale

1. Izvoarele dreptului informațional.
2. Istoria dezvoltării legislației în domeniul informațional.
3. Structura legislației în domeniul informațional și locul legislației informaționale în sistemul legislativ al Republicii Moldova.

1. Izvoarele dreptului informațional.

Curtea Constituțională a definit noi drepturi fundamentale, care rezultă din dreptul la informație:

- dreptul persoanei de a fi informată prompt, corect și clar asupra măsurilor preconizate sau luate de autoritățile publice;
 - accesul liber la sursele de informație politică, științifico-tehnică, socială, culturală ș.a.
 - dreptul de a recepționa personal și în condiții bune emisiunile radiofonice și televizate.
- Au fost formulate și obligațiile constituționale ale statului în acest domeniu:
- asigurarea de către autoritățile publice a cadrului juridic necesar pentru difuzarea liberă și amplă a informației de orice natură;
 - asigurarea informării corecte a cetățenilor asupra treburilor publice și problemelor de interes personal;
 - favorizarea pluralismului în mass-media de stat și private prin obligarea acestora de a exercita informarea corectă a opiniei publice.

2. Istoria dezvoltării legislației în domeniul informațional.

Cadrul juridic este chemat să realizeze dreptul de proprietar asupra informației cu diferențierea proprietății organizațiilor de stat în organelor administrative; structurilor comerciale, datelor personale a cetățenilor.

La sfârșitul anilor 70 comunitatea internațională a formulat două principii, care au fost luate ca bază la crearea cadrului juridic a securității informaționale în mai multe țări și sunt următoarele:

- definirea hotarelor amestecului statului în viața personală a cetățenilor cu utilizarea sistemelor informatice;

- implementarea mecanismelor administrative de protecție a cetățenilor contra astfel de amestecuri.

Cu ajutorul normelor de drept în domeniul securității informaționale trebuie să fie realizate următoarele sarcini:

- referirea informației drept deschisă sau închisă;
- definirea drepturilor de acces la informații;
- definirea drepturilor persoanelor de răspundere în vederea atribuirii și modificării parafelor anumitor informații;
- modurile și procedurile de acces;
- modul de control, documentare și analiză a acțiunilor personalului
- responsabilitățile pentru neîndeplinirea cerințelor definite;
- demonstrarea vinovăției răufăcătorilor;
- pedepsirea vinovaților;

3. Structura legislației în domeniul informațional și locul legislației informaționale în sistemul legislativ al Republicii Moldova.

Totalitatea reglementărilor relațiilor din domeniul informațional arată încă odată spre existența unui obiect distinct de reglementare, și anume:

- Constituția RM art. 4, 5, 23, 30, 32, 33, 34, 40, 52, 54, 55, 117;
- Legea privind accesul la informație nr. 982, adoptată la 11.05.2000
- Declarația Universală a Drepturilor Omului, la care RM a aderat 1990, art. 1, 19, 20, 29
- Pactul internațional cu privire la drepturile economice, sociale și culturale, în vigoare pentru RM din 1993, art. 15, 16, 18;
- Pactul internațional cu privire la drepturile civile și politice, în vigoare pentru RM din 1993, art. 19, 20, 21;
- Convenția Internațională cu privire la Drepturile Copilului, în vigoare pentru RM din 25.02.1993, art. 13, 15, 16, 17, 29;
- Convenția internațională privind eliminarea tuturor formelor de discriminare rasială, în vigoare pentru RM din 25 februarie 1993, art.2, 5;

- Convenția pentru Apărarea Drepturilor Omului și a Libertăților Fundamentale, în vigoare pentru RM din 1 februarie 1998, art. 6, art.8, art. 10, art. 11, art. 14, art. 34, art. 35, art. 36, art. 37, art. 38, art. 39, art. 40, art. 41, art. 44, art. 52;

- Mai multe recomandări ale Consiliului Europei către Statele membre;

- Hotărâri ale Parlamentului în domeniu și alte acte normative adoptate în domeniu.

În ultimul timp, un subdomeniu al dreptului informațional, care este internetul, prezintă în ultimul timp mai multe probleme și indică spre mai multe lacune și lipse de reglementare.

Obiectivele de referință

- să definească noțiunea de izvor de drept informațional;

- să identifice premisele și particularitățile dezvoltării legislației informaționale;

- să stabilească structura legislației informaționale în vigoare și să stabilească locul legislației informaționale în sistemul legislativ al Republicii Moldova.

TEMA 4. Resursele informaționale

1. Conceptul resurselor informaționale.
2. Regimul juridic al resurselor informaționale.
3. Reglementarea juridică a unor categorii aparte de resurse informaționale

1. Conceptul resurselor informaționale

Pe fondul dezvoltării rețelei informatice globale, de către chiar participanții constanți la aceasta, s-a conturat un proces de autoreglementare, prin care membrii diferitelor sub-comunități electronice au convenit asupra unor coduri de conduită, mai mult sau mai puțin elaborate, independent de vreo obligație ce le-ar fi fost impusă prin lege. Cu toate acestea, complexitatea relațiilor sociale din Internet, riscul apariției unor fenomene generatoare de pericol social și de prejudicii, victimizarea unor categorii de persoane, precum și eficiența relativă a mijloacelor sancționatorii autoimpuse în cadrul comunităților de internauti, au constituit factori esențiali ai declansării unor demersuri legislative la nivel statal și internațional.

În primul planul preocupărilor de ordin normativ se înscrie, tot mai pregnant, problematica extrem de complexă, a conținuturilor din Internet. Aceasta, deoarece spațiul virtual este, prin esența lui, un loc de manifestare a libertății de exprimare, a libertății de a primi și transmite informații, reclamând observarea respectării unor reguli ce privesc îndeosebi limitele acestei libertăți fundamentale. Fiind vorba, în ultima instanță de un aspect de drept constituțional, este firesc să existe un interes de reglementare la nivelul statelor și, având în vedere natura globală a Internetului, o preocupare a acestora de a crea un cadru juridic adecvat și la nivel internațional.

Studiul de față este menit să pună în lumină tocmai mutațiile pe care noile tehnologii le generează în spațiul public, modificarea mentalităților, dezvoltarea unei anumite culturi a comunicării, gradul de toleranță față de conținuturile de idei traficate în Internet – elemente care, la rândul lor, influențează modul în care juristii înțeleg să se raporteze la libertatea de exprimare, în special din perspectiva dreptului constituțional și a dreptului penal.

În contextul problematicii conținuturilor din Internet, următoarele aspecte prezintă, actualmente, un interes cu totul special:

1. Pornografia adultă,
1. Pornografia infantilă

2. Rasismul si xenophobia
3. Insulta si calomnia
4. Instructiunile privind fabricarea materialelor explosive
5. Plangerile impotriva produselor comerciale
6. Modalitatile de diseminare a unor continuturi

Pornind de la terminologia utilizata in doctrina si practica juridica a altor state, intelegem ca, pentru analiza din cuprinsul prezentului studiu, sa utilizam notiunea de "continuturi negative", termen ce include atat continuturi prohibite expres de lege, dar si elemente aflate intr-o zona "gri", tot mai controversata, sau care, in orice caz, beneficiaza de tratamente juridice diferite de la o tara la alta, fara a putea fi totusi considerate continuturi acceptate social.

Studiul de fata nu are, desigur, pretentia de a epuiza o tematica atat de extinsa care, in dimensiunile sale de baza – doctrina, jurisprudenta si legislatie – cunoaste o dinamica permanenta pe plan international. El isi propune, in schimb, sa ofere o introducere in analiza subiectelor evocate mai sus, precum si a zonelor de interferenta cu acestea, in scopul familiarizarii teoreticienilor si practicienilor din Romania cu un fenomen juridic nou, deosebit de complex si sensibil.

2. Regimul juridic al resurselor informaționale.

Sistemul informațional integrat al organelor de drept (în continuare - SIIOD) constituie totalitatea mijloacelor software, hardware, informaționale, organizaționale, sistemelor de transmitere a datelor, tehnologiilor de utilizare a lor, normelor de drept și infrastructurii, destinate pentru susținerea informațională a activității organelor de drept. Ca rezultat al funcționării sistemului, se formează resursa informațională unică a organelor de drept din țară.

Resursa informațională a organelor de drept reprezintă o totalitate sistematizată de date despre evenimentele care au loc în sfera de ocrotire a normelor de drept. Resursa respectivă este parte integrantă a Resurselor informaționale de stat ale Republicii Moldova, și anume, ale segmentului "Administrarea și controlul de stat"

Noțiuni de bază

În prezenta Concepție se utilizează următoarele noțiuni și definiții:

integrarea sistemelor informaționale ale organelor de drept - unificarea sistemelor informaționale automatizate ale organelor de drept într-un sistem unic, administrarea fiecărui sistem fiind efectuată individual de către fiecare organ de drept, iar dirijarea metodică a acestora va fi efectuată coordonat, în modul stabilit;

3. Reglementarea juridică a unor categorii aparte de resurse informaționale

Spațiul informațional al SIIOD reprezintă ansamblul următoarelor resurse informaționale:

- Registrul informației criminalistice și criminologice;
- Registrul dosarelor judecătorești;
- Registrul procedurilor de executare;
- Registrul persoanelor reținute, arestate și condamnate;
- Registrul de stat al armelor;
- Registrul obiectelor păzite;
- Registrul accidentelor rutiere;
- Registrul dactiloscopic;
- Registrul infrastructurii organelor de drept.

Resursele și fluxurile informaționale

Fiecare din resursele informaționale formate din nou trebuie să fie descrise detaliat în Concepția corespunzătoare, cu indicarea funcțiilor sistemului care o formează, a obiectelor informaționale și identificării lor.

În afară de aceasta, SIIOD asigură accesul operativ la datele sistemelor automatizate care formează resursele informaționale de importanță statală:

Registrul de stat al populației conține date despre persoanele fizice și documentele care le-au fost eliberate;

Registrul de stat al unităților de drept conține date despre toate tipurile de organe de drept, inclusiv despre activitatea, documentele și ștampilele lor;

Registrul de stat al transportului conține date despre mijloacele de transport (inclusiv agregatele cu număr) și documentele de înmatriculare;

Registrul de stat al conducătorilor de vehicule conține date privind dreptul persoanei fizice de a conduce mijlocul de transport corespunzător;

Registrul de stat al blanchetelor de strictă evidență și al timbrelor de acciz oferă date despre blanchetele de strictă evidență și timbrele de acciz confecționate și despre circulația lor;

Registrul vamal de stat conține date despre mărfurile și alte obiecte deplasate peste frontiera de stat;

Registrul Serviciului Grăniceri conține date despre traversarea frontierei de stat de către persoanele fizice și unitățile de transport;

Sistemul informațional geografic național servește pentru stabilirea spațială a datelor despre locurile comiterii infracțiunilor și obiectele infrastructurii, de asemenea, oferă posibilitatea de aplicare a metodelor de analiză spațială a evenimentelor și fenomenelor care au loc în sfera criminală.

Obiectivele de referință

- să delimiteze categoriile de resurse informaționale;
- să analizeze raportul dintre resursele informaționale de stat și cele cu caracter privat;
- să explice nivelul de intervenție a statului în reglementarea raporturilor sociale obiect al cărora sunt resursele informaționale;
- să formuleze opinii asupra reglementării juridice a unor categorii aparte de resurse informaționale.

TEMA 5. Dreptul la acces la informație

1. Drepturile și libertățile informaționale de bază, temeuri și restricții.
2. Dreptul de acces la informație.
3. Reglementarea juridică a dreptului la informației.
4. Semnătura electronico-digitală ca instituție a dreptului informațional.
5. Protecția dreptului de acces la informație

1) Drepturile și libertățile informaționale de bază, temeuri și restricții

Într-un stat constituțional oricare tip de activitate trebuie să fie reglementat. Din păcate, asigurarea legislativă a relațiilor informaționale în Republica Moldova lipsește, iar această domeniu a legislației este “terra incognita” pentru organele legislative din țară.

Într-o societate contemporană informația deține un rol important, iar resursele informaționale sunt una dintre cele mai importante active ale statului, de rând cu resursele naturale, umane, financiare, etc. și definesc potențialul lui.

Crearea societății contemporane informațională în Republica Moldova necesită rezolvarea unui complex de sarcini în vederea formării mediului informațional, care ar asigura dezvoltarea eficace a sistemelor informatice și a rețelelor de transfer a datelor, formarea resurselor informaționale, elaborarea produselor informaționale, prestarea serviciilor informaționale, pregătirea cadrelor în acest domeniu, etc.

În 1946, Adunarea Generală a Națiunilor Unite a adoptat una dintre primele sale rezoluții, în care se spune: “Libertatea de informare este un drept fundamental al omului și... piatra de încercare a tuturor libertăților cărora Națiunile Unite le sunt credincioase”.

Este o afirmație foarte generală. Ce credeți că a vrut să spună ONU prin această rezoluție?

Având în vedere că liberul acces la informație este considerat un drept al omului atât de important, faptul că el nu este formulat mai clar în standardele internaționale ale drepturilor omului ar putea fi surprinzător. Textul Articolului 19 din Declarația Universală a Drepturilor Omului este clar și fără echivoc:

“Toți oamenii au dreptul la liberă opinie și exprimare; acest drept înseamnă libertatea de a-ți exprima nemijlocit propria opinie și de a căuta, primi și comunica o informație din orice mijloc și indiferent de frontiere” (“sublinierea noastră”).

Deși libera exprimare pare benefică atât pentru cei “care comunică informația”, cât și pentru cei care o primesc, ideea potrivit căreia cetățenii au dreptul să obțină informații de la instituțiile guvernamentale nu era unanim recunoscută la acea vreme. Suedia avea garantată în Constituție libertatea informației începând din 1776, dar ea încă se înscria într-o minoritate.

Scriitorul american Walter Lippmann afirmase că un oficial ales nu răspunde decât în fața instituției sale, nu și în fața electoratului: “Acolo unde guvernul este dominat de opinia maselor, funcțiile puterii sunt grav afectate”. În mod asemănător, sistemul britanic al democrației parlamentare se baza pe principiul conform căruia numai legislativul putea monitoriza guvernul, nu și publicul. În viziunea lui Walter Bagehot, principalul teoretician al guvernării parlamentare britanice, democrația nu putea funcționa decât “dacă guvernării nu trebuie să dea socoteală vulgului”.

Acestea erau concepțiile încă predominante în majoritatea cercurilor guvernamentale din anii '40. (Ca să fim cinstiți, aceste concepții sunt larg răspândite și astăzi). Iată de ce textul Rezoluției Adunării Generale a ONU a însemnat o rupere atât de radicală de trecut. Să ni-l reamintim:

“Libertatea de informare este un drept fundamental al omului și... piatra de încercare a tuturor libertăților cărora Națiunile Unite le sunt credincioase”.

Poate că acesta este primul lucru la care se gândește cineva atunci când aude cuvintele “liber acces la informații”. Guvernele, ca și alte instituții cu putere de decizie, cum ar fi companiile comerciale, dețin informații despre toți locuitorii țării. Aceste informații sunt de la cele mai simple – locul nașterii unei persoane, adresa acesteia – până la cele mai complexe, cum ar fi cele medicale.

Cantitatea și complexitatea informațiilor deținute a crescut o dată cu dezvoltarea tehnologiei. Astfel, computerizarea documentelor guvernului și companiilor face mult mai ușor schimbul de informații între diverse categorii de documente.

Nimic înfricoșător în capacitatea propriu-zisă a guvernelor de a deține informații. Dacă guvernele nu ar deține astfel de informații, ele nu ar putea să ofere publicului serviciile așteptate și nici nu ar înțelege drepturile fiecăruia. De exemplu, oamenii ar fi nemulțumiți dacă li s-ar spune că nu pot vota la alegerile viitoare pentru că autoritățile electorale nu i-au înregistrat.

La fel, cineva s-ar putea îngrijora dacă, atunci când vine să extragă bani din cont, ar constata că banca nu îi are contul înregistrat. Așadar, este normal ca o instituție să dețină date despre persoane, pentru că numai așa o societate poate funcționa normal.

Și, totuși, ceva îi îngrijorează pe oameni: teama că “Big Brother” știe prea multe despre viața lor de zi cu zi. Deseori, această teamă este justificată. Mai întâi, există un motiv de ordin practic pentru care oamenii sunt îndreptățiți să știe ce informații dețin autoritățile despre ei. Un alt motiv ar fi acela că oamenii trebuie să aibă posibilitatea să cunoască aceste date și, dacă sunt eronate, să le poată corecta. Dar chiar dacă nu ar exista un motiv pur practic pentru accesul la informații, oamenii tot trebuie să aibă dreptul elementar de a le afla.

Conform tratatelor internaționale pentru drepturile omului, dar și potrivit legislațiilor naționale, individul are dreptul la viață privată. Accesul la informare este unul din mijloacele prin care un individ se poate asigura că dreptul la viață privată îi este respectat.

Guvernele și celelalte instituții dețin multe informații care pot afecta bunăstarea individului ca membru al societății, chiar dacă aceste informații nu se referă la el în mod direct.

Vă puteți gândi la anume tipuri de informații deținute de guvern, pe care o persoană ar trebui să le cunoască?

Există multe tipuri de informații deținute de guvern, care afectează viața individului. Ele se pot înscrie în oricare dintre categoriile următoare (sau în multe alte categorii):

- politică;- viață socială;- sănătate;- educație;- mediu;- planuri de investiții;- securitate;- justiție.

În toate aceste domenii, individul, ca cetățean, are diverse drepturi. Dacă nu primesc informații exacte despre activitatea guvernului în aceste domenii, atunci oamenii nu își pot exercita drepturile pe deplin.

2) Dreptul de acces la informație

În 1946, Adunarea Generală a Națiunilor Unite a adoptat una dintre primele sale rezoluții, în care se spune: “Libertatea de informare este un drept fundamental al omului și... piatra de încercare a tuturor libertăților cărora Națiunile Unite le sunt credincioase”.

Este o afirmație foarte generală. Ce credeți că a vrut să spună ONU prin această rezoluție?Ce înțelegem prin liberul acces la informație?

Având în vedere că liberul acces la informație este considerat un drept al omului atât de important, faptul că el nu este formulat mai clar în standardele internaționale ale drepturilor omului ar putea fi surprinzător. Textul Articolului 19 din Declarația Universală a Drepturilor Omului este clar și fără echivoc:

“Toți oamenii au dreptul la liberă opinie și exprimare; acest drept înseamnă libertatea de a-ți exprima nemijlocit propria opinie și de a căuta, primi și comunica o informație din orice mijloc și indiferent de frontiere” (“sublinierea noastră”).

Deși libera exprimare pare benefică atât pentru cei “care comunică informația”, cât și pentru cei care o primesc, ideea potrivit căreia cetățenii au dreptul să obțină informații de la instituțiile guvernamentale nu era unanim recunoscută la acea vreme. Suedia avea garantată în Constituție libertatea informației începând din 1776, dar ea încă se înscria într-o minoritate.

Scriitorul american Walter Lippmann afirmase că un oficial ales nu răspunde decât în fața instituției sale, nu și în fața electoratului: “Acolo unde guvernul este dominat de opinia maselor, funcțiile puterii sunt grav afectate”. În mod asemănător, sistemul britanic al democrației parlamentare se baza pe principiul conform căruia numai legislativul putea monitoriza guvernul, nu și publicul. În viziunea lui Walter Bagehot, principalul teoretician al guvernării parlamentare britanice, democrația nu putea funcționa decât “dacă guvernării nu trebuie să dea socoteală vulgului”.

Acestea erau concepțiile încă predominante în majoritatea cercurilor guvernamentale din anii '40. (Ca să fim cinstiți, aceste concepții sunt larg răspândite și astăzi). Iată de ce textul Rezoluției Adunării Generale a ONU a însemnat o rupere atât de radicală de trecut. Să ni-l reamintim: “Libertatea de informare este un drept fundamental al omului și... piatra de încercare a tuturor libertăților cărora Națiunile Unite le sunt credincioase”.

Poate că acesta este primul lucru la care se gândește cineva atunci când aude cuvintele “liber acces la informații”. Guvernele, ca și alte instituții cu putere de decizie, cum ar fi companiile comerciale, dețin informații despre toți locuitorii țării. Aceste informații sunt de la cele mai simple – locul nașterii unei persoane, adresa acesteia – până la cele mai complexe, cum ar fi cele medicale.

Cantitatea și complexitatea informațiilor deținute a crescut o dată cu dezvoltarea tehnologiei. Astfel, computerizarea documentelor guvernului și companiilor face mult mai ușor schimbul de informații între diverse categorii de documente.

Nimic înfricoșător în capacitatea propriu-zisă a guvernelor de a deține informații. Dacă guvernele nu ar deține astfel de informații, ele nu ar putea să ofere publicului serviciile așteptate și nici nu ar înțelege drepturile fiecăruia. De exemplu, oamenii ar fi nemulțumiți dacă li s-ar spune că nu pot vota la alegerile viitoare pentru că autoritățile electorale nu i-au înregistrat.

La fel, cineva s-ar putea îngrijora dacă, atunci când vine să extragă bani din cont, ar constata că banca nu îi are contul înregistrat.

Așadar, este normal ca o instituție să dețină date despre persoane, pentru că numai așa o societate poate funcționa normal.

Și, totuși, ceva îi îngrijorează pe oameni: teama că “Big Brother” știe prea multe despre viața lor de zi cu zi. Deseori, această teamă este justificată. Mai întâi, există un motiv de ordin practic pentru care oamenii sunt îndreptățiți să știe ce informații dețin autoritățile despre ei. Un alt motiv ar fi acela că oamenii trebuie să aibă posibilitatea să cunoască aceste date și, dacă sunt eronate, să le poată corecta. Dar chiar dacă nu ar exista un motiv pur practic pentru accesul la informații, oamenii tot trebuie să aibă dreptul elementar de a le afla.

Conform tratatelor internaționale pentru drepturile omului, dar și potrivit legislațiilor naționale, individul are dreptul la viață privată. Accesul la informare este unul din mijloacele prin care un individ se poate asigura că dreptul la viață privată îi este respectat.

Guvernele și celelalte instituții dețin multe informații care pot afecta bunăstarea individului ca membru al societății, chiar dacă aceste informații nu se referă la el în mod direct.

Vă puteți gândi la anume tipuri de informații deținute de guvern, pe care o persoană ar trebui să le cunoască?

Există multe tipuri de informații deținute de guvern, care afectează viața individului. Ele se pot înscrie în oricare dintre categoriile următoare (sau în multe alte categorii):

- politică;- viață socială;- sănătate;- educație;- mediu;- planuri de investiții;- securitate;- justiție.

3) Reglementarea juridică a dreptului la informației

Cadrul juridic este chemat să realizeze dreptul de proprietar asupra informației cu diferențierea proprietății organizațiilor de stat în organelor administrative; structurilor comerciale, datelor personale a cetățenilor.

La sfârșitul anilor 70 comunitatea internațională a formulat două principii, care au fost luate ca bază la crearea cadrului juridic a securității informaționale în mai multe țări și sunt următoarele:

- definirea hotarelor amestecului statului în viața personală a cetățenilor cu utilizarea sistemelor informatice;
- implementarea mecanismelor administrative de protecție a cetățenilor contra astfel de amestecuri.

Cu ajutorul normelor de drept în domeniul securității informaționale trebuie să fie realizate următoarele sarcini:

- referirea informației drep deschisă sau închisă;
- definirea drepturilor de access la informații;
- definirea drepturilor persoanelor de răspundere în vederea atribuirii și modificării parafelor anumitor informații;
- modurile și procedurile de acces;
- modul de control, documentare și analiză a acțiunilor personalului
- responsabilitățile pentru neîndeplinirea cerințelor definite;
- demonstrarea vinovăției răufăcătorilor;
- pedepsirea vinovaților;

4) Semnătura electronico-digitală ca instituție a dreptului informațional

Noțiunile ce urmează de reținut:

mijloacele semnăturii digitale - mijloacele tehnice și/sau de program ce asigură crearea cheii publice și cheii private, crearea semnăturii digitale și/sau verificarea autenticității acesteia;

semnătură digitală - atribut indispensabil al documentului electronic, obținut în urma transformării criptografice a acestuia cu utilizarea cheii private, destinat să confirme autenticitatea documentului electronic; LEGE Nr. 264 din 15.07.2004 cu privire la documentul electronic și semnătura digital.

Potrivit Articolul 18 al Legii nominalizate prevede următoarele privind semnăturai digital:(1) Documentul electronic este semnat cu semnătura digitală a persoanei abilitate, în modul stabilit de legislație sau de contract, să semneze cu semnăturăolografă documentul echivalent pe suport de hîrtie.(2) Semnătura digitală este creată de titularul certificatului cheii publice prin mijloacele semnăturii digitale, utilizîndu-se cheia privată.(3) Modul de aplicare a semnăturii digitale în documentele electronice ale autorităților publice este stabilit de Guvern.

Conform aceleeași Legi Articolul 19. Sunt prevăzute efectele juridice ale semnăturii digitale:(1) Semnătura digitală produce aceleași efecte juridice ca și semnătura olografă în documentul pe suport de hîrtie, cu condiția:

a) autenticității semnăturii digitale, confirmate prin mijloacele de certificare ale acesteia; și

b) valabilității, la momentul semnării documentului electronic, a certificatului cheii publice perfectat și eliberat conform legislației.

(2) Semnătura digitală este echivalată juridic cu semnătura olografă în documentul pe suport de hârtie autentificat cu ștampilă în cazul în care există împuternicirile de utilizare a ștampilei.

(3) Conținutul documentului pe suport de hârtie autentificat cu ștampilă și transformat în document electronic poate fi autentificat cu semnătura digitală a persoanei abilitate. În acest caz, drept document original se consideră documentul pe suport de hârtie.

Cît privește verificarea autenticității semnăturii digitale se efectuează prin mijloacele certificate ale semnăturii digitale, cu utilizarea certificatului cheii publice al alcătuitorului care a semnat documentul electronic.

Mijloacele semnăturii digitale nu constituie mijloace de cifrare a informației și sînt supuse certificării obligatorii în conformitate cu legislația privind certificarea mărfurilor și serviciilor.

Mijloacele semnăturii digitale trebuie să asigure:

- a) unicitatea cheii private și cheii publice create;
- b) dificultatea de calcul necesară la deducerea cheii private și a semnăturii digitale;
- c) confidențialitatea cheii private.

5) Protecția dreptului de acces la informație

Conform Articolul 38 a Legii cu privire dreptului de acces la informație este prevăzut ”(1) Persoanele fizice și juridice poartă răspundere, stabilită de legislație, pentru neîndeplinirea cerințelor prezentei legi. (2) Intermediarul în circulația electronică a documentelor poartă răspundere stabilită de legislație, pentru neexecutarea sau executarea necorespunzătoare a obligațiilor și calitatea necorespunzătoare a serviciilor prestate, precum și pentru prejudiciul cauzat de aceste acțiuni (inacțiuni).(3) Pentru acces ilegal la informația cuprinsă în documentele electronice, persoanele poartă răspundere conform legislației cu privire la accesul la informație.(4) Litigiile care apar în cadrul circulației electronice a documentelor, precum și cele legate de utilizarea documentelor electronice și de aplicarea semnăturii digitale, se soluționează de către subiecții circulației electronice a documentelor în conformitate cu legislația și contractele încheiate.”

Centrul de certificare a cheilor publice poartă răspundere pentru prejudiciul cauzat ca urmare a neîndeplinirii obligațiilor prevăzute de prezenta lege, cu excepția cazurilor în care

centrul de certificare aduce probe doveditoare că nu a putut împiedica producerea prejudiciului.

Centrul de certificare nu poartă răspundere pentru prejudiciul cauzat ca urmare a utilizării certificatului cheii publice cu încălcarea restricțiilor de utilizare a acestuia sau a restricțiilor privind limitele valorii operațiunilor în care acesta poate fi utilizat.

Titularul certificatului cheii publice poartă răspundere pentru prejudiciul cauzat de:

a) neîndeplinirea obligațiilor prevăzute de prezenta lege;

b) semnarea documentelor electronice cu utilizarea cheii sale private de către alte persoane, inclusiv în perioada de la solicitarea suspendării valabilității sau revocării certificatului cheii publice până la înscrierea, în termenul stabilit, a mențiunii respective în registrul certificatelor cheilor publice, cu excepția cazurilor în care titularul certificatului va aduce probe doveditoare că documentul electronic a fost semnat de o altă persoană.

Obiectivele de referință:

- să stabilească drepturile și libertățile informaționale de bază;
- să analizeze temeiurile și restricțiile aduse drepturilor și libertăților informaționale;
- să definească dreptul de acces la informație și principiile acestuia;
- să stabilească mecanismele de protecție juridică a dreptului de acces la informație;
- să cunoască noile posibilități oferite de utilizarea semnăturii digitale și efectele juridice a actelor semnate prin semnătură digitală;
- să analizeze avantajele și impactele legate de utilizare de scară largă a noilor tehnologii informaționale.

TEMA 6. Inviolabilitatea vieții private

1. Conceptul și structura dreptului la inviolabilitatea vieții private.
2. Protecția juridică a dreptului la inviolabilitatea vieții private.
3. Datele cu caracter personal – obiect specific de protecție în domeniul informațional

1. Conceptul și structura dreptului la inviolabilitatea vieții private.

Inviolabilitatea vieții personale se afirmă ca un drept fundamental al omului încă din cele mai vechi timpuri, odată cu primele manifestări scrise de libertate, constituind conținutul esențial al declarațiilor, documentelor politicojuridice și ale actelor vechii Rome și al celor din timpurile feudale, formând mai târziu conținutul fundamental al tuturor "Bill of Rights" și al "declarației drepturilor" adoptate din secolul XVII și până astăzi. În epoca contemporană, recunoașterea libertății persoanei ca drept fundamental al omului se impune din ce în ce mai puternic, devenind un imperativ universal dictat de necesitățile de progres social.

Ca urmare, atât pe plan internațional, în Declarația universală a drepturilor omului adoptată de Adunarea Generală a O.N.U. în 1948; în Pactul internațional relativ la drepturile civile și politice, adoptat de aceeași Adunare Generală în 1966 și în Convenția Europeană pentru apărarea drepturilor omului, semnată la Roma în 1950 care constituie expresii ale legităților, structurilor și proceselor sociale contemporane, ca și pe plan național, în Constituție sau în alte acte fundamentale ale statului, inviolabilitatea persoanei primește consacrare juridică, chiar dacă uneori recunoașterea libertății ca drept fundamental rămâne sub forma unui simplu principiu de drept, nefiind asigurate și garanțiile materiale și juridice pentru realizarea lor efectiv.

„Dreptul la respectarea vieții private constituie sfera fiecărei existențe în care nimeni nu se poate amesteca fără a fi invitat”. I. Rivero

Conceptul dreptului la viață privată a fost explicat mai întâi ca „dreptul de a fi lăsat în pace”, însă acesta a evoluat până în zilele noastre într-un concept mai larg, care ar putea fi definit ca dreptul unei persoane fizice de a decide câtă informație personală să divulge, cui și pentru ce anume.

Prin dezvoltarea unei vaste jurisprudențe în domeniu, Curtea Europeană a Drepturilor Omului a stabilit că prin protecția familiei se înțelege protecția legăturilor familiale, chiar dacă acestea nu sunt oficializate prin căsătorie, adopție, recunoaștere a unui copil natural etc.

Prin dreptul la viață privată sunt recunoscute dreptul la relații sociale, dreptul la intimitatea vieții private, dreptul la un mediu sănătos (drept nerecunoscut ca atare, însă protejat indirect dacă prin poluarea mediului este prejudiciată integritatea fizică și morală a subiecților).

Republica Moldova se află, deocamdată, la etapa de promovare a semnificației dreptului de viață privată. Acest drept nu este perceput încă în suficientă măsură ca un drept inerent ființei umane, care solicită statului nu numai datoria de neimixtiune, dar și obligațiuni pozitive care cer în mod concret de la autorități să întreprindă măsuri rezonabile și adecvate pentru a proteja drepturile individului.

2. Protecția juridică a dreptului la inviolabilitatea vieții private.

Deseori instanțele judecătorești din țară și din străinătate sunt puse în situația de a găsi un echilibru între diferitele dispoziții privind drepturile fundamentale ale omului. În domeniul informațional problema cea mai stringentă este instituirea unui echilibru între dreptul la viața privată și dreptul la libertatea de exprimare (inclusiv dreptul la informație).

De reținut în context dispoziția art. 19 alin. (3) din Pactul internațional cu privire la drepturile civile și politice, conform căreia exercitarea libertății de opinie și libertății de a primi sau de a comunica informații poate fi supusă anumitor limitări, stabilite în mod expres prin lege și care constituie măsurile necesare:

- a) respectării drepturilor sau reputației altora;
- b) apărării securității naționale, ordinii publice, sănătății sau moralității publice.

Dispoziții similare conțin Declarația Universală a Drepturilor Omului (art. 19 și 29), Convenția Europeană pentru Drepturile Omului (art. 10) și Constituția Republicii Moldova (art. 32 și 54).

Lezarea onoarei și demnității se poate produce prin difuzarea informațiilor defaimatoare, care nu corespund realității, pe când încălcarea dreptului la viața privată poate să se manifeste printr-o multitudine de acțiuni și inacțiuni, inclusiv răspunderea unor informații care, deși corespund realității, tin de domeniul vieții private și nu puteau fi publicate sau divulgate decât cu consimțământul subiectului pe care-l privesc. Încălcarea dreptului la viața privată, sub aspectul abordat în acest studiu, se poate manifesta prin colectarea, prelucrarea, stocarea neautorizată și divulgarea fără temei legal a informațiilor despre viața personală, familială, intimă, despre starea sănătății și alte aspecte ale vieții particulare a omului.

Dispoziția constituțională este elocventă prin laconismul ei: “Statul respectă și ocroteste viața intimă, familială și privată” (art.28). Norma poate fi interpretată diferit:

recunoasterea caracterului absolut al dreptului la viata privata si neadmiterea sub nici o forma a imixtiunilor in acest domeniu si constatarea faptului ca aceasta norma impune obligatii doar statului. Multe din reglementarile legislative in vigoare argumenteaza incalcarea dreptului la viata privata prin ratiuni de interes public, care sint prioritare. Cu un anumit grad de relativitate, distingem urmatoarele categorii sociale si juridice in domeniul vietii private: secretul personal, intimitatea personala (secretul individualitatii, secretul identitatii sociale, secretul datelor biografice, secretul datelor medicale); secretul familial (confidentialitatea raporturilor familiale, secretul adoptiei); secretul corespondentei (inclusiv existenta corespondentei, continutul acesteia si contactele).

Daca ne-am conduce doar dupa art. 4 din Legea presei, care statueaza ca: „Publicatiile periodice si agentiile de presa publica, potrivit aprecierilor proprii, orice fel de materiale si informatii, tinind cont de faptul ca exercitiul acestor libertati ce comporta datorii si responsabilitati este supus unor formalitati, conditii, restringeri si unor sanctiuni prevazute de lege, care constituie masuri necesare, intr-o societate democratica [...] pentru a impiedica divulgarea unor informatii confidentiale...”, raspunsul ar fi afirmativ si categoric.

Astfel, Legea presei constituie o bariera legala in exercitarea unor atributii caracteristice profesiei de jurnalist. Sa presupunem ca jurnalistul detine informatii veridice despre hobby-ul unei persoane, care consta in confectionarea la domiciliu a substantelor explozive. Insi faptul de a avea un hobby nu este condamnabil, dar avind in vedere ca prin acesta se urmareste un scop criminal si se pune in pericol viata, sanatatea si bunurile altor persoane, potentialul pericol social devine prioritar dreptului la ocrotirea vietii private si indreptateste attentionarea opiniei publice. Cu parere de rau, in contextul art. 4 din Legea presei si art. 177 din noul Cod penal, situatia jurnalistului in cazul descris devine absurda. Legea Federatiei Ruse cu privire la mijloacele de informare in masa stipuleaza o exceptie pentru jurnalisti (dispozitia nu se extinde asupra celorlalti cetateni), care consta in dreptul jurnalistului de a dobindi, pastra si difuza informatii despre viata privata, daca aceasta serveste interesului public. Legea Republicii Moldova privind accesul la informatie, fiind reformatoare si argumentata doctrinar, prevede posibilitatea divulgarii informatiilor cu caracter personal in cazul in care interesul public prevaleaza (art. 8 alin. (8), dar face aceasta in contextul obiectului sau de reglementare si nu poate fi aplicata pentru rezolvarea situatiei particulare descrise mai sus.

Este admisibila publicarea, in cadrul reportajelor, articolelor si altor materiale jurnalistice, a informatiilor ce permit identificarea persoanei retinute, arestate, banuite sau

invinuite de savirsirea unei infractiuni? Prin informatiile respective se aduce atingere dreptului la viata privata?

Pentru moment, raspunsul la intrebarea formulata nu poate fi argumentata juridic. In opinia noastra, persoana suspectata sau acuzata de savirsirea unei infractiuni nu poate impiedica difuzarea informatiilor ce permit identificarea sa, inclusiv imaginea vizuala, pe motivul protectiei dreptului la viata privata, or, interesul public pentru descoperirea crimelor indreptateste actiunea jurnalistului, facind posibila aparitia de noi martori, inclusiv persoane care sa ofere inculpatului un alibi, de victime necunoscute anchetei, dovezi etc. In astfel de cazuri insa legea impune sa se utilizeze cu maxima atentie termenii juridici, evitandu-se termenii gen “criminal”, “infractor” pina la pronuntarea sentintei de instanta judecatoreasca. In plus, din considerente de etica profesionala, in cazul neadeveririi faptelor, se va comunica in cadrul aceleiasi rubrici, la care a fost plasata informatia anterioara, despre achitarea persoanei respective sau despre sistarea procesului in privinta acestuia.

Pe cine trebuie sa informeze jurnalistul despre efectuarea inregistrarii (audio, video, foto) si de la cine trebuie sa-si ceara voie? Jurnalistul, care colecteaza informatii despre viata privata a persoanei, urmeaza sa preintimpine si sa solicite acordul persoanei vizate sau al reprezentantilor sai legali. In cazul in care vrea sa obtina informatii de alt gen, jurnalistul de asemenea este obligat sa avertizeze cetateanul sau persoana publica asupra efectuarii inregistrarilor.

Este in drept jurnalistul sa efectueze inregistrari (video, foto) in locurile publice fara acordul persoanelor prinse in obiectiv? Aflarea persoanei in locurile publice, discursurile publice ale persoanei etc. nu pot fi atribuite la domeniul vietii private a acesteia. In consecinta, nu este necesara o permisiune expresa.

Este in drept jurnalistul sa efectueze filmari (video, foto) in case sau de case si alte proprietati apartinand persoanelor private si, in special, functionarilor publici fara consimtamintul acestora?

Legea nu face distinctie (decit cu unele exceptii, una dintre care o vom analiza aici) intre viata privata a cetatenilor simpli si cea a functionarilor publici, aparind-o in mod egal. Daca jurnalistul patrunde in mod ilegal in domiciliul sau resedinta persoanei, indiferent de statutul acesteia, el se face raspunzator de incalcarea art. 177 “Incalcarea inviolabilitatii vietii personale” si art. 179 “Violarea de domiciliu” din noul Cod penal. Totodata, daca patrunde in mod legal in domiciliul sau resedinta persoanei, dar efectueaza filmari fara acordul acesteia, jurnalistului i se imputa raspundere doar in temeiul art. 177.

Daca jurnalistul filmeaza proprietatea, inclusiv casa, santierul de constructie etc. fara sa patrunda ilegal in casa si da publicitatii informatiile respective cu identificarea persoanelor la care se refera, el este actionat in judecata in temeiul art. 177 din Codul penal. O derogare de la aceasta regula prevede Legea privind declararea si controlul veniturilor si al proprietatii demnitarilor de stat, judecatorilor, procurorilor, functionarilor publici si a unor persoane cu functie de conducere (nr.1264-XV din19.07.2002), care in art. 13 stabileste caracterul public al anumitor informatii. Art. 13 alin. (1) da lista functiilor publice, detinatorii carora sint obligati sa faca declaratii de venit, raspunzind exigentei absolut legale privind instituirea controlului societatii asupra surselor de venit ale functionarilor publici.

Raspunderea penala, conform Legii nr. 1264-XV, este aplicabila unor fapte de un pericol social redus, fapt ce intra in contradictie cu insusi conceptul de infractiune. In alte tari, inasa, raspunderea penala, incriminind incalcarea inviolabilitatii vietii private, prevede citeva elemente calificative obligatorii pentru incadrarea faptei in contextul infractional: faptele ce incalca dreptul la viata privata trebuie sa fi fost savirsite din motive josnice; aceste fapte trebuie sa fi cauzat un prejudiciu drepturilor si intereselor legitime.

Este in drept jurnalistul sa filmeze persoanele cu functie de raspundere si functionarii publici in exercitarea atributiilor de serviciu fara acordul lor?Persoana cu functie de raspundere si functionarul public (aceste notiuni nu sint sinonime), ca si orice alta persoana, se pot opune efectuarii unor inregistrari (audio, video, foto) doar daca prin aceasta li se lezeaza dreptul la viata privata. Or, exercitarea obligatiilor de serviciu nu poate fi atribuita sub nici o forma la domeniul vietii lor private, prin urmare nu este necesar acordul lor pentru efectuarea filmarilor.

Totodata, in cazul in care, in cadrul unei discutii sau interviu, jurnalistul urmareste scopul de a obtine informatii de la persoana cu functie de raspundere sau functionar, el trebuie sa atentioneze persoana respectiva asupra efectuarii inregistrarilor (ceea ce nu inseamna ca jurnalistul trebuie sa solicite consimtamintul ei).

Este in drept persoana sa distruga materialul (casete, filmul, fotografia etc.) pe care a fost inregistrata, fara acordul ei, informatia cu caracter personal? Poate persoana sa ceara distrugerea informatiei?

Obiectivele de referință

- să descrie conceptul și conținutul dreptului la inviolabilitatea vieții private;
- să cunoască mecanismele juridice de protecție a dreptului la inviolabilitatea vieții private;
- să stabilească particularitățile datelor cu caracter personal ca obiect specific de protecție;
- să analizeze temeiurile juridice care permit utilizarea, prelucrarea și transmiterea datelor cu caracter personal.

7. Dreptul mass-media ca instituție a dreptului informațional

1. Apariția și evoluția dreptului mass-media în Republica Moldova.
2. Libertatea de exprimare: concept, limite, răspundere.
3. Subiecții dreptului mass-media

1. Apariția și evoluția dreptului mass-media în Republica Moldova

Relațiile sociale sunt într-o continuă evoluție, astfel apar noi relații sociale care trebuiesc reglementate de lege. Unele din ele se încadrează în obiectul ramurilor de drept existente, devenind reglementate fie prin modificarea unor acte normative din domeniu, fie prin adoptarea unui act normativ nou, iar altele, pentru că reprezintă o categorie de relații sociale distinctă, necesită adoptarea unui cadru normativ complex și complet. În felul acesta se creează noi ramuri de drept. De altfel, criteriile principale de deosebire a ramurilor de drept îl reprezintă obiectul și metoda de reglementare. Trebuie să evidențiem că nu crearea oficială a unei ramuri noi de drept este premisa pentru apariția unui obiect distinct de reglementare, ci anume aceste relații care au trăsături comune, ce reprezintă o categorie distinctă și care necesită o reglementare amplă, sunt premisa pentru apariția unei noi ramuri de drept, aceste relații reprezentând obiectul de reglementare al ramurii de drept respective.

Cît privește dreptul mass-media, ca premisă pentru apariția acestei ramuri de drept a fost dezvoltarea progresivă a societății informaționale în ultimele decenii, iar relațiile din cadrul acestui domeniu presupunînd necesitatea de a fi reglementate, acestea reprezentînd obiectul de reglementare a dreptului informațional.

O condiție-cheie pentru democratizarea continuă a societății, participarea cetățenilor la guvernare și eficientizarea activității administrației publice, pentru prevenirea și combaterea corupției o constituie realizarea consecventă a liberului acces la informațiile oficiale, transparența instituțională/decizională a autorităților și instituțiilor publice, promovarea reformelor revine monitorizării permanente a implementării legislației.

În ultimii zece ani, mai multe țări au elaborat legi cu privire la liberul acces la informații, printre acestea numărîndu-se Fiji, Japonia, Mexic, Africa de Sud, Coreea de Sud, Thailanda, Trinidad – Tobago, Marea Britanie, precum și majoritatea țărilor din Europa Centrală și de Est. Aceste țări s-au alăturat astfel unor state precum Suedia, SUA, Finlanda, Olanda, Australia și Canada, care promulgaseră asemenea legi cu mai mult timp în urmă.

2. Libertatea de exprimare: concept, limite, răspundere.

Libertatea de expresie se aplica nu numai "informatiilor" sau "ideilor" care sunt primite favorabil, dar si acelor care ofenseaza, socheaza sau deranjeaza statul sau orice alt segment al populatiei. Aceasta înseamna pluralism, toleranta si spirit deschis, în absenta carora nu putem vorbi de existenta unei "societati democratice". Prin urmare, fiecare "formalitate", "conditie", "restrictie" sau "sanctiuni" impuse în acest domeniu trebuie sa fie proportionala cu legitimitatea scopului urmarit.

Libertatea de expresie, care este protejata prin art. 10 al Conventiei, este socotita drept una din cheile de bolta ale democratiei. Asadar, potrivit art. 10, "Orice persoana are dreptul la libertatea de exprimare. Acest drept cuprinde libertatea de opinie si libertatea de a primi sau de a comunica informatii ori idei fara amestecul autoritatilor publice si fara a tine seama de frontiere". Dispozitiile articolului amintit nu împiedica însa statele, "sa supuna societatile de radiodifuziune, de cinematografie sau de televiziune unui regim de autorizare".

De asemenea, exercitarea acestor libertati, ce comporta îndatoriri si responsabilitati, "poate fi supusa unor formalitati, conditii, restrângeri sau sanctiuni prevazute de lege, care constituie masuri necesare, într-o societate democratica, pentru securitatea nationala, integritatea teritoriala sau siguranta publica, apararea ordinii si prevenirea infractiunilor, protectia sanatatii sau a moralei, protectia reputatiei sau a drepturilor altora pentru a împiedica divulgarea de informatii confidentiale sau pentru a garanta autoritatea si imparialitatea puterii judecatoresti".

Libertatea de expresie este si un element esential din care decurg alte drepturi si libertati, si, totodata consecinta logica a dreptului la libertatea de gândire, de constiinta si de religie, care face obiectul art. 9 al Conventiei, potrivit caruia: "Orice persoana are dreptul la libertatea de gândire, de constiinta si de religie; acest drept include libertatea de a-si schimba religia sau convingerea, precum si posibilitatea de a-si manifesta religia sau convingerea în mod individual sau în colectiv, în public sau în particular, prin cult, învatamânt, practici si îndeplinirea ritualurilor". Alin. 2 al art. 9 din Conventie statueaza ca, "libertatea de a-si manifesta religia sau convingerile nu poate face obiectul altor restrângeri decât acelea care, prevazute de lege, constituie masuri necesare, într-o societate democratica, pentru siguranta publica, protectia ordinii, a sanatatii sau a moralei publice ori pentru protejarea drepturilor si libertatilor altora".

Având în vedere cele de mai sus, nu este deloc surprinzator ca au fost deferite Curtii Europene a Drepturilor Omului un numar mare de spete referitoare la libertatea de expresie. Astfel, unul dintre cele mai celebre cazuri este Sunday Times contra Marea

Britanie, din 1979, caz ce a pornit de la o hotarâre judecatoreasca emisa de un tribunal britanic pentru a împiedica ziarul Sunday Times sa publice un articol referitor la un proces aflat pe rol. Articolul aducea la cunostinta opiniei publice faptul ca numerosi copii se nascusera cu malformatii grave deoarece mamele lor luasera, în timpul sarcinii, un medicament numit "*thalidomina*". Curtea a hotarât ca respectiva ordonanta judecatoreasca a încalcat libertatea de expresie: articolul din Sunday Times era de interes public si publicul avea dreptul de a-i cunoaste continutul, chiar daca procesul al carui obiect îl constituia medicamentul era înca pe rol.

Libertatea de exprimare se coroboreaza cu "*îndatoriri si responsabilitati*" si poate fi subiectul multor restrictii "*necesare într-o societate democratica*". Curtea a aplicat riguros limitele dreptului la libertatea de expresie. Astfel, de exemplu, în cazul **Handyside contra Marea Britanie**, din 1976, Curtea a hotarât ca statul a fost îndreptatit sa aplice restrictii fata de publicarea "*Micului manual rosu*" pentru scolari, o carte având drept scop educatia sexuala a tinerilor dar care a fost considerata o "*publicatie obscena*" în virtutea influentei negative pe care ar fi putut-o avea asupra moralitatii tinerilor cititori.

Asadar, desi Conventia Europeana asigura un înalt grad de protectie a drepturilor omului, mai sunt înca necesare si alte actiuni în scopul întaririi si promovarii dreptului la libertatea de expresie. În cadrul Consiliului Europei, Comitetul Ministrilor a luat pozitie în aceasta problema prin intermediul **Declaratiei sale asupra Libertatii de Expresie si Informare din 29 Aprilie 1982**, declaratie ce fixeaza drept obiective: "*respectarea drepturilor enuntate de Articolul 10*", garantarea "*absentei cenzurii, a controlului sau constrângerilor arbitrare*" în domeniul mijloacelor de comunicare în masa, si sustine, de asemenea, cu tarie "*existenta unui larg spectru de mijloace de comunicare independente, ce reflecta diversitatea ideilor si opiniilor*".

Convenția Europeană pentru Apărarea Drepturilor Omului și a Libertăților Fundamentale (în continuare Convenția) 263 a fost adoptată în baza Declarației Universale a Drepturilor Omului, cu mult timp înainte de adoptarea pactelor internaționale din 1966 din sistemul Națiunilor Unite de protecție a drepturilor omului, ceea ce ne îndreptățește să afirmăm că pionieratul în acest domeniu aparține sistemului european.

Convenția a fost primul instrument al drepturilor omului care a stipulat expres limitări a libertății de exprimare. Libertatea de exprimare constituie unul din fundamentele esențiale ale unei societăți democratice și una din condițiile esențiale pentru progresul ei și pentru realizarea potențialului fiecărui individ. Conținutul articolului 10 este aplicabil nu doar „informației” sau „ideilor” care sunt primite favorabil sau considerate inofensive, sau sunt

primite indiferent, dar de asemenea aplicabile celor care ofensează, șochează sau tulbură statul sau vreun sector al populației. Acestea sunt cerințele pluralismului, toleranței și orizontului lărgit, valori fără de care nu există o societate democratică.”

Articolul 10 din Convenție protejează toate formele de exprimare (inclusiv în domeniul artei și științei) și ce e mai interesant, importanța politică a exprimării în contextul său concret nu joacă un anumit rol pentru nivelul oferit de protecție.²⁶⁵ Felul exprimării, necesar în societatea democratică, se pare, primește cea mai mare protecție în legătura cu faptul că el este privit ca piatra de temelie și elementul determinant al democrației: „În sistemul democratic, acțiunile sau greșelile guvernării trebuie să fie obiect al observării minuțioase nu doar din partea organelor de drept sau puterii judiciare, dar și din partea opiniei publice”.

3. Subiecții dreptului mass-media

Subiecți ai prezentei dreptului mass-media sînt furnizorii de informații și solicitanții informației.

Furnizori de informații, adică posesori ai informațiilor oficiale, obligați să le furnizeze solicitanților în condițiile prezentei legi, sînt:

a) autoritățile publice centrale și locale - autoritățile administrației de stat, prevăzute în Constituția Republicii Moldova și anume: Parlamentul, Președintele Republicii Moldova, Guvernul, administrația publică, autoritatea judecătorească;

b) instituțiile publice centrale și locale - organizațiile fondate de către stat în persoana autorităților publice și finanțate de la bugetul de stat, care au ca scop efectuarea atribuțiilor de administrare, social-culturale și altor atribuții cu caracter necomercial;

c) persoanele fizice și juridice care, în baza legii sau a contractului cu autoritatea publică ori instituția publică, sînt abilitate cu gestionarea unor servicii publice și culeg, selectează, posedă, păstrează, dispun de informații oficiale.

Pot solicita informații oficiale, în condițiile prezentei legi:

a) orice cetățean al Republicii Moldova;

b) cetățenii altor state, care au domiciliul sau reședința pe teritoriul Republicii Moldova;

c) apatrizii stabiliți cu domiciliul sau cu reședința pe teritoriul Republicii Moldova.

Obiectivele de referință

- să identifice conceptul libertății de exprimare;
- să explice natura și trăsăturile activității mijloacelor de informare în masă;
- să analizeze evoluția dreptului mass-media în Republica Moldova;
- să prezinte categoriile de subiecți ai dreptului mass-media.

TEMA 8. Dreptul de proprietate și dreptul proprietății intelectuale ca domeniu de reglementare a dreptului informațional

1. Informația, resursele informaționale ca obiect al dreptului de proprietate și a drepturilor exclusive.
2. Probleme de aplicare ale instituției proprietății intelectuale în dreptul informațional

1. Informația, resursele informaționale ca obiect al dreptului de proprietate și a drepturilor exclusive.

Civilizația fiind, în esența ei, o problemă de informație se evidențiază câteva etape revoluționare în istoria civilizației în care dezvoltarea tehnologică majoră a schimbat fundamental premisele pentru diseminarea informației implicând și o reevaluare a modelelor de gândire vechi și adânc înrădăcinate: *aparitia limbajului, inventarea limbajului scris, inventarea tiparului, dezvoltarea industrialismului, mediilor electronice și digitale*. Pentru o mai bună înțelegere a accesului la informație, am subliniat *importanța* strategică, economică și culturală a informației plecând de la *natura* informației considerată ca o resursă în societatea informațională ale cărei *caracteristici* o fac perfect compatibilă cu natura organizației publice realizând o radiografiere a elementelor definitorii pentru societatea informațională în care trăim: *trăsături și caracteristici, dimensiuni (tehnologică, socială, științifică, economică, politico-administrativă, juridică, culturală), evaluare cantitativă și calitativă a stării societății informaționale*.

Adoptate încă din 1948 și reconfirmate, la Geneva, în 1993, *drepturile omului* sintetizează esența principiilor de respectare a integrității corporale, a libertății și proprietății individuale pe principiul egalității servind *drept fundament moral global al accesului la informații*. *Accesul liber la informație* este unul dintre drepturile fundamentale ale omului, reflectat de articolul 19 al Declarației Universale a Drepturilor Omului a Organizației Națiunilor Unite, de articolul 10 din Convenția Europeană a Drepturilor Omului, de articolul II-71 din Convenția de Tratat Constituțional, și nu în ultimul rând de articolul 30 al Constituției României. Acest drept permite oricui să își prezinte punctele de vedere,

concepțiile sau convingerile în legătură cu orice problemă de interes colectiv sau personal, fără nici un fel de îngrădire, în cadrul și cu respectarea valorilor morale și juridice ale societății, fiind strâns legat de *libertatea de exprimare* pentru care *Curtea Europeană a Drepturilor Omului a stabilit o serie de principii, reguli și criterii ce caracterizează pluralismul, toleranța și spiritul de deschidere într-o societate democratică.*

2. Probleme de aplicare ale instituției proprietății intelectuale în dreptul informațional

Pe parcursul ultimilor ani s-a înregistrat o serie de progrese semnificative în domeniul asigurării drepturilor de proprietate intelectuală (PI), fapt atestat și de interesul crescând față de această sferă. Racordarea legislației Republicii Moldova la standardele și normele europene, uniformizarea practicii judiciare în domeniul proprietății intelectuale, dar și intensificarea colaborării dintre mediul public și cel privat contribuie la edificarea unei percepții clare privind caracterul imperativ al protecției și respectării drepturilor de PI.

Acestea sunt concluziile formulate în cadrul Mesei rotunde „Aspecte practice privind asigurarea drepturilor de proprietate intelectuală în Republica Moldova” organizate pe 8 decembrie curent de Agenția de Stat pentru Proprietatea Intelectuală a Republicii Moldova (AGEPI) în cooperare cu Asociația Business Software Alliance (BSA) și Asociația Națională a Companiilor Private din Domeniul Tehnologiilor Informaționale și Comunicațiilor (ATIC).

La eveniment au participat reprezentanți ai conducerii instituțiilor și autorităților publice abilitate cu responsabilități în domeniul protecției drepturilor de PI: Ministerul Justiției, Ministerul Tehnologiei Informației și Comunicațiilor, Ministerul Afacerilor Interne, Curtea Supremă de Justiție, Serviciul Vamal, Procuratura Generală, Cancelaria de Stat, Ambasada SUA în RM, AGEPI, precum și reprezentanții titularilor de drepturi - ATIC, BSA Moldova, REACT România.

Doamna Lilia Bolocan, Director general AGEPI, a subliniat că, deși domeniul autohton al drepturilor de PI este la o vârstă fragedă, întregul sistem de protecție a proprietății intelectuale a fost elaborat, fiind pe deplin funcțional. Dumneaei a apreciat înalt deschiderea sectorului privat față de inițiativele ce țin de realizarea drepturilor de PI și a menționat că este foarte important ca instituțiile prezente în cazul mesei rotunde să rămână în aceeași abordare de colaborare și parteneriat privind asigurarea drepturilor de PI.

Prezent in cadrul sesiunii de deschidere a evenimentului, dl Oleg Efrim, Ministru al Justitiei, a mentionat ca in ultimii ani tara noastra a facut un salt semnificativ in ceea ce priveste cadrul legal care reglementeaza aspectele de PI, legislatia noastra fiind inalt apreciata de experti internationali in domeniu.

„Drepturile de proprietate intelectuala posedo o valoare economica din ce in ce mai mare. Statele dezvoltate din Vest, Statele Unite ale Americii, mai recent China, India, statele mari si cele in curs de dezvoltare investesc foarte mult in aceasta zona de creativitate si inovatie. Ca sa pastram stimulii necesari pentru aceasta activitate, trebuie sa protejam drepturile de proprietate intelectuala” a mentionat dl Dorin Recean, Viceministru al Tehnologiei Informatiionale si Comunicatiilor, participant la eveniment.

In opinia dlui Tudor Darie, Consilier al Prim-ministrului Republicii Moldova pe Politici de Tineret si Tehnologii Informatiionale, este foarte important ca raporturile dintre detinatorul de drepturi si consumatorul operei sa fie cat se poate de firesti, fiind mult mai convenabil ca opera sa fie procurata in mod legal si nu ilegal.

Cele trei sesiuni ale mesei rotunde au fost consacrate problemelor majore precum practica judiciara in domeniul proprietatii intelectuale, asigurarea drepturilor de proprietate intelectuala la frontiera, constatarea si urmarirea penala a incalcarilor in domeniul proprietatii intelectuale, fiecare dintre ele generand un fructuos schimb de opinii si dezbateri.

Conform opiniei participantilor, conjugarea eforturilor si actiunilor va permite identificarea si excluderea lacunelor si verigilor slabe ale cadrului normativ si va asigura protectia efectiva a drepturilor de PI. Integrarea activa a tuturor institutiilor abilitate cu atributii in domeniul asigurarii drepturilor de PI intr-un amplu mecanism de colaborare, cu finalitati clare, obiective si responsabilitati bine determinate este cu atat mai importanta si fezabila, cu cat domeniul este unul foarte complex, dar si in permanenta schimbare.

Discutiile din cadrul mesei rotunde au purtat un caracter constructiv si au contribuit incontestabil la consolidarea platformei de comunicare interinstitutionala, constituind un pas important in atingerea obiectivelor de asigurare a drepturilor de proprietate intelectuala in Republica Moldova.

Obiectivele de referință

- să analizeze informația, resursele informaționale ca obiect al dreptului de proprietate;
- să explice probleme de aplicare ale instituției proprietății intelectuale în dreptul informațional;
- să analizeze informația, resursele informaționale ca obiect al drepturilor exclusive;
- să stabilească cum sunt legate categoriile „document” și „rezultatul” activității intelectuale;
- să formuleze opinii asupra conceptului de „copyright”.

9. Bazele juridice ale securității informaționale

1. Conceptul, obiectul securității informaționale și locul ei în sistemul asigurării securității naționale
2. Bazele teoriei priorităților. Prioritățile naționale ale Republicii Moldova în domeniul informațional
3. Bazele teoriei impactelor. Doctrina securității informaționale a Republicii Moldova cu privire la impactele principale din domeniul informațional și sursele acestora.
4. Principiile, sarcinile, funcțiile și standardele asigurării securității informaționale
5. Dreptul și legislația în domeniul asigurării securității informaționale

1. Conceptul, obiectul securității informaționale și locul ei în sistemul asigurării securității naționale

O politica de securitate, de regulă, are în vedere două laturi: a subiectului și a obiectului politicii. Subiectul este reprezentat de ceva activ în SMSI (utilizator, program, proces etc.), iar obiectul este cel asupra căruia acționează un subiect (fișiere, dosare, diferite dispozitive și echipamente etc.). Se impune elaborarea unui set de reguli utilizate de SMSI, pentru ca acesta să poată determina în ce caz un anumit subiect este autorizat să aibă acces la un anumit obiect. Politica de securitate are ca scop primordial asigurarea integrității, disponibilității și confidențialității informației. Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate. Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor sistemului informațional (SI). Diverse aplicații au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a SI.

Confidențialitatea se referă la protecția datelor împotriva accesului neautorizat. Utilizatorul răspunde personal de asigurarea confidențialității datelor încredințate prin procedurile de acces la SI. Politica de securitate are ca scop, de asemenea, stabilirea cadrului normativ necesar pentru elaborarea regulamentelor și procedurilor de securitate. Acestea sînt obligatorii pentru toți utilizatorii SI

Ce este informația ? Informația este conceptul care sta la baza acestei ere. Informația, dacă nu este deja, cu siguranță va fi obiectul principal de lucru în anii ce vor urma. Când spunem informație, ne gândim în principal la informația digitală. Odată cu dezvoltarea

tehnologiei, spațiile virtuale care mai demult existau doar în imaginație au început să prindă viață. Astfel a luat naștere WWW-ul (world wide web). Acest acronim este unul dintre cele mai cunoscute deoarece toată lumea știe că “pe www poți găsi orice”; orice informație cu caracter public bineînțeles. Printre alte invenții digitale care ne facilitează accesul la informație se numără FTP (file transfer protocol) și bineînțeles motoarele de căutare.

Search engines cine nu a auzit de Google sau Altavista ? Motoarele de căutare reprezintă unele dintre cele mai puternice ustensile pentru accesul la informația digitală. Acestea stochează în baza lor de date informații despre conținutul serverelor. Revenind la ideea de la care am plecat și anume aceea că informația stă la baza multor activități pe care le desfășurăm ne punem problema: “Ce facem cu informațiile sensibile?”. Pe cât de simplu pare, pe atât de complicat este răspunsul: “le protejăm”. Nevoia de securitate la nivel informațional este din ce în ce mai stringentă. Pe zi ce trece numărul companiilor care au nevoie de canale securizate crește; numărul persoanelor care doresc confidențialitatea informațiilor crește; și lista continuă.

Din aceste dorințe de confidențialitate, existente de altfel de mult timp dar sub alte forme, s-au născut ideile, teoriile, programele și cercetările legate de securitatea informației.

2. Bazele teoriei priorităților. Prioritățile naționale ale Republicii Moldova în domeniul informațional

Principiile, valorile generale, obiectivele, liniile directorii de bază ale securității naționale. Amenințările, riscurile și vulnerabilitățile cu impact asupra securității naționale a Republicii Moldova

Statutul de neutralitate permanentă. Republica Moldova este un stat suveran și independent, unitar și indivizibil. Teritoriul ei este inalienabil. În conformitate cu art.11 din Constituție, Republica Moldova proclamă neutralitatea sa permanentă, ceea ce presupune că țara noastră nu este parte la blocuri militare și nu admite dislocarea de trupe militare sau de armamente ale altor state și ale blocurilor militare pe teritoriul său.

Statutul de neutralitate permanentă reprezintă principiul de bază, piatra de temelie a conceptului securității naționale. Astfel, toate acțiunile desfășurate de întregul sistem de securitate națională al Republicii Moldova, îndreptate spre asigurarea securității naționale, se bazează pe acest principiu. În acest sens, Republica Moldova depune eforturi pentru asigurarea respectării neutralității sale permanente de către subiecții de drept internațional.

Obiectivele securității naționale și liniile directorii de bază în asigurarea securității

naționale. Securitatea națională reprezintă condiția fundamentală a existenței poporului din Republica Moldova, a statului moldovenesc și este un obiectiv al țării. Obiectivele securității naționale a Republicii Moldova sînt: asigurarea și apărarea independenței, suveranității, integrității teritoriale, ordinii constituționale, dezvoltării democratice, securității interne, consolidarea statalității Republicii Moldova. Un loc aparte în acest sens revine apărării și promovării valorilor, intereselor și obiectivelor naționale. Securitatea națională nu este numai securitatea statului, ci și securitatea societății și a cetățenilor Republicii Moldova, atît pe teritoriul Republicii Moldova, cît și peste hotarele ei. Securitatea națională a Republicii Moldova se realizează prin măsuri adecvate de natură politică, economică, diplomatică, socială, juridică, educativă, administrativă și militară, prin activitate de informații, contrainformații, precum și prin depășirea eficientă a crizelor, în conformitate cu legislația în vigoare și cu dreptul internațional. Călea de integrare a Republicii Moldova în Uniunea Europeană, întreținerea bunelor relații pe plan bilateral, regional, participarea la cooperare multilaterală sînt factorii care fac posibilă apărarea intereselor Republicii Moldova și atingerea scopului securității naționale.

3. Principiile, sarcinile, funcțiile și standardele asigurării securității informaționale

PRINCIPIILE DE REALIZARE A POLITICII DE SECURITATE:

Responsabilității – stabilirea clară a responsabilităților referitoare la securitate pentru proprietarii, furnizorii, administratorii și utilizatorii sistemelor informaționale;

sensibilizării – toate persoanele interesate asupra acestui aspect trebuie informate corect și oportun;

eticii – elaborarea unor reguli de conduită în utilizarea SI;

pluridisciplinarității – metodele tehnice și organizatorice care trebuie luate în vederea securității SI au caracter multidisciplinar și cooperant;

proporționalității – prevede ca nivelul de securitate și măsurile de protecție să fie proporțional cu importanța informațiilor gestionate;

integrității – securitatea este necesară la toate etapele de prelucrare a informațiilor (creare, colectare, prelucrare, stocare, transport, ștergere etc.);

promptitudinii – mecanismele de securitate trebuie să răspundă prompt și să permită o colaborare rapidă și eficientă în caz de detectare a eventualelor pericole;

reevaluării – prevede revizuirea periodică a cerințelor de securitate și a mecanismelor de implementare a lor;

Obiectivele de referință

- să identifice conceptul și obiectul securității informaționale;
 - să determine căile de sporire a protecției diferitor categorii de informație în dependență de modalitate de acces la ea;
 - să compare teoria clasică a dreptului natural și teoria dreptului natural renăscut;
 - să cunoască ce prevede doctrina securității informaționale a Republicii Moldova pentru asigurarea echilibrului între interesele societății, statului și persoanelor;
- să prezinte diversitatea principiilor, sarcinilor, funcțiilor și standardelor asigurării securității informaționale.

10. Protecția informației cu acces limitat și dreptul la informația cu acces limitat

1. Conceptul, trăsăturile și structura informației cu acces limitat
2. Secretul de stat
3. Secretul comercial
4. Secretul bancar
5. Secretul profesional
6. Secretul de serviciu

Deseori instanțele judecătorești din țară și din străinătate sunt puse în situația de a găsi un echilibru între diferitele dispoziții privind drepturile fundamentale ale omului. În domeniul informațional problema cea mai stringentă este instituirea unui echilibru între dreptul la viața privată și dreptul la libertatea de exprimare (inclusiv dreptul la informație).

De reținut în context dispoziția art. 19 alin. (3) din Pactul internațional cu privire la drepturile civile și politice, conform căreia exercitarea libertății de opinie și libertății de a primi sau de a comunica informații poate fi supusă anumitor limitări, stabilite în mod expres prin lege și care constituie măsurile necesare:

- a) respectării drepturilor sau reputației altora;
- b) apărării securității naționale, ordinii publice, sănătății sau moralității publice.

Dispoziții similare conțin Declarația Universală a Drepturilor Omului (art. 19 și 29), Convenția Europeană pentru Drepturile Omului (art. 10) și Constituția Republicii Moldova (art. 32 și 54).

Lezarea onoarei și demnității se poate produce prin difuzarea informațiilor defaimatoare, care nu corespund realității, pe când încălcarea dreptului la viața privată poate să se manifeste printr-o multitudine de acțiuni și inacțiuni, inclusiv răspindirea unor informații care, deși corespund realității, țin de domeniul vieții private și nu puteau fi publicate sau divulgate decât cu consimțământul subiectului pe care-l privesc. Încălcarea dreptului la viața privată, sub aspectul abordat în acest studiu, se poate manifesta prin colectarea, prelucrarea, stocarea neautorizată și divulgarea fără temei legal a informațiilor despre viața personală, familială, intimă, despre starea sănătății și alte aspecte ale vieții particulare a omului.

Dispoziția constituțională este elocventă prin laconismul ei: “Statul respectă și ocrotăște viața intimă, familială și privată” (art.28). Norma poate fi interpretată diferit: recunoașterea caracterului absolut al dreptului la viața privată și neadmiterea sub nici o formă a imixtiunilor în acest domeniu și constatarea faptului că această normă impune obligații doar

statului. Multe din reglementarile legislative in vigoare argumenteaza incalcarea dreptului la viata privata prin ratiuni de interes public, care sunt prioritare. Cu un anumit grad de relativitate, distingem urmatoarele categorii sociale si juridice in domeniul vietii private: secretul personal, intimitatea personala (secretul individualitatii, secretul identitatii sociale, secretul datelor biografice, secretul datelor medicale); secretul familial (confidentialitatea raporturilor familiale, secretul adoptiei); secretul corespondentei (inclusiv existenta corespondentei, continutul acesteia si contactele).

Daca ne-am conduce doar dupa art. 4 din Legea presei, care statueaza ca: „Publicatiile periodice si agentiile de presa publica, potrivit aprecierilor proprii, orice fel de materiale si informatii, tinind cont de faptul ca exercitiul acestor libertati ce comporta datorii si responsabilitati este supus unor formalitati, conditii, restringeri si unor sanctiuni prevazute de lege, care constituie masuri necesare, intr-o societate democratica [...] pentru a impiedica divulgarea unor informatii confidentiale...”, raspunsul ar fi afirmativ si categoric.

Astfel, Legea presei constituie o bariera legala in exercitarea unor atributii caracteristice profesiei de jurnalist. Sa presupunem ca jurnalistul detine informatii veridice despre hobby-ul unei persoane, care consta in confectionarea la domiciliu a substantelor explozive. Insa faptul de a avea un hobby nu este condamabil, dar avind in vedere ca prin acesta se urmareste un scop criminal si se pune in pericol viata, sanatatea si bunurile altor persoane, potentialul pericol social devine prioritar dreptului la ocrotirea vietii private si indreptateste attentionarea opiniei publice. Cu parere de rau, in contextul art. 4 din Legea presei si art. 177 din noul Cod penal, situatia jurnalistului in cazul descris devine absurda. Legea Federatiei Ruse cu privire la mijloacele de informare in masa stipuleaza o exceptie pentru jurnalisti (dispozitia nu se extinde asupra celorlalti cetateni), care consta in dreptul jurnalistului de a dobindi, pastra si difuza informatii despre viata privata, daca aceasta serveste interesului public. Legea Republicii Moldova privind accesul la informatie, fiind reformatoare si argumentata doctrinar, prevede posibilitatea divulgarii informatiilor cu caracter personal in cazul in care interesul public prevaleaza (art. 8 alin. (8), dar face aceasta in contextul obiectului sau de reglementare si nu poate fi aplicata pentru rezolvarea situatiei particulare descrise mai sus.

Este admisibila publicarea, in cadrul reportajelor, articolelor si altor materiale jurnalistice, a informatiilor ce permit identificarea persoanei retinute, arestate, banuite sau invinuite de savirsirea unei infractiuni? Prin informatiile respective se aduce atingere dreptului la viata privata?

Pentru moment, raspunsul la intrebarea formulata nu poate fi argumentata juridic. In opinia noastra, persoana suspectata sau acuzata de savirsirea unei infractiuni nu poate impiedica difuzarea informatiilor ce permit identificarea sa, inclusiv imaginea vizuala, pe motivul protectiei dreptului la viata privata, or, interesul public pentru descoperirea crimelor indreptateste actiunea jurnalistului, facind posibila aparitia de noi martori, inclusiv persoane care sa ofere inculpatului un alibi, de victime necunoscute anchetei, dovezi etc. In astfel de cazuri insa legea impune sa se utilizeze cu maxima atentie termenii juridici, evitandu-se termenii gen "criminal", "infractor" pina la pronuntarea sentintei de instanta judecatoreasca. In plus, din considerente de etica profesionala, in cazul neadeveririi faptelor, se va comunica in cadrul aceleiasi rubrici, la care a fost plasata informatia anterioara, despre achitarea persoanei respective sau despre sistarea procesului in privinta acestuia.

Pe cine trebuie sa informeze jurnalistul despre efectuarea inregistrarii (audio, video, foto) si de la cine trebuie sa-si ceara voie? Jurnalistul, care colecteaza informatii despre viata privata a persoanei, urmeaza sa preintimpine si sa solicite acordul persoanei vizate sau al reprezentantilor sai legali. In cazul in care vrea sa obtina informatii de alt gen, jurnalistul de asemenea este obligat sa avertizeze cetateanul sau persoana publica asupra efectuarii inregistrarii.

Este in drept jurnalistul sa efectueze inregistrari (video, foto) in locurile publice fara acordul persoanelor prinse in obiectiv? Aflarea persoanei in locurile publice, discursurile publice ale persoanei etc. nu pot fi atribuite la domeniul vietii private a acesteia. In consecinta, nu este necesara o permisiune expresa.

Este in drept jurnalistul sa efectueze filmari (video, foto) in case sau de case si alte proprietati apartinand persoanelor private si, in special, functionarilor publici fara consimtamintul acestora?

Legea nu face distinctie (decit cu unele exceptii, una dintre care o vom analiza aici) intre viata privata a cetatenilor simpli si cea a functionarilor publici, aparind-o in mod egal. Daca jurnalistul patrunde in mod ilegal in domiciliul sau resedinta persoanei, indiferent de statutul acesteia, el se face raspunzator de incalcarea art. 177 "Incalcarea inviolabilitatii vietii personale" si art. 179 "Violarea de domiciliu" din noul Cod penal. Totodata, daca patrunde in mod legal in domiciliul sau resedinta persoanei, dar efectueaza filmari fara acordul acesteia, jurnalistului i se imputa raspundere doar in temeiul art. 177.

Daca jurnalistul filmeaza proprietatea, inclusiv casa, santierul de constructie etc. fara sa patrunda ilegal in casa si da publicitatii informatiile respective cu identificarea persoanelor la care se refera, el este actionat in judecata in temeiul art. 177 din Codul penal. O derogare de

la aceasta regula prevede Legea privind declararea si controlul veniturilor si al proprietatii demnitarilor de stat, judecatorilor, procurorilor, functionarilor publici si a unor persoane cu functie de conducere (nr.1264-XV din19.07.2002), care in art. 13 stabileste caracterul public al anumitor informatii. Art. 13 alin. (1) da lista functiilor publice, detinatorii carora sint obligati sa faca declaratii de venit, raspunzind exigentei absolut legale privind instituirea controlului societatii asupra surselor de venit ale functionarilor publici.

Raspunderea penala, conform Legii nr. 1264-XV, este aplicabila unor fapte de un pericol social redus, fapt ce intra in contradictie cu insusi conceptul de infractiune. In alte tari, inasa, raspunderea penala, incriminind incalcarea inviolabilitatii vietii private, prevede citeva elemente calificative obligatorii pentru incadrarea faptei in contextul infractional: faptele ce incalca dreptul la viata privata trebuie sa fi fost savirsite din motive josnice; aceste fapte trebuie sa fi cauzat un prejudiciu drepturilor si intereselor legitime.

Este in drept jurnalistul sa filmeze persoanele cu functie de raspundere si functionarii publici in exercitarea atributiilor de serviciu fara acordul lor?Persoana cu functie de raspundere si functionarul public (aceste notiuni nu sint sinonime), ca si orice alta persoana, se pot opune efectuarii unor inregistrari (audio, video, foto) doar daca prin aceasta li se lezeaza dreptul la viata privata. Or, exercitarea obligatiilor de serviciu nu poate fi atribuita sub nici o forma la domeniul vietii lor private, prin urmare nu este necesar acordul lor pentru efectuarea filmarilor.

Totodata, in cazul in care, in cadrul unei discutii sau interviu, jurnalistul urmareste scopul de a obtine informatii de la persoana cu functie de raspundere sau functionar, el trebuie sa atentioneze persoana respectiva asupra efectuarii inregistrarilor (ceea ce nu inseamna ca jurnalistul trebuie sa solicite consimtamintul ei).

Este in drept persoana sa distruga materialul (caseta, filmul, fotografia etc.) pe care a fost inregistrata, fara acordul ei, informatia cu caracter personal? Poate persoana sa ceara distrugerea informatiei?

Noțiunile ce urmează de reținut:

protecția secretului de stat – complex de măsuri organizatorico-juridice, tehnico-inginerești, criptografice, operative de investigații și de altă natură, destinate prevenirii divulgării sau pierderii informațiilor atribuite la secret de stat;

purtători materiali de informații atribuite la secret de stat – obiecte materiale, inclusiv câmpuri fizice, în care informațiile atribuite la secret de stat sînt expuse în formă de texte, semne, simboluri, imagini, semnale, soluții tehnice, procese etc.;

secret de stat – informații protejate de stat în domeniul apărării naționale, economiei, științei și tehnicii, relațiilor externe, securității statului, asigurării ordinii de drept și activității autorităților publice, a căror divulgare neautorizată sau pierdere este de natură să aducă atingere intereselor și/sau securității Republicii Moldova.

Protejarea secretului de stat se realizează prin organizarea sistemului național de protecție a secretului de stat. Ele sînt executorii și pentru cetățenii străini și apatrizii care și-au asumat obligația sau sînt obligați, conform statutului lor, să execute prevederile legislației Republicii Moldova cu privire la secretul de stat.

Sistemul național de protecție a secretului de stat include totalitatea organelor de protecție a secretului de stat, a metodelor și mijloacelor de protejare a informațiilor și a purtătorilor materiali de informații atribuite la secret de stat, precum și totalitatea măsurilor întreprinse în acest domeniu.

Sistemul național de protecție a secretului de stat vizează:

- a) protecția juridică – ansamblul prevederilor conținute în actele legislative și normative ce reglementează protecția secretului de stat;
- b) protecția prin măsuri procedurale – ansamblul reglementărilor prin care deținătorii de informații atribuite la secret de stat stabilesc măsuri interne de lucru și de ordine interioară în vederea realizării protecției informațiilor;
- c) protecția fizică – ansamblul activităților de pază, de asigurare a securității și de apărare a informațiilor atribuite la secret de stat prin măsuri și mijloace de control fizic;
- d) protecția sistemelor informaționale și de telecomunicații – ansamblul activităților de asigurare a securității informațiilor atribuite la secret de stat prin aplicarea metodelor și mijloacelor criptografice și tehnice de protecție a informațiilor, precum și a procedurilor tehnico-organizatorice;
- e) protecția personalului – ansamblul verificărilor și al măsurilor ce vizează cetățenii cărora li se perfectează dreptul de acces la secretul de stat sau care au acces la acesta în scopul prevenirii și înlăturării riscurilor pentru securitatea și protecția secretului de stat.

Sistemul național de protecție a secretului de stat este destinat:

- a) să prevină accesul neautorizat, divulgarea și pierderea secretului de stat;
- b) să identifice împrejurările, precum și persoanele care, prin acțiunile sau inacțiunile lor, pot pune în pericol securitatea secretului de stat;
- c) să garanteze că informațiile atribuite la secret de stat sînt accesibile exclusiv persoanelor îndreptățite să le cunoască în legătură cu îndeplinirea atribuțiilor de serviciu sau în baza unui alt temei legal;

d) să asigure securitatea sistemelor de telecomunicații, a sistemelor informaționale și a rețelelor de transmitere a secretului de stat.

Gradul de secretizare a informațiilor atribuite la secret de stat trebuie să corespundă gravității prejudiciilor ce pot fi cauzate intereselor și/sau securității Republicii Moldova în cazul divulgării sau pierderii acestor informații.

Sînt stabilite 4 grade de secretizare a informațiilor atribuite la secret de stat și 4 parafe de secretizare corespunzătoare pentru purtătorii materiali de asemenea informații:

a) „Strict secret” – grad de secretizare atribuit informațiilor a căror divulgare neautorizată poate aduce prejudicii deosebit de grave intereselor și/sau securității Republicii Moldova;

b) „Secret” – grad de secretizare atribuit informațiilor a căror divulgare neautorizată poate dăuna grav intereselor și/sau securității Republicii Moldova;

c) „Confidențial” – grad de secretizare atribuit informațiilor a căror divulgare neautorizată poate dăuna intereselor și/sau securității Republicii Moldova;

d) „Restricționat” – grad de secretizare atribuit informațiilor a căror divulgare neautorizată poate fi în dezavantajul intereselor și/sau securității Republicii Moldova sau poate să conducă la divulgarea unei informații secretizate cu parafa „Strict secret”, „Secret” sau „Confidențial”.

Prin secret comercial se înțeleg informațiile ce nu constituie secret de stat, care țin de producție, tehnologie, administrare, de activitatea financiară și de altă activitate a agentului economic, a căror divulgare (transmitere, scurgere) poate să aducă atingere intereselor lui.

Informațiile ce constituie secret comercial sînt proprietate a agentului antreprenoriatului sau se află în posesia, folosința sau la dispoziția acestuia în limitele stabilite de el în conformitate cu legislația.

Informațiile ce constituie secret comercial trebuie să corespundă următoarelor cerințe:

a) să aibă valoare reală sau potențială pentru agentul antreprenoriatului;

b) să nu fie, conform legislației, notorii sau accesibile;

c) să aibă mențiunea ce ar corespunde cu desfășurarea de către agenții antreprenoriatului a măsurilor respective necesare pentru păstrarea confidențialității lor prin aplicarea sistemului de clasificare a informațiilor date, elaborarea regulamentelor interne de secretizare, marcarea corespunzătoare a documentelor și altor purtători de informație, organizarea lucrărilor secrete de secretariat;

d) să nu constituie secret de stat și să nu fie protejate de dreptul de autor, de drepturile conexe și de brevetul de invenție;

e) să nu conțină informații despre activitatea negativă a persoanelor fizice și juridice care ar putea atinge interesele statului.

Prin divulgare a secretului comercial se înțeleg acțiunile intenționate sau din imprudență ale funcționarilor publici, demnitarilor de stat, lucrătorilor agentului economic, precum și ale altor persoane care dispun de informații ce constituie secret comercial care le-au fost încredințate sau le-au devenit cunoscute în legătură cu serviciul sau munca lor, ce au condus la dezvăluirea prematură, folosirea și răspândirea necontrolată a acestora.

Obiectele secretului comercial

(1) Obiecte ale secretului comercial (know-how) sînt interesele economice și informațiile tănuite intenționat despre diferitele aspecte și domenii ale activității economice de producție, de administrare, tehnico-științifice, financiare a agentului economic, a căror protecție este condiționată de interesele concurenței și posibila periclitate a securității economice a agentului economic.

(2) Atribuirea neîntemeiată a informației accesibile la secret comercial este interzisă.

(3) Conținutul și volumul de informații ce constituie secret comercial sînt stabilite de agentul antreprenoriatului.

(4) Obiecte ale secretului comercial nu pot fi:

a) documentele de constituire, precum și documentele ce dau dreptul de a practica activitate de antreprenoriat și anumite tipuri de activitate economică ce urmează a fi licențiate;

b) informațiile în forma stabilită a dărilor de seamă statistice, precum și a dărilor de seamă privind exercițiul economico-financiar și alte date necesare pentru verificarea corectitudinii calculării și achitării impozitelor și a altor plăți obligatorii;

c) documentele de achitare a impozitelor, a altor plăți la bugetul public național;

d) documentele care atestă solvabilitatea;

e) informațiile privind componența numerică și structura personalului, salariul lucrătorilor, condițiile de muncă, precum și cele privind disponibilitatea locurilor de muncă;

f) informațiile cu privire la poluarea mediului înconjurător, încălcarea legislației antimonopol, nerespectarea regulilor de protecție a muncii, comercializarea producției care dăunează sănătății consumatorilor, precum și cu privire la alte încălcări ale legislației și mărirea prejudiciului cauzat.

Nu constituie obiecte ale secretului comercial al întreprinderilor de stat și municipale pînă la privatizare și în procesul privatizării datele privind:

a) volumul proprietății întreprinderii și al mijloacelor ei bănești;

b) investirea mijloacelor în activele rentabile (hârții de valoare) ale altor întreprinderi, în obligații și împrumuturi, în fondurile statutare ale întreprinderilor mixte;

c) obligațiile de credit, comerciale și alte obligații ale întreprinderii, care decurg din legislație, și din contractele încheiate de ea;

d) contractele cu întreprinderile nestatale.

Subiecții secretului comercial elaborează instrucțiuni, regulamente privind asigurarea păstrării secretului comercial în care se stabilesc:

a) conținutul și volumul informațiilor ce constituie secret comercial;

b) modul de atribuire informațiilor, lucrărilor și articolelor a mențiunii "Secretul întreprinderii" și de scoatere a acestei mențiuni;

c) procedura admiterii lucrătorilor agentului economic, precum și a persoanelor antrenate în activitatea lui, la informațiile ce constituie secret comercial;

d) modul de folosire, evidență, păstrare și marcarea a documentelor și a altor purtători de informație, a articolelor, obiectul cărora constituie secret comercial;

e) organizarea controlului asupra modului de folosire a informațiilor ce constituie secret comercial;

f) procedura de asumare a obligațiilor reciproce de către agenții economici privind păstrarea secretului comercial la încheierea contractelor de desfășurare a unor acțiuni comune;

g) modul de aplicare a măsurilor de influență disciplinară și materială prevăzute de legislația asupra lucrărilor care au divulgat secretul comercial;

h) punerea răspunderii pentru asigurarea păstrării secretului comercial în seama persoanei cu funcții de răspundere a agentului economic.

Un sistem judiciar viabil reprezintă principala componentă a societății democratice, deoarece el vizează toate domeniile vieții sociale. Iată de ce problemele înfăptuirii justiției în Republica Moldova continuă să rămână un deziderat important, care merită atenție și consolidarea eforturilor comune în vederea reafirmării imaginii țării pe plan internațional, inclusiv în contextul vectorului de integrare europeană.

Respectarea drepturilor omului în sectorul justiției este unul dintre pilonii de bază de care se fundamentează reforma sectorului justiției. Astfel, Parlamentul Republicii Moldova în anul 2012 a adoptat un set de legi prin care a modificat unele prevederi din Codul de procedură civilă și Codul de procedură penală precum și alte legi de incidență în contextul reformei, menite să eficientizeze într-o măsură mai mare accesul liber la justiție și dreptul la

un proces echitabil. Efectul modificărilor operate în opinia avocaților parlamentari vor putea fi apreciate în timp.

De remarcat că procedurile penale și civile au multe tangențe între ele, fiind ghidate de multiple principii și norme procesuale comune. Pentru a statua conceptul transparenței și publicității ședințelor de judecată, e suficient de citat prevederile art. 10 din Legea RM privind organizarea judecătorească „Caracterul public al dezbaterilor judecătorești și principiul contradictorialității” și art. 23 Cod Procedură Civilă al RM „Caracterul public al dezbaterilor judiciare”. Art. 10 din Legea RM privind organizarea judecătorească stabilește caracterul public al ședințelor de judecată. Ședințele închise au loc doar în cazurile expres prevăzute de lege, cu respectarea întocmai a procedurii judiciare. Art. 23 Cod de Procedură Civilă a RM prevede: În toate instanțele, ședințele de judecată sunt publice. În ședința de judecată nu se admit minorii de până la vârsta de 16 ani dacă nu sunt citați în calitate de participanți la proces sau de martor. Pot avea loc ședințe închise numai în scopul protejării informației ce constituie secret de stat, taină comercială ori a unei alte informații a cărei divulgare este interzisă prin lege. Instanța de judecată poate dispune judecarea pricinii în ședință secretă pentru a preveni divulgarea unor informații care se referă la aspectele intime ale vieții, care lezează onoarea, demnitatea sau reputația profesională ori la alte circumstanțe care ar putea prejudicia interesele participanților la proces, ordine publică sau moralitate. Ședința poate fi declarată secretă pentru întregul proces sau numai pentru efectuarea unor anumite acte procedurale. Privitor la examinarea pricinii în ședință secretă, instanța judecătorească emite o încheiere motivată. Ședința secretă se desfășoară în prezența participanților la proces, iar în caz de necesitate la ea asistă de asemenea martorul, expertul, specialistul și interpretul.

Instanța judecătorească ia măsurile de rigoare în vederea păstrării secretului de stat, tainei comerciale, informației despre viața intimă a persoanei. Participanții la proces și alte persoane care asistă la actele procesuale în cadrul cărora pot fi divulgate date ce constituie astfel de secrete sunt somați de răspundere în cazul divulgării lor. Judecarea pricinii în ședință secretă se efectuează cu respectarea tuturor regulilor de procedură civilă. Hotărârile ședinței secrete oricum se pronunță public. În cazul dezbaterii pricinii în ședință secretă, pot fi eliberate unor alte persoane decât părțile copii de pe încheieri, rapoarte de expertiză sau declarații ale martorilor doar cu permisiunea dată de președintele ședinței.

Articolul 18 [Cod de Procedură Penală a Republicii Moldova](#) “[Caracterul public al ședințelor de judecată](#)” statuează că în toate instanțele judecătorești ședințele sunt publice, cu excepția cazurilor prevăzute de prezentul articol. Accesul în sala de ședință poate fi interzis

presei sau publicului, prin încheiere motivată, pe parcursul întregului proces sau al unei părți din proces, în interesul respectării moralității, ordinii publice sau securității naționale, când interesele minorilor sau protecția vieții private a părților în proces o cer, sau în măsura considerată strict necesară de către instanță când, datorită unor împrejurări speciale, publicitatea ar putea să prejudicieze interesele justiției. În procesul în care un minor este victimă sau martor, instanța de judecată va asculta declarațiile acestuia într-o ședință închisă. Judecarea cauzei în ședința închisă a instanței trebuie argumentată și efectuată cu respectarea tuturor regulilor procedurii judiciare.

În toate cazurile, hotărârile instanței de judecată se pronunță în ședință publică.

Art. 14 din [Legea RM privind organizarea judecătorească](#) prevede dreptul la utilizarea mijloacelor tehnice. Ședințele de judecată se înregistrează prin utilizarea mijloacelor tehnice video sau audio ori se consemnează prin stenografiere. Înregistrările și stenogramele se transcriu de îndată. Înregistrarea audio și/sau video a ședințelor de judecată se realizează în modul stabilit de Consiliul Superior al Magistraturii. Grefierul sau specialistul în stenografie consemnează toate afirmațiile, întrebările și susținerile participanților la proces și ale altor persoane care participă la judecarea cauzei, precum și ale judecătorilor. Înregistrarea audio și video, fotografierea, precum și utilizarea altor mijloace tehnice, de către participanții la proces și de către alte persoane se admit numai în condițiile legii procesuale.

Codul de procedură civilă mult mai în detaliu reglementează folosirea mijloacelor tehnice pentru înregistrarea lucrărilor ședințelor de judecată (vezi art. 18 Cod Procedură Civilă). Potrivit acestei norme, pentru documentarea lucrărilor ședinței de judecată și conservarea probelor, instanța judecătorească poate utiliza orice mijloc tehnic în conformitate cu prezentul cod și alte legi. Pentru exercitarea drepturilor și obligațiilor procesuale, participanții la proces pot efectua înregistrarea audio a ședinței de judecată. Înregistrarea video, fotografierea, utilizarea altor mijloace tehnice decât cele cerute în condițiile alin. (11) art. 18 Cod Procedură Civilă pot fi admise numai de președintele ședinței de judecată și numai la deschiderea ședinței și pronunțarea hotărârii. Încălcarea prevederilor alin.(2) se sancționează cu amendă de până la 20 unități convenționale și cu confiscarea înregistrărilor (peliculei, pozelor, casetelor etc.).

Accesul la materialele dosarelor aflate în curs de examinare are loc în baza prevederilor Codului procedură civilă și Codului procedură penală, legislației în vigoare ce reglementează accesul la informație, secretul de stat, secretul comercial, cu privire la avocatură și alte acte normative. Având în vedere specificul și volumul mare al informației

cercetate în cadrul ședințelor de judecată, accesul la materialele dosarelor aflate în examinarea instanțelor judecătorești poate fi unul dificil.

Regulile privind accesul la date și informații ce se conțin în dosare depind de statutul procesual al acestora. Părților pe proces și participanților procesuali, accesul la materialele dosarului le este garantat de Codurile procesuale, deoarece accesul la materialele dosarelor este un drept procesual al acestora. Pentru restul persoanelor, accesul la materialele dosarelor deja examinate sau aflate în examinare li se asigură parțial în baza Legii RM privind accesul la informație, pe când codurile procesuale se referă doar la unele aspecte specifice, așa cum secretul urmăririi penale, secretizarea informației în scopul protecției părții vătămate, martorilor și altor persoane ce conlucrează cu organul de urmărire penală pe cauze penale. Reieșind din specificul și importanța majoră pe care le reprezintă asemenea categorii de dosare, anume în acest context merită de evidențiat și faptul, că potrivit art. 20 din Legea presei, ce reglementează drepturile și obligațiile jurnalistului în scopul exercitării atribuțiilor sale profesionale este în drept să obțină și să difuzeze informații, să fie primit în audiență de persoane oficiale, să facă imprimări audiovizuale, să filmeze și să fotografieze, să asiste la ședințele publice ale instanțelor de judecată de orice nivel, să aibă acces în zonele calamităților naturale, să asiste la mitinguri, demonstrații și la alte manifestații publice, să se adreseze oricărei instituții pentru a verifica faptele și circumstanțele vizate în anumite materiale, să renunțe la pregătirea și semnarea unui material, dacă acesta vine în contradicție cu convingerile sale, să-și retragă semnătura de sub un material al cărui conținut, după părerea sa, a fost denaturat în procesul redactării, să ceară păstrarea secretului paternității (de autor), să beneficieze de facilități și proprietăți la transport și telecomunicații, la cazare în hoteluri pe teritoriul republicii.

Confiscarea notițelor jurnalistului este interzisă. Mijloacele lui tehnice pot fi ridicate numai în cazul în care servesc drept probă într-o cauză penală.

Obiectivele de referință

- să stabilească particularitățile reglementării juridice în domeniul securității informaționale a societății și a personalității;
- să determine semnele distinctive ale producției erotice și pornografice;
- să formuleze elementele vieții private și să ofere o caracterizare generală a vieții private;
- să definească secretul de stat și secretul comercial;
- să evidențieze principiile libertății de exprimare în domeniul reflectării activității

organelor de ocrotire a normelor de drept.

Bibliografie:

Acte normativ-juridice

1. Constituția Republicii Moldova adoptată la 29.07.1994 (M.O. nr.1 din 12.08.1994);
2. Legea serviciului public nr.443-XIII din 4 mai 1995;
3. Legea nr.982-XIV din 11 mai 2000 privind accesul la informație;
4. Legea nr.467-XV din 21 noiembrie 2003 cu privire la informatizare și la resursele informaționale de stat;
5. Legea nr.264-XV din 15 iulie 2004 cu privire la documentul electronic și semnătura digitală;
6. Legea Republicii Moldova cu privire la protecția datelor cu caracter personal nr. 17 din 15.02.2007, publicată în Monitorul Oficial Nr. 107-111 art Nr : 468
7. 7.Legea Republicii Moldova cu privire la informatică nr.1069-XIV din 22.06.2001, publicată în Monitorul Oficial nr.73-74 din 05.07.2001
8. Legea Republicii Moldova privind comerțul electronic nr. 2488-XV din 223 iulie 2004, publicată nr. 138-146 din 13 august 2004
9. Legea Republicii Moldova cu privire la registre nr. 1320-XIII din 25.09.1997
10. Legea Republicii Moldova cu privire la telecomunicații nr.520-XIII din 07.07-1995
11. Legea Republicii Moldova cu privire la actele de stare civilă nr.100-XV din 26.04.2001
12. Legea Republicii Moldova cu privire la actele de identitate din sistemul național de pașapoarte nr.273-XIII din 09.11.1994

Decretele Președintelui Republicii Moldova

- Privind edificarea societății informaționale în Republica Moldova nr.1743-III din 19.03. 2004
- Decretul Președintelui cu privire la crearea Sistemului național de pașapoarte și Registrului de Stat al populației nr. 144 din 20.09.1993

Hotărârile Guvernului Republicii Moldova

- Hotărîre cu privire la aprobarea Concepției Sistemului informațional automatizat "Registrul informației criminalistice și criminologice"
- Hotărîre cu privire la aprobarea Concepției Sistemului informațional automatizat "Registrul de stat al armelor"
- Hotărîre cu privire la aprobarea Concepției Sistemului informațional automatizat "Registrul de stat al accidentelor rutiere"
- Hotărîre cu privire la unele acțiuni de implementare a Strategiei Naționale de edificare a societății informaționale - "Moldova electronică" în anul 2007 nr. 606 din 01.06.2007 (Monitorul Oficial nr.78-81/640 din 08.06.2007)
- Hotărîre cu privire la transmiterea unui imobil nr.184 din 20.02.2007 (Monitorul Oficial nr.29-31/200 din 02.03.2007)
- Hotărîre cu privire la Intreprinderea de Stat Registrul animalelor nr. 119 din 07.02.2007 Monitorul Oficial nr.21-24/135 din 16.02.2007
- Hotărîre cu privire la Registrul de stat al actelor juridice al Republicii Moldova nr. 1381 din 07.12.2006 (Monitorul Oficial nr.189-192/1475 din 15.12.2006)
- Hotărîre cu privire la aprobarea Concepției sistemului informațional automatizat "Registrul funcțiilor publice și al funcționarilor publici" nr. 1373 din 01.12.2006 (Monitorul Oficial nr.189-192/1471 din 15.12.2006)
- Hotărîre cu privire la sistemul informațional automatizat "Registrul de stat al circulației alcoolului etilic și a producției alcoolice" nr. 1255 din 31.10.2006 (Monitorul Oficial nr.170-173/1340 din 03.11.2006)
- Hotărîre cu privire la transmiterea unui imobil nr. 1228 din 23.10.2006 (Monitorul Oficial nr.170-173/1319 din 03.11.2006)
- Hotărîre cu privire la aprobarea Concepției Sistemului informațional integrat al organelor de drept nr. 1202 din 17.10.2006 (Monitorul Oficial nr.168-169/1293 din 27.10.2006)
- Hotărîre cu privire la aprobarea Concepției sistemului informațional automatizat "Registrul resurselor și sistemelor informaționale de stat" nr. 1032 din 06.09.2006 (Monitorul Oficial nr.150-152/1131 din 22.09.2006)
- Hotărîre pentru aprobarea Regulamentului cu privire la evidența de stat a organelor centrale de specialitate ale administrației publice nr. 1004 din 29.08.2006 (Monitorul Oficial nr. 142-145/1087 din 08.09.2006)

- Hotărîre pentru aprobarea Regulamentului privind mecanismul de realizare a Planului de acțiuni "Moldova electronică" Nr.27 din 06.01.2006 (Monitorul Oficial al R.Moldova nr.9-12/59 din 20.01.2006)
- Dispoziție Nr.70-d din 21.07.2005 (Monitorul Oficial al R.Moldova nr.98-100/779 din 22.07.2005)
- Hotărîre cu privire la aprobarea Regulamentului Ministerului Dezvoltării Informaționale Nr.30 din 10.01.2006 (Monitorul Oficial al R.Moldova nr.13-15/85 din 24.01.2006)
- HOTĂRÎREA GUVERNULUI REPUBLICII MOLDOVA privind aprobarea modificărilor ce se operează în Hotărîrea Guvernului nr.21 din 16 ianuarie 2003 Nr.45 din 19.01.2005 (Monitorul Oficial al R.Moldova nr.13-16/95 din 21.01.2005)
- Hotărîre cu privire la actele de identitate ale refugiaților Nr.626 din 28.06.2005 (Monitorul Oficial al R.Moldova nr.95-97/715 din 15.07.2005)
- Hotărîre cu privire la aprobarea structurii și efectivului-limită ale aparatului central al Ministerului Dezvoltării Informaționale Nr.606 din 24.06.2005 (Monitorul Oficial al R.Moldova nr.89-91/668 din 01.07.2005)
- HOTĂRÎRE cu privire la aprobarea modificărilor și completărilor ce se operează în Hotărîrea Guvernului nr.376 din 6 iunie 1995 nr. 571 din 23.05.2006 (Monitorul Oficial nr. 83-86/615 din 02.06.2006)
- HOTĂRÎRE cu privire la crearea sistemelor și resurselor informaționale automatizate de stat nr. 562 din 22.05.2006 (Monitorul Oficial nr. 79-82/591 din 26.05.2006)
- HOTĂRÎREA GUVERNULUI REPUBLICII MOLDOVA Hotărîre cu privire la crearea sistemului informațional automatizat "Nomenclatorul de stat al medicamentelor" Nr.549 din 07.06.2005 (Monitorul Oficial al R.Moldova nr.83-85/605 din 17.06.2005)
- Hotărîre pentru aprobarea Acordului între Guvernul Republicii Moldova și Guvernul Republicii Azerbaidjan cu privire la colaborarea în domeniul informatizării și tehnologiilor informaționale, semnat la 21 aprilie 2005 la Chișinău Nr.661 din 08.07.2005 (Monitorul Oficial al R.Moldova nr.95-97/722 din 15.07.2005)

- Hotărîre cu privire la aprobarea componenței nominale a Colegiului Ministerului Dezvoltării Informaționale Nr.782 din 01.08.2005 (Monitorul Oficial al R.Moldova nr.104-106/846 din 05.08.2005)
- HOTĂRÎRE cu privire la modificarea Hotărîrii Guvernului nr.959 din 9 septembrie 2005 nr. 805 din 10.07.2006 (Monitorul Oficial nr. 106-111/838 din 14.07.2006)
- Hotărîre cu privire la aprobarea modificărilor și completărilor ce se operează în Hotărîrea Guvernului nr.197 din 12 martie 2001 Nr.833 din 08.08.2005 (Monitorul Oficial al R.Moldova nr.110-112/903 din 19.08.2005)
- Hotărîre pentru aprobarea modificării ce se operează în Hotărîrea Guvernului nr.179 din 20 februarie 2003 Nr.883 din 19.08.2005 (Monitorul Oficial al R.Moldova nr.113-116/955 din 26.08.2005)
- HOTĂRÎRE Cu privire la măsurile de asigurare a confirmării cetățeniei și documentării populației din localitățile din stînga Nistrului (Transnistria) Nr.959 din 09.09.2005 (Monitorul Oficial al R.Moldova nr.123-125/1032 din 16.09.2005)
- Hotărîre privind modificarea Hotărîrii Guvernului nr.735 din 16 iunie 2003 Nr.1063 din 07.10.2005 (Monitorul Oficial al R.Moldova nr.135-138/1142 din 14.10.2005)
- Hotărîre cu privire la aprobarea Concepției Sistemului informațional automatizat "Registrul de stat al blanchetelor de strictă evidență și al timbrelor de acciz" Nr.1100 din 25.10.2005 (Monitorul Oficial al R.Moldova nr.145-147/1191 din 04.11.2005)
- Hotărîre cu privire la aprobarea modificărilor ce se operează în anexa nr.1 la Hotărîrea Guvernului nr.376 din 6 iunie 1995 Nr.286 din 17.03.2006 (Monitorul Oficial al R.Moldova nr.47-50/320 din 24.03.2006)
- Hotărîre cu privire la Pagina Oficială a Republicii Moldova în rețeaua Internet nr. 765 din 05.07.2006 (Monitorul Oficial nr. 106-111/819 din 14.07.2006)
- Hotărîre cu privire la Concepția guvernării electronice nr. 733 din 28.06.2006 (Monitorul Oficial nr. 106-111/799 din 14.07.2006)
- Hotărîre privind paginile oficiale ale autorităților administrației publice în rețeaua Internet nr. 668 din 19.06.2006 (Monitorul Oficial nr. 98-101/726 din 30.06.2006)

- Hotărîrea Guvernului Republicii Moldova pentru aprobarea Regulamentului privind mecanismul de realizare a Planului de acțiuni "Moldova electronică" № 27 din 06.01.2006
- Hotărîrea Guvernului Republicii Moldova Nr.959 din 09.09.2005 "cu privire la măsurile de asigurare a confirmării cetățeniei și documentării populației din localitățile din stînga Nistrului (Transnistria)"
- Hotărîrea Guvernului Republicii Moldova "Cu privire la modificarea Hotărîrii Guvernului № 21 din 16 ianuarie 2003" № 645 din 4 iulie 2005
- Hotarirea Guvernului Republicii Moldova "Privind Strategia Națională de edificare a societății informaționale - „Moldova electronică” № 255 din 09.03.2005 "
- Regulamentul "Cu privire la modul de elaborare a sistemelor informaționale automatizate de importanță statală "
- Hotarirea Guvernului Republicii Moldova cu privire la crearea sistemului informațional automatizat "Registrul de stat al documentelor, mărcilor de acciz și blanchetelor de strictă evidență" № 1392 din 16.12.2004
- Hotărîrea Guvernului Republicii Moldova despre măsurile privind crearea sistemului informațional automatizat "Registrul de stat al unitatilor de drept" № 272 din 6.03.2002
- Hotarirea Guvernului Republicii Moldova cu privire la stabilirea termenului de valabilitate a actelor de identitate de tip vechi № 21 din 16.01.2003
- Hotărîrea Guvernului Republicii Moldova cu privire la crearea Sistemului Informațional Geografic Național Nr.1298 din 28.10.2003
- Hotărîrea Guvernului Republicii Moldova despre crearea Sistemului informațional automatizat "Registrul de stat al unităților administrativ-teritoriale și al străzilor din localitățile de pe teritoriul Moldovei" Nr.1518 din 17.12.2003
- Hotarirea Guvernului Republicii Moldova cu privire la aprobarea Concepției și Regulamentului cu privire la sistemul informațional automatizat de evidență și control al persoanelor, mijloacelor de transport și marfurilor (incarcaturilor), care trec frontiera de stat și/sau vamala "FRONTIERA" № 1126 din 28.08.2002

- Hotărîrea Guvernului Republicii Moldova cu privire la crearea sistemului informational automatizat "Registrul de stat al conducătorilor de vehicule " № 1058 din 6.08.2002
- Hotărîrea Guvernului Republicii Moldova "Cu privire la aprobarea și punerea în aplicare a tipurilor mecanolizabile de permis de conducere și certificat de înmatriculare a mijloacelor de transport Nr.778 din 20.11.95"
- Hotărîrea Guvernului Republicii Moldova "Cu privire la stabilirea termenului de valabilitate a actelor de identitate de tip vechi" Nr.21 din 16.01.2003
- Regulamentul Comisiei Naționale "Pentru Edificarea Societății Informaționale în Republica Moldova"
- Hotărîrea Guvernului Republicii Moldova "Despre aprobarea Politicii de edificare a societății informaționale în Republica Moldova" 1
- Hotărîrea Guvernului Republicii Moldova "Privind aprobarea Politicii naționale în domeniul telecomunicațiilor Nr.975 din 13.09.2001"
- Hotărîrea Guvernului Republicii Moldova cu privire la măsurile suplimentare de realizare a Sistemului național de pașapoarte Nr. 376 din 06.06.95
- Hotărîrea Guvernului Republicii Moldova cu privire la funcțiile de baza, structura și statele de personal ale Departamentului Tehnologii Informaționale nr. 650 din 16.07.2001
- Hotărîrea Guvernului Republicii Moldova cu privire la Departamentul Tehnologii Informaționale nr.398 din 06.06.2001
- Hotărîrea Guvernului Republicii Moldova pentru aprobarea Concepției sistemului informațional automatizat "Registrul de stat al populației" și Regulamentului cu privire la Registrul de stat al populației nr. 333

Literatura teoretică:

1. I. VASIU, L. VASIU, *Informatică juridică și drept informatic 2005*, Ed. Albastră, Cluj-Napoca, 2005.
2. I. VASIU, *Criminalitatea informatică*, Ed. Nemira, București, 2001.
3. V. PATRICIU, I. VASIU, G. PATRICIU, *Internetul și Dreptul*, Ed. All Beck, București, 1999.
4. I. VASIU, L. VASIU, *Frauda informatică*, *Revista Română de Drept Penal*, Nr. 1, 2005.
5. I. VASIU, L. VASIU, *Protecția datelor personale*, *Revista Română de Drept Penal*, Nr. 2, 2005.

6. I. VASIU, L. VASIU, Aspecte legale privind sistemul numelor de domenii Internet, *Revista Română de Dreptul Proprietatii Intelectuale*, Anul II, Nr. 1 (3), Iunie, 2005.
7. I. VASIU, L. VASIU, Pirateria informatică, *Revista Română de Dreptul Proprietății Intelectuale*, Anul II, Nr. 1 (2), Martie, 2005.
8. I. VASIU, L. VASIU, Comerțul electronic și sistemul proprietății intelectuale, *Revista Română de Dreptul Proprietății Intelectuale*, Anul II, Nr. 2, Iunie, 2005.
9. L. VASIU, I. VASIU, Riscul de atac electronic asupra sistemelor de informații, Publicată în Fenomene și procese cu risc major la scară națională (Coord. F. Gh. Filip, B. C. Simionescu), Ed. Academiei Române, 2004 - Parte a Proiectului International FP 6 (al 6-lea Program Cadru European de Cercetare-Dezvoltare).
10. I. VASIU, L. VASIU, Un cadru holohedral pentru protejarea tehnică a proprietății intelectuale digitale, *Revista Română de Dreptul Proprietății Intelectuale*, Anul III, 2006.
11. I. VASIU, L. VASIU, *Totul despre hackeri*, Ed. Nemira, 2001.
12. I. VASIU, L. VASIU, The Romanian Integrated Justice Information System, Abstract publicat in *Proceedings of the OECD Seminar Implementing High Quality Regulation: Communication, Compliance and Enforcement*, Ljubljana, Slovenia, 2004.
13. L. VASIU, I. VASIU, Dissecting Computer Fraud: From Definitional Issues to a Taxonomy, Publicata în *Proceedings of the 37th Hawaii International Conference on System Sciences*, Hawaii, USA, IEEE Computer, 2004.
14. L. VASIU, I. VASIU, A Taxonomy of Malware Use in the Perpetration of Computer-related Fraud', In U.E. Gattiker (Ed.), *EICAR 2004 Conference: Best Paper Proceedings*, Copenhagen
15. Ruxandra Anescu, Vlad Anescu - *Comerțul electronic* - Tribuna Economică, nr.4/2003
16. Alexandru Bleoanca – *Comunicările comerciale efectuate prin posta electronica* – Revista de Drept Comercial 2/2003 pag. 104-112
17. Dumitru Mazilu - *Adaptarea legislației românești la exigențele actuale privind schimburile comerciale prin mijloace electronice* - Revista de Drept Comercial, nr.11/2002
18. Valeriu Stoica, Alexandru Bleoancă - *Enumerarea din lista cuprinsă în anexa la Ordonanța Guvernului nr.130/2000 privind regimul juridic al contractelor la distanță este limitativă sau exemplificativă?* - Revista de Drept Comercial, nr.11/2002

19. Tiberiu Gabriel Savu - *Unele considerații pe marginea efectelor noii reglementări privind comerțul electronic asupra regulilor în materia formării contractului* - Revista de Drept Comercial, nr.9/2002
20. Tiberiu Gabriel Savu - *Consacrarea legală a semnăturii electronice*, în Revista de Drept Comercial, nr.7-8/2002
21. Cristian Adochitei – *Infractiuni pe Internet – Hartuirea electronica* – Revista Dreptul 7/2002 pag 49-52
22. Horatiu Dan Dumitru, Catalin Baiculescu – *Legea privind comerțul electronic* – Pandectele Romane 6/2002, 1/2003, 2/2003
23. Ioan I. Bălan - *Contractele la distanță și protecția consumatorilor* - Dreptul nr.1/2002
24. Moise Bojinca – *Contractele comerciale la distanta* – Revista de Drept Comercial 1/2002 pag. 86-90
25. Ioan Schiau – *Cadrul Juridic al comerțului electronic* – Revista de Drept Comercial nr 1/2002 pag 56-72
26. Camelia-Tatiana Ciulei – *Consideratiuni privind aspectele juridice pe care le implica crearea unui site comercial pe Internet* – Revista de Drept Comercial nr. 10/2001 pag 84-94
27. Centrul de Resurse Juridice din Bucuresti - *Protectia sferei private in Internet* – Revista de Drept Comercial 7-8/2001 pag. 255-285 si Revista de Drept Comercial 9/2001 pag. 91-125
28. Camelia Tatiana Ciulei - *Probleme juridice legate de introducerea semnăturii electronice si folosirea ei in tranzactiile pe Internet* – Revista de Drept Comercial nr. 6/2001 pag. 88-95
29. Catalin Predoiu, Anca Maria Șandru - *Comerțul prin internet. Studiu economic si juridic* - Juridica nr. 10/2000 pag 377-385
30. Cornelia Rotaru – *Consideratiuni privind protectia drepturilor de proprietate intelectuala pe Internet* – Revista de Drept Comercial nr. 7-8/2000
31. Bogdan Boreschievici, Daniel Plosca, Daniel Dumitru – *Marca vs DNS – Probleme noi in protectia proprietatii industriale* - Revista Romana de Proprietate Industriala nr. 4/1997 si nr. 5/1997

TEMA 11. Protecția sistemelor informaționale și a dreptului asupra sistemelor informaționale

1. Impactele de bază asupra sistemelor informaționale și a drepturilor de acces la acestea

2. Protecția dreptului la sistemul informațional

3. Particularitățile reglementării juridice a relațiilor în Internet

4. Protecția juridică sistemelor informaționale și a drepturilor asupra acestora

Obiectivele de referință

- să identifice șirul de obiecte protejate prin intermediul normelor juridice informaționale;
- să determine particularitățile reglementării juridice a relațiilor în Internet;
- să stabilească impactele și riscurile de utilizare a sistemelor informaționale și să prezinte soluții de ocolire a acestora.

