

PAZA INSTITUȚIILOR

Paza instituțiilor reprezintă un segment important al activității tuturor structurilor din Sistemul Național de Apărare, precum și obiectul de activitate a numeroase societăți private. Importanța acestei misiuni rezultă din necesitatea asigurării la nivelul întregii țări a unui climat de ordine și siguranță publică, care reprezintă garanția existenței și dezvoltării statului național român, ca stat suveran, unitar, independent și indivizibil și a exercitării neîngrădite a drepturilor, libertăților și îndatoririlor fundamentale ale cetățenilor.

În condițiile situației operative actuale, caracterizată prin creșterea ratei criminalității, amplificarea fenomenului terorist pe plan internațional și a crimei organizate, între sarcinile încredințate Jandarmeriei Române, ca structură specializată a statului, în paza obiectivelor, bunurilor și valorilor, trebuie să sporească aportul adus la siguranța și integritatea sediilor instituțiilor.

Aderarea României la structurile militare euro-atlantice și iminenta integrare în Uniunea Europeană, determină abordarea într-o manieră nouă a problemei pazei obiectivelor, atât la nivel ministerial, cât și guvernamental.

Diversitatea și multitudinea obiectivelor la care trebuie asigurată paza, este în concordanță cu varietatea argumentelor ce susțin opțiunea menținerii măsurilor de pază, protecție și intervenție, în locuri și în condiții speciale când există o stare de pericol, de amenințare sau de risc major din partea unor factori de natură să pună în pericol siguranța acestora, a personalului care-și desfășoară activitatea în ele și a instalațiilor.

Această susținere are la bază următoarele **argumente**:

- necesitatea protejării fizice a bunurilor și sediilor unde își desfășoară activitatea structurile administrative și de putere ale statului;
- protecția și asigurarea climatului de muncă a demnitarilor români, precum și a celor străini, pe timpul cazării sau desfășurării unor activități protocolare, în condiții de liniște, ordine și de maximă siguranță;
- descurajarea oricăror încercări de atentat îndreptate împotriva demnitarilor sau a oricăror forme de agresiune, de natură infracțională sau teroristă;
- asigurarea înfăptuirii actului de justiție în condiții de ordine și siguranță;
- protecția fizică a sediilor instanțelor judecătorești, parchetelor și a documentelor necesare înfăptuirii actului de justiție;
- protecția și asigurarea climatului de muncă al magistraților;
- necesitatea protejării valorilor importante ale statului român (tezaur și rezerva valutară);
- protecția valorilor importante pe timpul colectării și transportului acestora, precum și asigurarea unui climat de ordine și siguranță pe timpul efectuării operațiunilor bancare;

- menținerea siguranței și protecției conductelor magistrale de transport produse petroliere amenințate de unele vulnerabilități și riscuri;
- necesitatea creșterii gradului de siguranță a transporturilor speciale de armament, muniție, substanțe explozive și periculoase aflate în atenția grupărilor de infractori sau chiar a celor teroriste;
- tendința unor grupări de persoane de a sustrage documente de arhivă cu repercusiuni grave asupra siguranței fondului arhivistic, deosebit de important atât pentru stat, cât și pentru cetățenii acestuia, impune măsuri sporite de pază.

Pentru alinierea la standardele statelor Uniunii Europene, România trebuie să-și revizuiască actualele criterii de stabilire a obiectivelor a căror pază se asigură cu efective de jandarmi. Trebuie excluse din competența Jandarmeriei Române bunurile și valorile deținute de persoane fizice și juridice, care pot fi păzite cu gardieni publici, cu pază proprie sau societăți private de pază.

Jandarmeria Română trebuie să asigure în continuare doar paza unităților bugetare, a sediilor misiunilor diplomatice și a unităților de interes strategic, care dețin instalații ori obiective de o deosebită importanță națională.

Sediul principal al materiei în problematica pazei instituțiilor îl reprezintă Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanei.

Referitor la instituțiile care necesită a fi asigurate cu pază, Legea nr. 333/2003 în art. 2 face o enumerare a acestora, astfel: „Ministerele și celelalte organe de specialitate ale administrației publice, centrale și locale, regiile autonome, companiile și societățile naționale, institutele naționale de cercetare-dezvoltare, societățile comerciale, indiferent de natura capitalului social, precum și alte organizații care dețin bunuri, ori valori cu orice titlu, denumite în prezenta lege unități, sunt obligate să asigure paza acestora”.

Deși legea se referă doar la unitățile care dețin valori cu orice titlu, formularea restrânge categoria instituțiilor beneficiare de pază, precum și a celor obligate să asigure paza numai la cele ale căror valori sunt cuantificabile din punct de vedere patrimonial. Pentru a fi mai cuprinzători vom interpreta textul de lege în sens larg prin includerea între instituțiile în cauză a tuturor obiectivelor care prezintă importanță pentru siguranța națională a României, precum și a celor care dețin sau manipulează informații clasificate, de orice natură.

Comandamentul Național al Jandarmeriei, în scopul îmbunătățirii și perfecționării activității în domeniul pazei obiectivelor, și-a stabilit următoarele **obiective prioritare**:

- eficientizarea dispozitivelor de pază în funcție de situația operativă, efectivele și mijloacele avute la dispoziție;
- creșterea capacității operative de intervenție la obiectivele asigurate cu pază de către jandarmi, precum și la transporturile de valori și speciale;
- îmbunătățirea dotării tehnico-materiale, a condițiilor de executare a serviciului, de cazare, hrănire și echipare a personalului care execută misiunea de pază și apărare a obiectivelor;
- creșterea competenței profesionale a tuturor categoriilor de personal pentru îndeplinirea atribuțiilor și sarcinilor ce le revin pe linia pazei și apărării obiectivelor încredințate;

- respectarea și aplicarea unitară a cadrului legislativ și regulamentar în îndeplinirea atribuțiilor specifice;

- adaptarea organizării structurilor de pază la noile cerințe și atribuții, rezultate din reorganizarea Jandarmeriei Române, în vederea creșterii capacității funcționale, optimizării și eficientizării tuturor activităților;

- asigurarea continuității în activitatea de coordonare a marilor unități și unităților de jandarmi, în vederea adoptării celor mai eficiente măsuri pentru executarea, în deplină siguranță, a misiunilor de pază și creșterea capacității operative de intervenție la obiectivele și transporturile date în competență;

- completarea și îmbunătățirea cadrului legislativ, în domeniul pazei obiectivelor, bunurilor, valorilor și transporturilor de valori și speciale, armonizarea prevederilor regulamentare, corespunzătoare noilor norme legale și asigurarea organizării și executării misiunilor și sarcinilor în raport de acestea;

- perfecționarea pregătirii personalului și ridicarea nivelului de competență pentru îndeplinirea atribuțiilor funcționale și desfășurarea tuturor activităților de organizare, coordonare și control a misiunilor de pază;

- cunoașterea permanentă a situației operative din zonele de responsabilitate a marilor unități, unităților, obiectivelor, precum și a tuturor datelor de interes pentru coordonarea întregii activități în domeniul asigurării pazei obiectivelor, a transporturilor de valori și speciale, precum și a misiunii de asigurare a pazei și intervenției la conductele magistrale de transport produse petroliere;

- intensificarea activităților informativ-operative de către structurile specializate ale Jandarmeriei și transmiterea oportună a datelor obținute, în vederea luării măsurilor specifice pentru prevenirea și combaterea faptelor de natură contravențională sau penală;

- realizarea unei permanente colaborări cu parchetele locale pe linia îndeplinirii atribuțiilor specifice, în scopul prevenirii sau adoptării unor soluții operative de rezolvare a situațiilor contravenționale sau infracționale în domeniul pazei;

- creșterea potențialului preventiv și a eficienței misiunilor de pază prin funcționarea unor sisteme viabile de legături operative și de intervenție coroborate cu o mobilitate și flexibilitate crescută a dispozitivelor de pază.

Comandamentul Național al Jandarmeriei, analizând dispozițiile legale, ce stabilesc obligații și responsabilități cu caracter general, pentru toate entitățile care păzesc obiective, dețin și manipulează valori sau mijloace și materiale ce reprezintă un potențial pericol pentru mediu, pentru sănătatea sau viața oamenilor, a propus și înaintat o serie de proiecte de acte normative, astfel:

- inițierea unui proiect de act normativ, privind protejarea conductelor magistrale de transport produse petroliere, care să asigure un regim sancționator, contravențional și penal, mult mai aspru;

- promovarea unui proiect de ordonanță pentru modificarea O.U.G. nr.271/2000 privind regimul activităților de transport, comercializare și recuperare a produselor petroliere în sensul acordării competenței Jandarmeriei de a constata și sancționa faptele prevăzute în acest act normativ;

Comandamentul Național al Jandarmeriei a fost consultat, dar fără a se ține cont de toate propunerile formulate, la redactarea actualei Legi nr.333/2003 privind paza bunurilor, și a elaborat proiectul Hotărârii de Guvern, ce va înlocui H.G. nr.523/1997.

Condițiile economico-sociale generate de procesul prelungit al tranziției pe care îl parcurge țara noastră, precum și evoluția situației operative internaționale, au amplificat o serie din factorii de risc existenți și au favorizat apariția unor factori noi, ce se pot concretiza sau materializa în acțiuni ostile îndreptate împotriva obiectivelor pe care Jandarmeria le asigură cu pază sau chiar împotriva elementelor din dispozitivele permanente sau temporare.

Ca potențiali factori de risc ar putea fi considerați:

- creșterea corupției la cote alarmante și tendința ei de a se transforma în fenomen;
- creșterea la cote alarmante a infraționalității;
- manifestarea fără precedent a modalităților de operare a infractorilor, în stil mafiot, cu tendințe tot mai vădite de acțiune după modelul elementelor crimei organizate;
- constituirea unor rețele, cu participarea elementelor autohtone și străine, având ca obiect de activitate contrabanda cu diverse produse, traficul de stupefiante, comerțul cu carne vie, traficul de materiale radioactive sau periculoase, ș.a.;
- accentuarea tensiunilor sociale ca urmare a scăderii nivelului de trai, creșterii șomajului și absenței unei perspective pozitive;
- accentuarea nemulțumirilor generate de măsurile „antipopulare” ale programului de reformă;
- tendința de migrare a forței de muncă în străinătate prin diverse societăți, cu acordul țărilor de destinație;
- existența unor instalații învechite, lipsa fondurilor și mijloacelor de protecție individuală și colectivă la unele obiective care au ca obiect de activitate producția de materiale periculoase sau în care se lucrează cu materiale periculoase;
- absența mijloacelor tehnice de pază și alarmare și efectivele reduse avute la dispoziție pentru realizarea dispozitivelor eficiente la unele obiective;
- insuficiența fondurilor financiare alocate, necesare cazării, dotării, echipării și hrănirii efectivelor care execută această misiune;

În momentul în care se analizează oportunitatea luării în pază a unui obiectiv, decizia finală trebuie să fie determinată și impusă de identificarea existenței unor riscuri asupra obiectivului respectiv, precum și de caracterul permanent sau temporar al acestora.

În funcție de existența acestor riscuri, caracteristice situației operative, la un moment dat, un obiectiv poate fi caracterizat ca fiind sau nu de importanță deosebită, fapt care va fi determinant în stabilirea instituției căreia i se va încredința paza acestuia, gradul de angajare al acesteia, precum și resursele umane și materiale care vor fi necesare pentru funcționarea pazei la acel obiectiv.

În scopul prevenirii situațiilor generatoare de riscuri și vulnerabilități în domeniul pazei obiectivelor, **s-au luat o serie de măsuri specifice** care constau în:

- identificarea potențialilor factori de risc asupra obiectivelor din competență;

- identificarea obiectivelor care prezintă vulnerabilități în sistemul de pază, reanalizarea măsurilor și asigurarea condițiilor optime;
- îmbunătățirea cooperării și a schimbului de informații cu celelalte structuri din Sistemul de Siguranță, Ordine Publică și Apărare;
- aplicarea cu strictețe a dispozițiilor cuprinse în planurile de apărare ale obiectivelor;
- identificarea și derularea unor activități curente de protecție și descurajare antiteroristă;
- întărirea dispozitivelor de pază și protecție în situațiile de criză și risc major;
- instituirea unor sisteme suplimentare de descurajare, prin patrulare, în zona obiectivelor vizate de elementele infractoare sau teroriste, de către forțe specializate ale Jandarmeriei.

Nivelul și complexitatea măsurilor de pază și protecție a obiectivelor, sunt racordate permanent la potențialul de risc, cuantificat în baza informațiilor de la structurile proprii sau cele specializate și pot fi intensificate gradual, ori extinse, pe categorii de obiective, în funcție de evoluția situației operative.

Misiunea de pază este deosebit de complexă necesitând diverse măsuri de ordin operativ-informativ, care au ca scop asigurarea securității și protecției obiectivelor păzite.

Obiectivele asigurate cu pază cu efective de jandarmi prezintă o serie de particularități, care le diferențiază în funcție de destinație, dimensiuni și amplasare în spațiu, durata și caracterul activităților ce se desfășoară în acestea, locul, rolul și importanța pe care le au în asigurarea securității valorilor democrației, protecției proprietății publice și private, a populației și mediului înconjurător, de nivelul pericolelor și riscurilor ce le amenință, precum și de natura și nivelul efectelor negative și urmărilor acestora în situația când obiectivul a fost afectat parțial sau total;

În funcție de natura și particularitățile obiectivelor păzite, unitățile și subunitățile de pază adoptă forme, procedee și metode de acțiune specifice. Formele de acțiune adoptate în executarea misiunii de pază pot avea caracter preventiv, ofensiv sau defensiv.

Pentru executarea în bune condițiuni a misiunii de pază obiective, în Jandarmeria Română sunt constituite structuri distincte, destinate executării misiunii de pază obiective, încadrate cu personal special pregătit și antrenat, cu o dotare corespunzătoare.

De asemenea, în toate unitățile Jandarmeriei Române, funcționează structuri mobile destinate intervenției în sprijinul forțelor care asigură paza obiectivelor.

Având în vedere amenințările și riscurile din ce în ce mai mari la adresa siguranței obiectivelor Jandarmeria Română și-a adaptat și dinamizat dispozitivele de pază, de la obiectivele din competență și a intensificat schimbul de date și informații de interes operativ cu celelalte forțe participante la executarea misiunii.

Ca o problemă profesională, **constituirea climatului de siguranță** în zona obiectivelor asigurate cu pază de jandarmi, este și va trebui să fie întotdeauna concepută sau realizată în conformitate cu strategiile și planurile de securitate ale instituțiilor vizate.

Prezentăm în continuare necesitatea realizării unui climat adecvat de siguranță, spre exemplu, pentru instituțiile financiar-bancare.

Această necesitate derivă din următoarele **pericole și considerente**:

- sumele importante de bani, precum și alte valori considerabile aflate în posesia sau în păstrarea instituțiilor financiar-bancare, pot fi puse în pericol prin sustrageri sau spargerii, prin atacuri informaționale, prin declanșarea unui incendiu ori prin producerea altor catastrofe naturale;

- clienții, aflați uneori în număr mare în clădirile instituției, precum și angajații instituțiilor pot fi puși în pericol de un atac armat, de declanșarea unui incendiu sau de producerea altor catastrofe naturale;

- angajații instituțiilor pot deveni victimele unor șantaje sau pot fi luați ostatici, în vederea obținerii unor sume de bani sau altor valori ori servicii, prin șantaj;

- atât instituțiile financiar-bancare în sine, cât și personalul de conducere al acestora, pot fi supuși unor atacuri sau pot deveni victimele unor zvonuri defăimătoare;

- credibilitatea instituțiilor și buna desfășurare a serviciilor acestora pot fi amenințate prin acțiuni sau atacuri informaționale ori prin blocarea canalelor, inclusiv a celor electronice, de realizare a serviciilor sau de comunicare;

- penetrarea măsurilor de siguranță și falsificarea înscrisurilor de valoare sau a cărților de credit pot aduce pe lângă pierderi valorice imediate și pierderea încrederii în instituție, producând, prin consecințe, alte pierderi importante de valori;

- pe lângă pierderile de valori, în cazul atacurilor informaționale reușite, apar și pericolele nesensizării căilor de atac, precum și cel al deteriorării sistemului informatic propriu sau asociat instituției ori al distrugerii bazelor de date ale acestora;

- atacurile împotriva instituțiilor financiar-bancare sunt deosebit de profesioniste, pregătite cu migală și au o multitudine de forme de manifestare greu de anticipat; se desfășoară cu repeziciune, sunt deosebit de violente și pot pune în pericol atât vieți omenești, cât și întreaga activitate a instituției atacate;

- de cele mai multe ori, bunurile dobândite în urma atacurilor împotriva instituțiilor sunt greu de recuperat, iar pierderile datorate incendiilor sau dezastrelor sunt adesea irecuperabile.

Fenomenul infracțional din instituțiile financiar-bancare nu se detașează de caracteristicile infracționale ale celorlalte atacuri care determină factori de risc. Complexitatea de pericole și fapte care amenință siguranța obiectivelor face obligatorie analiza cât mai corectă a pericolelor potențiale la care este expusă instituția financiar-bancară, în urma căreia trebuie determinate cu profesionalism, responsabilitate și realism (și marcate pe documentele strict confidențiale) posibilele căi ale atacurilor din exterior sau din interior (proprii angajați) ori în colaborare, posibilitățile de declanșare a unui incendiu, tipurile răufăcătorilor, modurile și procedurile previzibile de atac asupra punctelor de interes special ale instituției, arhitectural-constructive sau din sistemele informatice și rețelele de calculatoare, precum și asupra personalului, încrederii în instituție și în înscrisurile de valoare sau în cărțile de credit elaborate sau utilizate de aceasta.

Pe lângă profesionalism, este necesar ca analiza de risc să fie abordată cu responsabilitate maximă, astfel încât nici un amănunt sau detaliu să nu fie ignorat.

O evaluare profesională și realistă a riscurilor va duce întotdeauna la o soluție optimă din punct de vedere al minimului raportului cost/performanță; prin tratarea diferențiată a amenințărilor și deci, prin „personalizarea soluției în funcție de situația concretă”.

La estimarea pericolului potențial pentru instituțiile financiar-bancare, trebuie să se țină seama de un sistem complex de factori, cum ar fi cei pentru securitatea fizică, pentru securitatea informațiilor, pentru protecția împotriva incendiilor și pentru protecția împotriva catastrofelor naturale.

Statisticile arată că pentru toate instituțiile financiar-bancare există aceleași **riscuri de bază care vizează:**

- valorile proprii băncii păstrate în casa de bani blindată sau în camera de tezaur, precum și în automatele de bani (folosite și de client și de angajați);
- valorile clienților păstrate în seiful blindat sau în spațiile închiriate din camera trezoreriei;
- bancnotele expuse la vedere în timpul tranzacțiilor în sala clienților;
- înscrisurile de valoare și cărțile de credit emise de instituțiile financiar-bancare;
- procedurile informatice de transfer de valori și de recunoaștere a colaboratorilor și clienților, băncile și bazele de date ale instituțiilor financiar-bancare.

Datorită pericolului imens pe care îl constituie un atac reușit pentru o instituție financiar-bancară, evenimentul care ar duce la consecințe catastrofice este cunoscut sub sintagma de „eveniment major” (top event), iar zonele sensibile de păstrare a valorilor sunt denumite „zone (camere sau puncte) vitale”.

Determinarea zonelor vitale este o problemă profesională și se realizează după o analiză atentă în care se investighează: acțiunile ostile posibile, obiectivele acestora, zonele avute în vedere și elementele care pot deveni ținte ale atacului.

Practica „evenimentelor majore” produse în instituțiile financiar-bancare a impus câteva **tipuri de infractori**, dintre care se detașează hoții (jefuitorii), teroriștii, spărgătorii și, mai nou, infractorii informaționali.

Hoțul/jefuitorul: o mare parte a acestui gen de infractori este formată din amatori care au de regulă ca motivație:

- situația materială dificilă (șomeri fără nici o perspectivă);
- stări psihice depresive, ca urmare a consumului de stupefiante și de alcool;
- libertini, neadaptați, grandomani sau cleptomani;
- împătimiți ai jocurilor de noroc.

Atacurile au loc cu sau fără o pregătire prealabilă și ca atare nu au un scenariu tipic, ceea ce conduce la imposibilitatea adoptării unui sistem standard de apărare.

Din studiile efectuate rezultă că peste 80% din făptași se află într-o stare extremă de agitație, atât înainte, cât și după comiterea infracțiunii. Pentru înfrângerea acestei stări, infractorul consumă băuturi alcoolice, stupefiante sau medicamente. În timpul atacului pot apărea situații neprevăzute, care pot determina reacții greu previzibile și necontrolabile, conducând la circumstanțe de extrem pericol. Folosirea armei, de regulă

neplănuită, servește, întâi de toate, la intimidare; în cazuri de nervozitate controlată și, cu predilecție, în cazul în care făptașul consideră că își poate crea o cale liberă pentru evadare, arma este folosită spontan pentru a provoca panică și teamă. Făptașul încearcă în fiecare caz să profite la maximum de momentul surpriză, căutând să obțină cât mai multe avantaje sau lucruri, într-un timp cât mai scurt și cu un risc minim.

Teroristul, are de regulă, și o motivație politică, recurgând la forme de atac „atipic”, caracterizate de următoarele:

- supravegherea prealabilă a băncii și/sau a căilor și mijloacelor de comunicații și de transport ale acestora (zile, săptămâni de-a rândul, pentru aflarea detaliilor necesare: program, locurile de acces ale persoanelor vizate etc.);

- bruierea, blocarea sau întreruperea, pentru anumite perioade, a mijloacelor și căilor de comunicație;

- testarea răspunsului forțelor și mijloacelor de securitate prin diferite procedee, de la crearea unor incidente în localul băncii, la lansarea unor zvonuri privind unele posibilități de penetrare a măsurilor de securitate, până la alarme false referitoare la plasarea unor încărcături explozive sau a existenței unor pericole de incendiu etc.;

- supravegherea angajaților ce sosesc sau pleacă și uneori acostarea acestora, înainte sau după începerea sau terminarea programului;

- atacuri asupra funcționarilor, conducerii băncii, în locuințele acestora, pentru a-i sili, sub amenințare, să revină la bancă și să deschidă camerele de valori.

Acestea sunt realizate aproape exclusiv de mai mulți făptași împreună. Acțiunea este premeditată, există multe variante de scenariu și, deci, nu se poate stabili un anumit comportament tipic. Făptuitorii acestui mod de atac sunt persoane dure, dispuse să ucidă pentru a-și realiza scopul, de cele mai multe ori special antrenate în acest sens.

Spărgătorul este tipul complet de răufăcător, întrunind pe lângă „calitățile” expuse anterior și o pregătire tehnică care îi permite să utilizeze cu eficiență maximă o cantitate mică de unelte manuale, portabile, moderne, de mare eficacitate. În acest scop, el dispune de o pregătire adecvată pentru care este dispus la un considerabil efort financiar și fizic.

Datorită progreselor rapide ce caracterizează tehnica, spărgătorul trebuie să-și mențină dotarea și pregătirea la zi. În privința dotării, la ora actuală există numeroase surse de unde pot fi procurate o multitudine de unelte perfecționate și miniaturizate, calitate importantă pentru transportul lor la locul acțiunii.

De asemenea, are, în general, cunoștințe tehnice despre sistemele de securitate pe care poate încerca să le neutralizeze.

Incendiatorul poate fi dintre angajați și în acest caz poate acționa și din greșeală, sub presiune (morală ori șantaj) sau ca urmare a unei pregătiri necorespunzătoare, în materie de prevenire a incendiilor. Există și riscul ca actul în sine să fie rezultatul unei colaborări premeditate între angajați și incendiatorii din afară. Acțiunile se pot desfășura individual sau în echipe, cu supravegherea prealabilă ori cu penetrarea măsurilor de prevenire (protecție) împotriva incendiilor.

Problema **infractorului informațional**, deci și a infracțiunilor informaționale este foarte complexă și controversată. Legislația actuală, incompletă și neclară, din punct de

vedere al incriminării faptelor de natură penală în domeniul informațional, conferă infractorilor o mai mare „libertate juridică” și, deci, o oarecare posibilitate de sustragere de la rigorile legii. Paleta infracțiunilor în acest domeniu se întinde de la simple indiscreții care pot pune în pericol afacerile sau interesele instituțiilor financiar-bancare, sau de la accesul neautorizat la informații, până la atacurile informaționale ce pot produce pagube valorice sau pot pregăti atacuri armate, furturi sau spargerii. La aceasta se adaugă și faptul că există mai multe tipuri de infractori informaționali, între care prezentăm patru din cei mai reprezentativi, astfel:

- **intrusul**, care este o persoană ce accesează neautorizat fișiere, baze sau bănci de date din instituțiile financiar-bancare, în scop informațional sau din „dorința de a cunoaște”. Poate fi o persoană fizică sau o instituție concurentă, un virus sau un program scăpat de sub control.

Efectele unui acces neautorizat pot fi: aflarea unor informații confidențiale, blocarea unor căi de acces, o alterare, o distrugere sau o deturnare de date (conturi).

Intrusul poate fi un bun informatician sau un novice, putând declanșa o acțiune singulară sau înlănțuită.

Cele mai eficiente metode de protecție împotriva intrusului, atât împotriva celor locali, cât și împotriva celor aflați în diferite puncte ale zonei de distribuție a unei rețele teleinformatice sunt: controlul riguros al accesului în baza de date, evidența strictă a serviciilor, utilizarea de software original, controlul antivirus, identificarea și autentificarea surselor și obiectivelor de procesare și comunicații, precum și autorizarea serviciilor de procesare ori comunicații.

- **hacker-ul**, este un intrus de tip special, profesionist sau amator, ce forțează cu precădere dispozitivele de asigurare a securității și de interzicere sau îngreunare a accesului persoanelor neautorizate, dar și zonele de procesare sau de stocare a informațiilor.

Spargerea codurilor și accesul neautorizat în baza de date se produce din curiozitate sau vendetism, iar urmările pot fi de tip „gentlemen” – când atentatorul lasă în urmă o atenționare, sau de tip „killer” – în cazul în care se produc adevărate dezastre informaționale: distrugerea bazelor de date, a programelor, a sistemelor de operare, a jurnalelor de evidențe și chiar a resurselor de procesare (memorii, imprimante etc.).

Hacker-ul nu are scopul de a-și însuși valori materiale; el poate fi folosit însă de către infractori sau instituții rivale, atât ca persoană, cât și prin exploatarea rezultatelor acțiunilor sale.

Metodele de protecție trebuie să fie orientate cu precădere către legăturile sau căile teleinformatice.

- **Atentatorul la sistemul informațional** este un infractor deosebit de periculos, care datorită manierei sale profesioniste de acțiune, reușește să culeagă date esențiale, fără a lăsa urme sau fără a distruge, logic ori fizic, informațiile și resursele de care s-a folosit.

Atacurile informaționale pot preceda sau însoți atentate grave, teroriste sau spargerii de amploare, dar pot fi și independente, urmărind destabilizarea serviciilor instituției financiar-bancare sau compromiterea acesteia.

Mijloacele de protecție sunt diverse și pot fi eficace numai dacă sunt integrate într-un mecanism profesional de asigurare a securității informaționale.

- **Infractorul informațional propriu-zis** este un infractor aparte, deosebit de periculos, ce își însușește valori materiale prin atacuri informaționale, vizând: deturnarea valorilor din conturi prin transferuri neautorizate, deschiderea de conturi duble sau false, rotunjirea rezultatelor operațiilor aritmetice la zecimalele aflate dincolo de controlul procesorului valoric, dar în limitele celui matematic, falsificarea înscrisurilor de valoare sau a cărților de credit etc.

Infrațiunile informaționale pot fi atât singulare, cât și colective, la care sunt atrași actuali sau foști angajați ai instituțiilor financiar-bancare, elaboratori de sisteme sau programe informatice achiziționate de către instituția financiar-bancară respectivă. Ele se desfășoară după o pregătire amănunțită și pot fi atât de tip fulger, cât și ca urmare a unei supravegheri îndelungate.

De obicei, infrațiunile informaționale sunt însoțite și de acțiuni de blocare sau de distrugere a resurselor sistemelor informatice sau ale rețelelor de calculatoare, fapt ce amplifică mult pagubele și poate duce la pierderea încrederii clienților, datorită întârzierii serviciilor sau apariției unor imperfecțiuni, încurcături, greșeli, erori etc.

Lupta împotriva acestora este deosebit de grea și costisitoare, necesitând o intensitate sporită, continuă și nu poate fi rezolvată decât de mecanisme integrate sau de sisteme profesionale de securitate a informațiilor, adaptabile, avizate și autorizate de către autoritățile publice competente.

Asigurarea securității unei instituții, indiferent de cine este păzită este rezultanta acțiunii mai multor categorii de forțe interne, și în unele cazuri chiar internaționale, care colaborează și se sprijină reciproc în vederea realizării unui scop comun. Aceasta ne îndreptățește să apreciem că paza obiectivelor, generic vorbind, trebuie prognozată, proiectată și executată ca o acțiune integrată, de o deosebită importanță deosebită pentru societatea contemporană.

Această prezentare nu și-a propus să epuizeze întreg domeniul de analiză a problematicii privind paza instituțiilor, ci provoacă la dezbateri și deschide calea spre observații sau sugestii care să ducă la perfecționarea muncii structurilor specializate și cu atribuții pentru îndeplinirea acestei misiuni, în scopul creșterii siguranței obiectivelor păzite.

Întocmit

General de brigadă dr. Costică Silion