POLITICI ŞI STRATEGII DE PROTECŢIE A INFORMAŢIILOR CLASIFICATE ÎN CONDIŢIILE ASPIRAŢIILOR DE INTEGRARE EUROPEANĂ A REPUBLICII MOLDOVA

Vitalie OJOG,
doctorand ULIM, Facultatea de Drept

SUMMARY

World is faced to various security risks and threats with which it has to cope. With this view, states, security intergovernmental and non-governmental organizations use a range of methods, techniques and procedures to eliminate, to mitigate or to counter security risks and threats. Under the present intern and international conditions, defined by complexity and a dynamic and random evolution, Moldova must be constantly preoccupied with ensuring its national security and defence. To this end, the system of classified information protection in Moldova should be developed in a high quality and efficient model. Due to the EU integration process, as a first stage, it is important to define the strategies and policies of the multilevel classified information safeguarding system in order to assure national and regional security.

Keywords: security risks, classified information, national security, information security, classified information safeguarding system, security incident.

REZUMAT

Actualele evoluţii interne şi internaţionale în domeniul securităţii relevă caracterul dinamic, complex şi fluid al riscurilor şi ameninţărilor cu impact direct asupra modului de funcţionare a instituţiilor Statului cu atribuţii în asigurarea securităţii naţionale şi, implicit, în asigurarea securităţii informaţiilor clasificate, ca latură a securităţii naţionale. Procesul de ajustare şi armonizare a normelor juridice naţionale şi ale statelor Uniunii Europene presupune implicit şi cercetări fundamentale în domeniul criteriilor şi sistemului de protecţie a informaţiilor clasificate. La etapa iniţială se impune conceptualizarea modelului adecvat al mecanismului de protecţie a informaţiilor clasificate, sarcinile, condiţiile, etapele şi metodele necesare pentru elaborarea acestui sistem complex.

Cuvinte-cheie: risc de securitate, informaţii clasificate, securitate naţională, securitatea informaţiilor, sistem de protecţie a infromaţiilor clasificate, incident de securitate.

Introducere. Problema securităţii informaţiilor nu mai este de mult numai apanajul structurilor militare, în ultima vreme căpătînd o pondere însumată atît în mediile de afaceri, cît şi în cele politice. Explozia tehnologiei informaţiilor în secolul care a fost denumit "Era Informaţională – Information Age" a spart demult barierele de timp şi spaţiu, permiţînd astfel o mai rapidă accesare a informaţiilor.

În contextul creşterii dependenţei de informaţii, dar şi al necesităţii de a le proteja, ***scopul articolului*** respectiv este identificarea şi aplicarea la nivel organizaţional a celor mai eficiente şi oportune soluţii de management al riscurilor de securitate în domeniul informaţiilor clasificate.

Actualele evoluţii interne şi internaţionale în domeniul securităţii relevă caracterul dinamic, complex şi fluid al riscurilor şi ameninţărilor cu impact direct asupra modului de funcţionare a instituţiilor statului cu atribuţii în asigurarea securităţii naţionale şi, implicit, în asigurarea securităţii informaţiilor clasificate, ca latură a securităţii naţionale. Persistenţa conflictelor clasice, militare, în anumite zone şi a ambiţiilor regionale ale unor state, emergenţa unor noi vectori în Asia sau Orientul Mijlociu se suprapun peste transferarea în plan nonstatal a relaţiilor internaţionale pe coordonatele dezvoltării organizaţiilor transnaţionale, a grupărilor teroriste sau extremiste cu veleităţi globale sau chiar a actorilor individuali. În acest sens, relaţiile dintre state şi actorii nonstatali au devenit o coordonată importanţă a descifrării dinamicii de securitate atît la nivel naţional, cît şi internaţional [1].

Un alt efect al revoluţiei tehnologice este reprezentat de creşterea capacităţilor civile şi comerciale de supraveghere – sateliţi, sisteme de tip GPS –, care duc la nevoia unei mai bune protecţii a informaţiilor din mediul militar şi la utilizarea la capacitate maximă a informaţiilor care provin din mediul civil, comercial. Într-un mediu ostil şi evolutiv, în care ameninţările şi vulnerabilităţile se redefinesc şi se amplifică permanent, protecţia informaţiilor clasificate devine o sarcină deosebit de complexă.

Unii savanţi – Ion Ciobanu, Aurel Nour, Nasty Vladoiu – insistă asupra faptului că, cel mai adesea, pentru protejarea informaţiilor clasificate se recurge la soluţii bazate pe mecanisme de securitate deplină. Indiferent de strategia aleasă, mecanismele de securitate deplină asigură integrarea funcţională, din punct de vedere al securităţii, a procesului ce trebuie protejat, pe baza reglementărilor legale în materie, într-o structură ierarhică eficientă. Conform celor relatate însă de Ilie Gheorghe şi Tiberiu Urdăreanu, "nu a fost, nu există şi nu va putea exista o măsură de securitate perfectă şi general valabilă. Deşi mai puţin, această remarcă este adevărată şi

pentru un mecanism de securitate deplină, deoarece orice sistem are slăbiciunile sale conceptuale, constructive, tehnologice şi, în plus, o dinamică de adaptare şi perfecţionare, de regulă, inferioară dinamicii de evoluţie a realităţii" [2].

Metode şi materiale aplicate. Aplicarea în cadrul articolului respectiv a metodelor logice, comparative, sociologice, prospective şi sistemice de cercetare, corelate cu studierea materialelor specialiştilor în protecţia informaţiilor din străinătate privind conceptele de vulnerabilitate, ameninţare şi risc informaţional şi consecinţele deosebite asupra viabilităţii sistemelor informaţionale şi îndeosebi asupra securităţii naţionale induc o necesitate ascendentă în abordarea standardelor puse la dispoziţie de NATO şi UE în elaborarea actelor normative specifice, precum şi amendarea celor în vigoare, pentru a fi în concordanţă cu cele mai noi cerinţe euroatlantice.

Succesul oricărui mecanism de securitate deplină, care a fost implementat în vederea protecţiei informaţiilor clasificate, depinde în mod indubitabil de eficienţa cu care organizaţiile analizează şi evaluează ameninţările şi vulnerabilităţile şi îşi asumă costurile pentru desfăşurarea managementului riscurilor de securitate, atât la nivel strategic, cât şi la nivel operaţional.

Complexitatea tipurilor de atacuri, a direcţiilor şi a cauzelor de insecuritate determină complexitatea şi ierarhizarea tipurilor de protecţie şi presupune integrarea acestora într-o strategie fundamentată pe evaluarea riscurilor insecurităţii şi a cheltuielilor totale privind măsurile de securitate.

Strategia de protecţie a informaţiilor clasificate ca element al securităţii naţionale. Politicile şi strategia de protecţie a informaţiilor, inclusiv coerentă şi pentru Republica Moldova, trebuie să aibă ca obiectiv realizarea unei securităţi de un anumit nivel, ierarhizate şi diferenţiate pentru anumite componente, servicii, informaţii sau utilizatori.

În acest context, se consideră că o societate informaţională trebuie să atingă un stadiu în care să dispună de un cadru legislativ şi metodologic adecvat, de structuri funcţionale şi de o dotare corespunzătoare. Cadrul respectiv urmează să asigure desfăşurarea nealterată şi în condiţii de siguranţă a proceselor decizionale, să protejeze conţinutul informaţiilor, să asigure funcţionarea în siguranţă a sistemelor informaţionale şi a elementelor de infrastructură de importanţă critică. Pe aceeaşi dimensiune se încadrează şi capacitatea sistemului să descurajeze, pe căi şi prin mijloace de natură informaţională, acţiunile de orice fel la adresa securităţii naţionale, inclusiv infracţiunile ce atentează la securitatea statului. Depistarea oportună şi precizarea originii, scopului, căilor şi mijloacelor de ducere a acţiunilor informaţionale, contracararea acestor acţiuni şi estimarea evoluţiei viitoare a unor acţiuni de acest tip, a costurilor şi implicaţiilor de contracarare a acestora constituie paliere adiţionale strict necesare a fi înglobate de sistemul juridic şi metodologic invocat. Nu în utlimul rînd, este importantă şi desfăşurarea de acţiuni informaţionale prin care să se contribuie la promovarea şi protejarea intereselor securităţii naţionale [3].

Un asemenea stadiu complex, care să asigure o securizare maximă a informaţiilor clasificate, poate fi atins prin îndeplinirea următoarelor obiective prioritare:

- elaborarea şi adoptarea politicii şi strategiei protecţiei informaţiilor, care să stabilească un şir de principii, obiective, cerinţe şi cadrul legal, structural, procesual şi metodologic;
- conştientizarea, la nivelul factorilor de decizie politico-militară, a necesităţii abordării şi dezvoltării instituţionalizate a domeniului protecţiei informaţiilor, plecînd de la analiza ameninţărilor, vulnerabilităţilor, riscurilor şi a oportunităţilor pe care le presupune dezvoltarea acestui domeniu vital pentru securitatea naţională;
- crearea cadrului legislativ la nivel naţional, dar şi la cel departamental, care să permită dezvoltarea instituţionalizată şi funcţionarea corespunzătoare a structurilor specifice;
- dezvoltarea unui cadru metodologic, format din metodologii, proceduri, algoritmi, cerinţe, standarde şi tehnici, care să permită funcţionarea tuturor structurilor şi capacităţilor, într-o viziune unitară din punct de vedere conceptual şi tehnic;
- pregătirea adecvată a resursei umane, într-o concepţie multidisciplinară, printr-o colaborare permanentă cu specialiştii din comunitatea de informaţii, cu cei din domeniile cercetării şi universitare, din ţară şi din străinătate [4];
- dezvoltarea infrastructurii de protecţie a informaţiilor, în acord cu cerinţele de securitate naţională şi de siguranţă informaţională, paralel cu evaluarea sistematică a vulnerabilităţilor, ameninţărilor şi riscurilor din domeniu, care să asigure implementarea metodologiilor, standardelor şi procedurilor necesare protecţiei informaţiilor în procesul de prelucrare, utilizare sau stocare a datelor.

Aşadar, este necesară punerea bazelor conceptuale şi metodologice, precum şi crearea unui cadru normativ, juridic şi instituţional care să permită dezvoltarea coerentă, globală şi unitară a domeniului protecţiei informaţiilor care, în acest context, pot fi considerate prioritare pentru Republica Moldova.

Realizarea cadrului normativ adecvat al domeniului protecţiei informaţiilor presupune asigurarea concordanţei acestuia cu aspectele normative complexe şi cu raporturile şi implicaţiile sociale ale informaţiei. Astfel, potrivit cercetătorului V. Fulga, legislaţia care nu ţine întotdeauna pasul cu tehnologia informaţiei şi cu implicaţiile sociale ale acesteia determină partea juridică să aprecieze

că alterarea, modificarea, distrugerea sau furtul de date şi informaţii din sistemele informaţionale nu sînt delicte împotriva bunurilor, ci provocate de neviabilitatea sistemelor informaţionale [5].

Ţinînd cont de faptul că protecţia informaţiilor este o problemă care presupune restricţionarea şi supervizarea unor manifestări comportamentale, se impune realizarea unui cadru normativ bine definit şi adecvat realităţii, în care protecţia să-şi poată manifesta elementele de voinţă şi de constrîngere.

În acest sens, protecţia informaţiilor trebuie înţeleasă ca o prioritate în ceea ce priveşte securitatea naţională şi trebuie să cuprindă:

1. prevederi în legile organice şi speciale referitoare la problematica de protecţie, confidenţialitate, dreptul de proprietate şi de autor, liberul acces la informaţii, dreptul de procesare şi de transmitere a informaţiilor;

2. procedurile legale specifice care reglementează strict aspecte de protecţie a informaţiilor sau privind autorităţile publice abilitate în domeniu;

3. norme de protecţie generală şi specifică, ce abordează securitatea proceselor sau diferite aspecte (protecţia fizică a persoanelor, a datelor şi a informaţiilor, condiţiile de mediu etc.), normele privind combaterea fenomenelor sau a faptelor periculoase, măsuri specifice etc.;

4. coduri deontologice rezultate în temeiul prevederilor, care sînt mai restrictive, dar unanim acceptate, în virtutea unor drepturi private şi inalienabile de protecţie a activităţii, a patrimoniului, a informaţiilor şi a personalului;

5. angajamente de securitate, care presupun stabilirea noului cadru de cunoaştere şi de responsabilitate reciprocă între persoane şi autorităţi.

Aplicarea legislaţiei privind protecţia informaţiilor trebuie să se transfere de la responsabilitatea formală a conducerii către responsabilităţile reale ale personalului, în funcţie de competenţa şi participarea efectivă a fiecăruia la activităţile structurii [6].

Riscurile şi ameninţările de securitate în domeniul protecţiei informaţiilor clasificate. Crearea structurilor şi realizarea mecanismelor destinate protecţiei informaţiilor au fost mult timp privite ca „un rău necesar”, însă s-a impus cu adevărat în Republica Moldova abia după anul 1990. Caracteristica activităţii de proiectare şi realizare a structurilor şi a mecanismelor de securitate privind protecţia informaţiilor, în condiţiile evoluţiei spectaculoase din domeniile comunicaţiilor şi IT, presupune ca structurile de securitate să corespundă şi să răspundă la noile ameninţări şi riscuri de securitate:

− evoluţia paralelă şi în concurenţă permanentă a tehnicilor puse în slujba crimei organizate şi a celor adecvate noilor tehnologii de securitate;

− pericolul dezinformării, atacului la imagine, sufocării informaţionale, precum şi al abuzului în procesarea informaţiilor;

− mutaţiile fundamentale în tehnologia informaţiilor şi a comunicaţiilor;

− limitarea acţiunii securităţii, din cauza insuficienţei resurselor financiare şi umane, în detrimentul protecţiei anticipative, a asumării conştiente şi inteligente a riscurilor în dinamica lor.

Conform unor studii conceptuale şi metodologice realizate inclusiv şi de autorii Roceanu I., Buga I., instituţionalizarea structurilor de protecţie a informaţiilor, ca mărime şi competenţe, depinde de un şir de factori flexibili ca valoare şi caracter [7]. Printre aceştia sînt trasate specificul şi interesele structurii care trebuie protejată, nivelul de informatizare, vulnerabilităţile, ameninţările şi posibilele riscuri de securitate, bugetul alocat, consecinţele unor evenimente nedorite, strategia, structura mecanismului de securitate şi performanţele mediului de securitate realizat.

De asemenea, în proiectarea acestor structuri este necesar să se ţină seama de cîteva aspecte, care sînt deosebit de pronunţate în condiţiile actuale ale Republicii Moldova. În acest sens rolul şi locul structurilor de protecţie a informaţiilor sînt condiţionate de interese, de confuzii între concept şi dimensionalităţi, de lipsa unei legislaţii corespunzătoare în materie. Totodată, structura de securitate este condiţionată, de cele mai multe ori, nu de aspectele funcţionale, ci de resursele financiare alocate. La acelaşi capitol se înscrie şi influenţarea locului, rolului şi competenţelor structurii de securitate de calităţile speciale, proiectele şi acţiunile acestora.

Deşi se recunoaşte că securitatea este un element de calitate şi stabilitate al oricărei activităţi, proces, sistem, totuşi acceptarea unei structuri de securitate este o problemă de decizie mai mult sau mai puţin condiţionată de limitele resurselor sau de dificultatea de a suporta unele costuri mari de securitate şi care nu se pot recupera în timp scurt [8].

Considerăm că niciun mecanism de securitate nu poate fi perfect sau absolut, deoarece, oricît s-ar investi, un mecanism are slăbiciunile sale conceptuale, constructive şi tehnologice, precum şi o dinamică de adaptare şi perfecţionare inferioară ritmului de evoluţie a realităţii.

Mecanismul de securitate se proiectează pentru a realiza o funcţionalitate rapidă şi descurajantă, reflexivă (măsuri şi contramăsuri), multidimensională (organizatorică, fizică şi informaţională), în scopul îndeplinirii unui şir de funcţii prioritare. Pe această dimensiune, un mecanism de securitate, inclusiv şi cel de protecţie a informaţiilor, trebuie să îndeplinească funcţiile:

1. Prevenirea şi descurajarea acţiunilor (atacurilor);

2. Detecţia anticipată a acţiunii răuvoitoare;

3. Întîrzierea;

4. Stoparea;

5. Reducerea efectelor acţiunilor reuşite;

6. Evidenţierea şi analiza evenimentelor de securitate.

Prevenirea producerii evenimentelor care generează insecuritate, precum şi măsurile de descurajare au importanţă deosebită, am putea spune decisivă, în procesul de protecţie a informaţiilor. Aspectul invocat se bazează pe considerentul că este mult mai costisitor să tratezi un eveniment decît să-l previi. Totodată, în domeniul protecţiei informaţiilor numărul evenimentelor similare este suficient de mare, încît să poată fi folosit pentru prevenire, iar majoritatea evenimentelor de insecuritate conţin elemente comune, deşi acestea se produc separat şi izolat. Adiţional eficacitatea prevenirii producerii evenimentelor care generează insecuritate este generată şi de faptul că existenţa acestora, care, deşi se produc separat şi se manifestă în mod diferit, pot duce la situaţii identice de hazard şi la exploatarea similitudinilor evenimentelor de insecuritate produse în alte medii social-economice.

Existenţa studiilor de potenţialitate criminală şi acţiunea structurilor competente de prevenire permanentă a actelor criminale, precum şi analiza situaţiilor de pregătire a actelor criminale şi exploatare a acţiunilor premergătoare atacurilor (supravegherea, concentrarea, procurarea de mijloace adecvate, culegerea de informaţii, situaţii de labilitate şi instabilitate, tipuri de atacuri repetate etc.) determină în fond oportunitatea şi eficacitatea aplicării principiului prevenirii în domeniul protecţiei informaţiilor clasificate.

Dacă prevenirea accidentelor şi a dezastrelor are deja o cultură formată şi se poate baza pe mijloace organizatorice şi tehnologice eficiente, prevenirea criminalităţii în mediul informaţional este încă departe de a avea, la rândul său, o astfel de cultură. De aceea, o componentă fundamentală a conceptului securităţii mediului informaţional o constituie prevenirea producerii evenimentelor şi acţiunilor nedorite [9].

În acest context prevenirea producerii evenimentelor care generează insecuritate, precum şi măsurile de descurajare au importanţă deosebită în combaterea infracţiunilor ce atentează la securitatea Statului cu componente informaţionale vădite – art. 337 CP RM „Trădare de Patrie", art. 338 CP RM „Spionaj", art. 344 CP RM „Divulgarea secretului de stat" şi art. 345 CP RM „Pierderea documentelor ce conţin secret de stat" [10].

Reieşind din faptul că este mai uşor să previi apariţia evenimentelor de insecuritate, decît să le tratezi sau să le atenuezi consecinţele, prevenirea poate fi considerată o acţiune de apărare bazată pe: cunoaşterea mediului informaţional, diagnoza şi prognoza fenomenului de securitate, organizarea unor acţiuni de prevenire în funcţie de particularităţile şi tipologia evenimentelor nedorite, anihilarea sau slăbirea factorilor de insecuritate, identificarea ameninţărilor şi vulnerabilităţilor, determinarea riscurilor din mediul informaţional, educarea personalului din mediu, evidenţierea factorilor de descurajare, participarea la iniţiativele de securitate colectivă şi la acţiunile de prevenţie şi descurajare întreprinse de autorităţile competente, precum şi proiectarea şi realizarea unor structuri şi mecanisme de securitate corespunzătoare [11].

Structura mecanismului de protecţie trebuie să fie de multinivel, ierarhică funcţional şi acţional, cu elemente structurate pe submecanisme de securitate. Ea este foarte complexă, iar metodologia de realizare a acesteia comportă, de regulă, patru etape:

I. Analiza şi evaluarea mediului de securitate, a riscului şi, apoi, definirea variantelor strategiilor de securitate (definirea mediului de securitate şi a valorilor de protejat; analiza şi evaluarea ameninţărilor, vulnerabilităţilor şi riscului de securitate; elaborarea variantelor, strategiilor de securitate; determinarea costurilor de securitate; acceptarea valorilor riscului rezidual acceptat de securitate).

II. Proiectarea, realizarea şi acreditarea mecanismelor de securitate (alegerea variantei strategiei de securitate; elaborarea programului de securitate, cu termene, responsabilităţi şi etape de implementare; executarea de teste şi inspecţii de securitate; omologarea şi acreditarea mecanismelor de securitate).

III. Autorizarea şi asigurarea mecanismului de securitate acreditat, ce reprezintă, practic, recunoaşterea legală a acestuia şi abilitarea funcţionării lui.

IV. Operaţionalitatea şi perfecţionarea, care presupune acţiuni declanşate pentru evaluarea permanentă a riscurilor, armonizarea proceselor de securitate, realizarea de schimbări, uneori structurale, semnificative, ce pot duce la adoptarea unei alte politici de securitate sau chiar proiectarea unui nou mecanism de securitate.

Concluzii. Analizînd principiile de proiectare, realizare şi funcţionare a unui mecanism de securitate, se poate aprecia că mecanismul de securitate trebuie să fie rezultatul unui proces complex, al unei concepţii realiste şi pragmatice, bazate pe analiza riscurilor, pe adoptarea de măsuri şi responsabilităţi complexe şi adecvate, pe valorificarea opţională a costurilor ce pot fi suportate. Importanţă maximă comportă şi aspectul adoptării strategiei de securitate, care trebuie să fie o consecinţă a realizării structurii de securitate şi o condiţie prealabilă de realizare a sistemului de securitate. Totodată, conceptualizarea mecanismului de securitate în calitate de un sistem deschis, adaptabil şi perfectibil asigură crearea structurilor eficace şi realizarea mecanismelor destinate protecţiei informaţiilor.

De asemenea, mecanismul de securitate destinat protecţiei informaţiilor trebuie să fie multifunc-

ţional, acoperind domeniile fizic, tehnologic, informaţional şi de personal, asigurînd toată gama de servicii de securitate: protejarea, descurajarea, detecţia, întîrzierea, stoparea, limitarea sau anihilarea consecinţelor producerii de evenimente nedorite de securitate, reluarea activităţii, după producerea acestora, şi analiza post-factum, pentru perfecţionarea reacţiilor de securitate.

Recenzent:
Alexandru MARIŢ,
conferenţiar universitar,
doctor în drept

Bibliografie

1. Colonel Michael E. Whitman, Herbert J. Mattord. *Principles of Information Security*. Third Edition, Canada: Thomson Course Technology, 2009, 265 p.

2. Ilie G., Urdăreanu T. *Securitatea deplină*. Bucureşti: Editura UTI, 2001, 266 p.

3. Ciobanu I. *Managementul securităţii informaţiilor in acţiunile militare întrunite*. Bucureşti: Editura AISM, 2002, 122 p.

4. Ilie G., Ciobanu I., Nour A. *Confruntarea informaţională şi protecţia informaţiilor.* Bucureşti: Editura Detectiv, 2006, 317 p.

5. Fulga V. *Tendinţe de dezvoltare a sistemelor informaţionale din perspectiva integrării în Uniunea Europeană.* În: Sesiunea de comunicări ştiinţifice, Bucureşti: Editura Universităţii Naţionale de Apărare „Carol I" [Catedra Sisteme Informaţionale Militare si Informaţii pentru Apărare], 2007, p. 354-365.

6. Ilie G., Stoian I., Ciobanu V. *Securitatea informaţiilor.* Bucureşti: Editura Militară, 1996, 28 p.

7. Roceanu I., Buga I. *Siguranţă şi securitate informaţională*. În: Gîndirea militară românească, nr. 3/2003, Bucureşti: Editura Statul Major General, 2003, 84 p.

8. Vladoiu N. *Informaţia clasificată – excepţie de la dreptul la informaţie.* În: Revista „Spaţiul sud-est european in contextul globalizării". Sesiunea de comunicări ştiinţifice cu participare internaţionala „Strategii XXI", 12-13 aprilie 2007. Bucureşti: Editura Universităţii Naţionale de Apărare „Carol I", 2007, 306 p.

9. Zisu C., Mihalcea A. *Securitatea sistemelor informaţional-decizionale: complexitate, structuralitate, operaţionalitate.* Bucureşti: Editura „Tritonic", 2007, 294 p.

10. Codul Penal al Republicii Moldova, nr. 985 din 18.04.2002. În: Monitorul Oficial al RM, nr. 128-129 din 13.09.2002.

11.Boaru Gh., Paun V. *Războiul informaţional. Atacul şi apărarea intr-o lume digitala* [Monografie], Bucureşti: Editura U.N.Ap., 2003, 86 p.

PREZENTAREA SPRE RECUNOAŞTERE. ESENŢA PSIHOLOGICĂ

Iurie BULAI,
master în drept, doctorand

SUMMARY

In this paper are treated the aspects of the essence and presentation for recognition tasks. The author analyzes the opinions of different scientists concerning the presentation for recognition and submits his own views on the essence, significance and tasks of this criminal investigation.

Keywords: presentation for recognition, identification, criminal investigation, criminal.

REZUMAT

În prezentul articol se abordează aspecte ce ţin de esenţa psihologică a prezentării spre recunoaştere. Autorul analizează opiniile unor savanţi cu privire la aspectele şi procesele psihologice ale prezentării spre recunoaştere şi înaintează propriile viziuni privind esenţa, importanţa şi sarcinile acestei acţiuni de urmărire penală.

Cuvinte-cheie: prezenterea spre recunoaştere, identificare, acţiune de urmărire penală, proces penal.

Introducere. Una dintre acţiunile de urmărire penală frecvent întîlnite este prezentarea spre recunoaştere. Frecvenţa şi faptul că este o acţiune reglementată strict de legislaţia procesual penală ar fi trebuit să determine succesul acestei măsuri. Cu regret, practica judiciară denotă faptul că în procesul de desfăşurare a acestei acţiuni se întîlnesc frecvent erori.

Actualitatea temei rezidă în necesita abordării uneia dintre acţiunile de urmărire penală frecvent întîlnite, precum şi a modului de abordare a acesteia atît în cadrul doctrinei criminalistice, cît şi în psihologie.

Scopul acestui articol este de a scoate în evidenţă esenţa psihologică a proceselor de percepere, memorizare, reproducere, a caracteristicilor şi a dificultăţilor de ordin psihologic ce se desfăşoară în sistemul nervos central şi care stau la baza recunoaşterii – acţiune care reprezintă esenţa prezentării spre recunoaştere.

Metode şi mijloace aplicate. În cadrul cercetării s-au utilizat un şir de metode: general ştiinţifică, logică, dialectică. A fost folosită metoda analitică, caracterizată prin cercetarea docrinei criminalistice şi a celei din domeniul psihologiei, îndreptate spre elucidarea mecanismelor psihice de percepere, memorare şi reproducere specifice instituţiei prerezentării spre recunoaştere.

Aspectele psihologice ce ţin de recunoaştere ca element psihologic au fost tratate de mai mulţi savanţi, printre care A. Goldstein, L. Harmon, A. Lesc, V.N. Panferov, A.M. Zinin, N.N. Gapanovici, B. G. Ananiev, C. Aioaniţoaie, I. Sandu, M.S. Şehter, M.I. Enicheev, S. Rusnac, I. Kertas etc.

Tratarea şi analiza aspectelor psihologice ale mecanismelor şi legităţilor ce stau la baza declanşării şi derulării diferitor procese psihice reprezintă elementele-cheie, cunoaşterea cărora garantează obţinerea unor rezultate complete şi obiective în cazul implicării factorului uman. În cazul prezentării spre recunoaşterea, esenţa şi particularităţile proceselor de percepere, memorizare, reproducere, tipurile de memorie existente, aspectele ce ţin de recunoaşerea succesivă şi simultană reprezintă