**Universitatea de Stat din Moldova**

**FACULTATEA RELAŢII INTERNAŢIONALE, ŞTIINŢE POLITICE ŞI ADMINISTRATIVE**

**REFERAT**

**Tema: Esența și conceptualizarea securității informaționale**

 **A elaborat:** *Vitalina Gupal gr. SSN01*

 **A verificat:** *Tatiana Busuncian dr., conf. univ.*

**ChiȘinĂu 2023**

***Cuprins:***

Introducere

1. Noțiuni generale privind securitatea informațională. Cadrul conceptual și terminologic.

2. Securitatea informațională în contextul globalizării.

3. Riscuri și amenințări la adresa securității informaționale.

Concluzie

Bibliografie

**Introducere:**

Încă din timpuri străvechi, informaţia a fost asociată cu puterea și, în ultimă instanţă, cu războiul. Relaţia dintre putere și informaţie a atras, de-a lungul timpului, atenţia mai multor gânditori, ca Sun Tzu, care a constatat: *„Cunoaște-ţi inamicul, cunoaște-te pe tine însuţi; victoria ta nu va fi niciodată în pericol”*, iar mai aproape de timpurile noastre, Carl von Clausewitz privea rolul cunoașterii în război ca *“un factor mai vital decât oricare altul”*.

Informaţia, privită în ansamblu, înseamnă cunoaștere, iar cunoașterea conduce inevitabil la progresul tehnologic, și, dintr-o altă perspectivă, la descătușarea persoanei umane și la afirmarea ei plenară, realizarea propriei libertăţi. Societatea modernă se află în mijlocul unor profunde transformări politice, economice, sociale și culturale. Toate aceste transformări au efecte globale asupra întregii societăţi, dar și, în manieră punctuală, produc un impact la nivel individual. Lumea devine din ce în ce mai complexă. Este o complexitate utilă, dar aceasta implică probleme de securitate, ale căror conexiuni de abia au început să fie descifrate și interpretate.

Securitatea informațiilor este practica de protejare a informațiilor prin atenuarea riscurilor informaționale. Aceasta implică protecția sistemelor informatice și a informațiilor prelucrate, stocate și transmise de aceste sisteme împotriva accesului, utilizării, dezvăluirii, întreruperii, modificării sau distrugerii neautorizate. Aceasta include protecția informațiilor personale, a informațiilor financiare și a informațiilor sensibile sau confidențiale stocate atât în formă digitală, cât și fizică. Securitatea eficientă a informațiilor necesită o abordare cuprinzătoare și multidisciplinară, care implică oameni, procese și tehnologie.

Securitatea informaţiei este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei. Dinamica tehnologiei informaţiei induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităţilor de inscripţionat CD-uri sau a memoriilor portabile de capacitate mare, induce riscuri de copiere neautorizată sau furt de date.

Lucrul în reţea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar frauda.

Dezvoltarea tehnologică a fost acompaniată şi de soluţii de securitate, producătorii de echipamente şi aplicaţii incluzând metode tehnice de protecţie din ce în ce mai performante. Totuşi, în timp ce în domeniul tehnologiilor informaţionale schimbarea este exponenţială, componenta umană rămâne neschimbată. Asigurarea securităţii informaţiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană.

Majoritatea incidentelor de securitate sunt generate de o gestiune şi organizare necorespunzătoare, şi mai puţin din cauza unei deficienţe a mecanismelor de securitate.

Este important ca organizaţiile să conştientizeze riscurile asociate cu utilizarea tehnologiei şi gestionarea informaţiilor şi să abordeze pozitiv acest subiect printr-oconştientizare în rândul angajaţilor a importanţei securităţii informaţiilor, înţelegerea tipologiei ameninţărilor, riscurilor şi vulnerabilităţilor specifice mediilor informatizate şi aplicarea practicilor de control.

Securitatea informațiilor protejează informațiile sensibile împotriva activităților neautorizate, inclusiv inspectarea, modificarea, înregistrarea și orice întrerupere sau distrugere. Scopul este de a asigura siguranța și confidențialitatea datelor critice, cum ar fi detaliile contului clientului, datele financiare sau proprietatea intelectuală.

Consecințele incidentelor de securitate includ furtul de informații private, manipularea datelor și ștergerea datelor. Atacurile pot perturba procesele de lucru și pot deteriora reputația unei companii și pot avea, de asemenea, un cost tangibil.

Organizațiile trebuie să aloce fonduri pentru securitate și să se asigure că sunt pregătite să detecteze, să răspundă și să prevină proactiv atacuri precum [*phishing*](https://www.imperva.com/learn/application-security/phishing-attack-scam/)*,*[*malware*](https://www.imperva.com/learn/application-security/malware-detection-and-removal/)*,* viruși, persoane rău intenționate din interior și [*ransomware*](https://www.imperva.com/learn/application-security/ransomware/)*.*

**1. Noțiuni generale privind securitatea informațională. Cadrul conceptual și terminologic.**

Adesea, termenul *securitate informațională* este folosit (slab spus incorect) ca sinonim pentru termenul securitatea informației, în realitate acestea fiind două concepte interdependente, dar diferite ca arie de acoperire, amploare, obiective, sarcini, instrumente utilizate.

În lume, conceptul de securitate a informației este definit aproape în mod egal/identic de către majoritatea organizațiilor internaționale de standardizate. ***Institutul Național de Standardizare și Tehnologie (NIST)*** din SUA prin seria de standarde NIST SP-800 se referă la necesitățile de securitate și confidențialitate a Departamentului de Stat al USA asupra informației și a sistemelor de procesare a informațiilor, în mare parte accentul fiind pus pe securitatea informației în sistemele cibernetice. Comitetul pentru securitatea datelor din industria cardurilor de plată prin standardul PCI DSS (Payment Card Industry Data Security Standard) stabilește cerințe de securitate aplicabile pentru toate componentele de sistem incluse sau conectate la mediul de date al deținătorilor de carduri bancare. *Organizația Internațională pentru Standardizare și Comisia Internațională pentru Electrotehnică (ISO/IEC)* în familia de standarde ISO/IEC 27k pune accentul pe informație ca un bun fundamental al organizației, care trebuie protejat corespunzător, iar tehnologia informației și a comunicațiilor electronice este, de obicei, un element esențial în crearea, procesarea, stocarea, transmiterea, protecția și distrugerea informației. Totodată, vocabularul mondial de electrotehnică ***Electropedia*** definește termenul de securitate a informației ca protecția informațiilor împotriva divulgării, transferului, modificării sau distrugerii neautorizate, indiferent de natura accidentală sau intenționată. Uniunea Internațională a Telecomunicațiilor (ITU) în privința securității informației face referință la seria de standarde NIST SP-800 și la familia de standarde ISO/IEC 27k. Cei de la ITU au creat, în baza ISO/IEC 27002, recomandările ITU-T X.1051, care servesc ca linii directoare pentru managementul securității informației în sistemele și serviciile de telecomunicații. În esență, securitatea informației presupune asigurarea protecției caracteristicilor fundamentale ale informațiilor: în literatura de specialitate referită ca triada *CIA (Confidentiality, Integrity and Availability).* Însă, în afară de protecția CIA, NIST, ISO, și alte organe de reglementare impun asigurarea și altor atribute adiționale bazate pe CIA, precum dreptul de posesie a informației, autenticitatea informației (asigurarea că un mesaj, o tranzacție sau un alt schimb de informații provin din sursa pe care se pretinde că este), non-repudierea (incapacitatea de negare a faptului emiterii informației și verificarea cu ușurință a emitentului), fiabilitatea (gradul de încredere). Totodată, acestea subliniază diversitatea formelor de manifestare a informației, diversitatea dispozitivelor și tehnologiilor informaționale și comunicaționale în procesele de stocare-prelucrare-transmitere etc.

**Securitatea informațională,** comparativ cu securitatea informației, reflectă o realitate sistemică mai complexă, înglobând în sine atât securitatea informației, securitatea sistemelor informaționale (IS), securitatea informatică (a calculatoarelor, a rețelelor și dispozitivelor de rețea, a tehnologiei informației (IT), adesea referită ca securitate cibernetică/securitatea informației în spațiul cibernetic, virtual, sau securitatea în Internet), protecția datelor cu caracter personal, cât și protecția drepturilor de autor, protecția drepturilor și libertăților omului în spațiul informațional, protecția spațiului informațional și a infrastructurii critice, protecția personalului care lucrează cu sistemele informaționale, protecția informației oficiale ale statului, inclusiv a informațiilor atribuite la secret de stat și a celor cu accesibilitate limitată, protecția spațiului informațional de impactul dezinformării etc[[1]](#footnote-1).

Conceptul de securitate informațională este aplicabil la nivelul persoanei, statului și al societății în întregime, curent definită ca Societate Informațională bazată pe Cunoaștere. „Securitate informațională – stare de protecție a resurselor informaționale, precum și a persoanei, a societății și a statului în spațiul informațional.

Spațiu informațional – mediu de activitate asociat cu formarea, crearea, transformarea, transmiterea, difuzarea, utilizarea și stocarea informațiilor, care produce efecte la nivel de conștiință individuală și/sau socială, de infrastructură informațională și de informație”. „Prin sintagma „securitate informațională” se are în vedere protecția persoanei, societății și a statului, a drepturilor și intereselor acestora în mediul informațional” de amenințările asupra caracteristicilor fundamentale ale informației.

Securitatea informațională implică tipul activului protejat ca parte componentă a unui sistem informațional și al activităților care contracarează provocarea daunelor obiectului dat. În calitate de obiect fiind considerat orice bun, sistem, informație, resursă umană, proces ce are valoare pentru persoană, organizație, societate și stat. În acest caz, conceptul de securitate informațională se referă la protecția de amenințările informaționale, când însuși obiectul protecției poate fi parte componentă sau proprietate a persoanei, a organizației, a unui sistem, a unei infrastructuri, a societății sau a statului în întregime. De exemplu: protecția datelor personale ale utilizatorului vis-à-vis de protecția informațională a persoanei (de spam, reclamă nesolicitată etc.); protecția informației oficiale a statului vis-à-vis de protecția spațiului informațional al statului etc.

În general, conceptul de securitate informațională este preluat ca model de asigurare a securității resurselor informaționale la nivel de stat. Exemple în acest sens pot servi: Concepția securității informaționale a Republicii Moldova, în care asigurarea securității informaționale este definită ca stare de protecție a resurselor informaționale, precum și a persoanei, societății și statului, în spațiul informațional, iar spațiul informațional, la rândul său, este divizat în digital, cibernetic și mediatic; Doctrina securității informaționale a Federației Ruse, prin care se garantează protecția împotriva amenințărilor informaționale interne și externe în scopul asigurării drepturilor constituționale și libertăților oamenilor și ale cetățenilor.

Sintetizând, conceptul de securitate informațională se referă la orice informații, IT sau non-IT (cărți, rapoarte, documente etc.), pe orice suporturi tradiționale (hârtie, pânză etc.) sau media electronice (bandă magnetică, CD etc.), sub orice formă (text, grafică, audio, video), comunicate în mod tradițional (scris, oral, poșta obișnuită) sau electronic (e-mail, chat, telefonie mobilă)[[2]](#footnote-2).

La nivel de stat, în țara noastră există cadrul normativ general de acces la informațiile oficiale stabilit prin Legea privind accesul la informație, unde este definit termenul informații oficiale, care sunt considerate toate informațiile aflate în posesia și la dispoziția furnizorilor de informații, iar politica statului în domeniul accesării informațiilor oficiale presupune că oricine are dreptul de a le prelucra în condițiile prevăzute de această lege. Totodată, este definită o categorie de informații oficiale care posedă accesibilitate limitată, din care fac parte așa informații ca informațiile cu caracter personal, informațiile atribuite la secretul de stat ș.a.

Or, domeniul securității informației se referă la orice acțiune, care implică asigurarea securității informațiilor sau a sistemelor informatice sau non-informatice care prelucrează informații, inclusiv componenta umană, componenta de infrastructură, componenta de suport pentru procesare-transportare-comunicare, inclusiv în rețele, Internet, la distanță, online etc. Evident, fiecare dintre aceste componente exercită impact asupra securității informației și constituie domeniu aparte, fiecare cu metodele și soluțiile sale. De exemplu, asigurarea triadei CIA, autenticității și non-repudierii unui document pe suport de hârtie oarecum diferă de un document electronic, aplicarea semnăturii olografe diferă tehnologic de aplicarea semnăturii electronice, modul de păstrare la fel este diferit etc.

În concluzie, ***securitatea informațională***, în mod general, poate fi definită ca stare a spațiului informațional, care asigură nevoile informaționale ale subiecților în relațiile informaționale, securitatea informațiilor și protecția subiecților relațiilor informaționale de influențe negative. Iar spațiul informațional poate fi definit drept mediu de activitate a subiecților preocupați de crearea, transformarea și consumul de informații. Astfel, conceptul „*securitate informațională*” este unul acoperitor, care include nu doar securitatea informațiilor, ci și protecția mediului obiectului (statului, organizației, persoanei) de impactul informațiilor negative sau de destabilizarea unor componente ale sistemului/obiectului respectiv. Rezumând, securitatea informațională poate fi definită ca protejarea persoanei, organizației, societății și statului în spațiul informațional, a drepturilor și intereselor acestora față de (1) acces, (2) utilizare, (3) divulgare, (4) modificare, (5) dislocare sau (6) distrugeri neautorizate ale atributelor informației, ale IS, TIC și infrastructurilor de procesare, depozitare, acces și transport al informațiilor, inclusiv mass-media, în scopul asigurării intimității persoanei, continuității afacerii, suveranității statului, diminuării pierderilor, dezinformării, inclusiv prevenirii scurgerii de date, spionaj[[3]](#footnote-3).

**2. Securitatea informațională în contextul globalizării.**

 La ziua de azi este evident că sfera informaţională, ca factor de organizare a societăţii contemporane, are o influenţă activă în situaţia politică, economică, de apărare şi alte componente ale securităţii statului. În mare parte, integritatea lumii contemporane, ca societate globală, este asigurată de schimbul informaţional.

Globalizarea, este un fenomen amplu dezbătut, nu putea să nu influenţeze aspectele legate de securitatea naţională, de ameninţările privind siguranţa oamenilor şi informaţiilor, a instituţiilor naţionale şi internaţionale. Extinderea la scară globală a utilizării diferitelor mecanisme de prelucrare şi comunicare a informaţiilor, de control al activităţilor a condus şi la apariţia nevoii de a lua în considerare noile aspecte ce influenţează securitatea spaţiului cibernetic global.

Implementarea activă şi multilaterală a tehnologiilor informaţionale a determinat transformarea structurii societăţii mondiale, conducînd treptat spre dispariţia frontierelor naţionale. In toate domeniile de activitate au apărut noi structuri funcţionale, la baza cărora se află Reţeaua. Acestea sînt şi corporaţiile transnaţionale, şi economia electronică (e-economia), şi asocierea colectivelor ştiinţifice, care lucrează asupra unor probleme comune, dar se află în diferite regiuni ale planetei. Dar aceste schimbări au atins şi partea negativă a vieţii umane. Structurile de reţea au devenit baza criminalităţii mondiale.

Reţelele de calculatoare sunt structuri deschise, la care se pot conecta un numar mare şi uneori necontrolat de calculatoare. Complexitatea arhitecturală şi distribuţia topologică a reţelelor conduc la o mărire necontrolată a mulţimii utilizatorilor cu acces nemijlocit la resursele reţelei- fişiere, baze de date, rutere etc. de aceea putem vorbi de o vulnerabilitate a reţelelor ce se manifestă în diferite moduri. Din această cauză un aspect crucial al reţelelor de calculatoare, în mod special al comunicaţilor pe Internet, îl constituie securitatea informaţiilor. Utilizatorii situaţi la mari distanţe trebuiesc bine identificaţi-în mod tipic prin parole. Cu părere de rău şi sistemele de parole au devenit vulnerabile, atât datorită hacker-ilor care şi-au perfecţionat metodele cât şi datorită alegerii incorecte a parolelor de către utilizatori. Necesitatea de securitate şi de autenticitate, apare la toate nivelele arhitecturale ale reţelelor.

În lume s-a creat spaţiul informaţional global unic, în care s-a manifestat o confruntare geostrategică informaţională între marile puteri, pentru atingerea superiorităţii în spaţiul informaţional mondial, în special în megapolisuri, centre-cheie ale societăţii informaţionale globale. Aceasta însă provoacă frecvent situaţii critice, deoarece omul de astăzi este practic permanent supus stresului[[4]](#footnote-4).

În condiţiile intersectării cu noile provocări şi ameninţări ale naturii, la care omul încă nu a reuşit să se adapteze şi să elaboreze contramăsuri, o actualitate deosebită capătă activitatea de asigurare a securităţii activităţii sale vitale - securitatea în sensul larg cuprinzînd toate domeniile activităţilor umane.

Securitatea naţională şi economia sînt total dependente de tehnologiile informaţionale şi de infrastructura informaţională. Nucleul infrastructurii informaţionale, de care depinde omenirea, se află Internetul. Utilizarea de către infractori a tehnologiilor informaţionale şi telecomunicaţionale, în primul rînd a reţelei Internet, prezintă un pericol serios în procesul de promovare a securităţii societăţii la nivel global. Cea mai importantă problemă de care sunt preocupaţi utilizatorii Internetului este problema securităţii informaţionale[[5]](#footnote-5).

Utilizării tehnicii de calcul în majoritatea domeniilor vieţii, precum şi conectarea calculatoarelor în reţele internaţionale a dus la faptul că infracţiunea comisă cu ajutorul sau prin intermediul calculatorului să fie mai diversă, mai periculoasă şi mai prezentă la nivel internaţional. La studierea factorilor generatori de acţiuni criminale s-a demonstrat că reţelele de comunicare şi calculatorul modern prezintă caracteristici specifice care sînt de mare utilitate pentru criminali şi implică serioase dificultăţi pentru potenţialele victime şi pentru aplicarea legii (probleme complexe de securizare a sistemelor, diversitatea sistemelor hard şi soft, lipsa de experienţă a multor utilizatori, anonimatul comunicării, criptarea şi mobilitatea internaţională). Grupurile care activează în domeniul crimei organizate, profesionişti în spionajul economic şi serviciile secrete din întreaga lume exploatează deja aceste noi caracteristici ale acţiunilor criminale cibernetice. Multe guverne, mulţi oameni de afaceri, mulţi utilizatori particulari nu realizează pericolul la care sînt expuşi prin aceste noi condiţii de comitere a crimei, nici semnificaţia protecţiei împotriva crimei cibernetice şi nici căile tehnice şi legale de contracarare a ameninţărilor infractorilor.

Odată cu avantajele şi transformările pozitive pe care le aduce globalizarea la nivelul naţiunilor, nu este lipsită de aspecte ce ridică, de multe ori, probleme şi îngrijorare, între care un loc din ce în ce mai important îl ocupă problematica securizării spaţiilor cibernetice, cu atît mai mult cu cît fenomenul terorismului a luat o amploare fără precedent, inclusiv terorismul informaţional.

În zilele noastre, este din ce în ce mai evident că, grupările teroriste utilizează pe larg Internetul pentru aşi atinge scopurile subversive. Printre cele mai bine reprezentate sînt mişcările de gherilă latino-americane, care dispun de o tehnică informatică de înaltă performanţă şi, de multe ori, de masive finanţări ce provin din fondurile unor capi ai traficanţilor de droguri. În condiţiile existenţei Internetului, teroriştii au posibilitatea de a lansa atacuri greu detectabile din orice punct al globului. Ei pot infecta sistemele informatice cu viruşi complecşi, care ar putea provoca disfuncţionalităţi grave în sisteme.

Calculatoarele au făcut ca multe activităţi economice să se desfăşoare mai uşor, dar în mod similar, ele au facilitat şi multe activităţi ilegale. Utilizarea tehnologiilor informaţionale şi comunicaţionale a permis ca vechile infracţiuni (de exemplu furtul de bani) să beneficieze de noi modalităţi de realizare şi a creat noi posibilităţi de fraudă (dirijarea de fonduri de către personalul angajat, „de încredere", care are sarcina de a actualiza fişierele).

 Infracţiunile comise cu ajutorul calculatorului, împotriva afacerilor sau pe seama companiilor economice, sînt comise de angajaţi, consideraţi persoane de încredere, sau de persoane din afara organizaţiei (hackeri, concurenţi neloiali, grupe criminale). Calculatorul, ca instrument al crimei, este foarte puternic. El nu numai că facilitează comiterea crimei, dar şi conferă infracţiunii un caracter devastator şi face extrem de dificilă identificarea autorului. Reţelele globale de sisteme informatice extind zona expusă infracţiunii şi fac ancheta, urmărirea judiciară şi arestul mult mai dificile. Un hoţ care fură o carte de credit obţine acces la o sumă mult mai mare decît cea la care ar avea acces un hoţ care fură un portofel. Informaţii confidenţiale privind afacerile pot fi furate din calculatoare şi sisteme de comunicare verbală fără să rămînă vreun semn care să indice intervenţia unui terţ prin „forţarea uşii".

Printre alte consecinţe negative ale informatizării, cauzate de dereglarea securităţii informaţionale, se numără terorismul şi huliganismul informaţional. Dacă hacherii pătrund în memoria sistemelor computerizate pentru satisfacerea ambiţiilor proprii, apoi cracherii mai şi „storc" băncile informaţionale. Asemenea „specialişti" sînt extrem de periculoşi pentru sistemele computerizate care dirijează rachetele de luptă, arma cosmică şi nucleară. Consecinţele amestecului lor „profesional" nu este greu de ghicit. Acest lucru poate deveni o tragedie nu numai pentru o ţară, dar şi pentru întreaga omenire.

Nivelul de securitate al calculatoarelor şi al reţelelor instalate în bănci, întreprinderi, administraţii şi organizaţii militare rămîne nesatisfăcător. O demonstrează miile de exemple de penetrări realizate de piraţii informatici, sabotaje, hold-up-uri electronice soldate cu milioane de dolari transferaţi.

Atacurile cibernetice asupra reţelelor informaţionale ale oricărei ţări pot avea consecinţe grave, cum ar fi întreruperea funcţionării unor componente-cheie, provocarea pierderilor de venituri şi proprietăţi intelectuale sau chiar pierderea vieţilor omeneşti. Contracararea unor astfel de atacuri necesită crearea unor componente riguroase, cum încă nu există în prezent, dacă se doreşte reducerea vulnerabilităţilor şi prevenirea sau diminuarea forţei capacităţilor îndreptate împotriva infrastructurilor critice[[6]](#footnote-6).

Ca rezultat al globalizării factorilor economici, politici şi militari, al expansiunii reţelelor şi sistemelor informaţionale globale, guvernele lumii, organizaţiile internaţionale sînt nevoite să-şi concentreze şi mai mult eforturile asupra asigurării securităţii globale, pentru că acum riscurile sînt mai mari ca oricînd, din cauza efectului de propagare în lanţ. Dacă pînă la apariţia reţelei globale asigurarea securităţii sistemelor informaţionale era o problemă de politică naţională, în momentul de faţă la stabilirea strategiilor şi politicilor de securizare a spaţiului cibernetic trebuie luate în considerare şi aspectele de compatibilizare şi standardizare la nivel global[[7]](#footnote-7).

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

Se practică două strategii de bază pe linia securităţii naţionale:

1. Tot ceea ce nu este interzis este permis.

2. Tot ceea ce nu este permis este interzis.

În multe ţări de pe glob, accesul la informaţiile naţionale este controlat prin legi privind secretul de stat, folosindu-se cea de-a doua strategie.

Statul, ca subiect de bază în asigurarea securităţii informaţiei prin intermediul organelor puterii legislative, executive şi judiciare, trebuie să asigure crearea condiţiilor privind realizarea securităţii şi coordonarea acţiunilor de securitate.

Scopurile securităţii informaţionale trebuie să fie stabilite pe baza priorităţilor constante ale securităţii naţionale ce corespund sarcinilor de lungă durată ale dezvoltării mediului informaţional al societăţii, incluzînd:

- apărarea intereselor naţionale ale statului în condiţiile globalizării proceselor informaţionale şi formării reţelelor informaţionale globale;

 - asigurarea organelor puterii şi conducerii de stat, persoanelor fizice şi juridice cu informaţie veridică, completă şi oportună, necesară pentru luarea deciziilor; prevenirea încălcării integrităţii resurselor informaţionale de stat, utilizării lor nelegitime şi ineficiente;

 - realizarea drepturilor cetăţenilor, organizaţiilor şi statului în vederea obţinerii, difuzării şi utilizării informaţiei;

 - susţinerea normelor democratice, în special a principiilor de interacţiune a statului, societăţii şi persoanei în mediul informaţional, în calitate de agenţi realmente egali ai relaţiilor democratice;

- protecţia informaţională a cetăţenilor.

Activităţile de bază trebuie orientate pe următoarele direcţii: depistarea, evaluarea şi pronosticarea surselor de pericol pentru securitatea informaţională, elaborarea unui complex de măsuri şi mecanisme pentru realizarea acesteia; crearea bazei normativ-legale de asigurare a securităţii informaţionale, coordonarea activităţii organelor puterii şi administrării de stat, structurilor menite să asigure securitatea informaţională; dezvoltarea sistemului de asigurare a securităţii informaţionale, perfecţionarea organizării ei, a formelor, metodelor şi mijloacelor de prevenire şi neutralizare a pericolelor securităţii informaţionale, lichidarea consecinţelor prejudicierii.

Dependenţa de informaţie este tot mai mare, chiar periculoasă. Există state care depind totalmente de informaţiile oferite de componentele spaţiului cibernetic naţional. Blocarea acestuia timp de cîteva ore poate să conducă la instaurarea haosului în ţara respectivă, afectînd, în bună măsură, şi securitatea sistemului informaţional global.

Experţii au declanşat o nouă ofensivă pentru perfecţionarea legislaţiei, întărirea rolului agenţilor de profil şi perfecţionarea produselor pentru prevenirea şi descoperirea delictelor informaţionale şi informatice. Deşi fenomenul infracţionalităţii informaţionale afectează majoritatea instituţiilor publice şi private, cu consecinţe de nebănuit, el capătă accente catastrofale cînd este vorba de siguranţa şi apărarea naţională, unde sistemul informaţional are o importanţă vitală în prelucrarea informaţiilor şi în asigurare fundamentării deciziilor.

 Iată de ce se impune cu acuitate necesitatea acordării unei atenţii sporite securităţii informaţiilor, în primul rînd prin asigurarea unei corecte clasificări a lor, dar şi prin elaborarea unor strategii coerente de securizare a spaţiului cibernetic.

**3. Riscuri şi ameninţări la adresa securității informaționale.**

Ameninţările specifice spaţiului cibernetic se caracterizează prin asimetrie şi dinamică accentuată şi caracter global, ceea ce le face dificil de identificat şi de contracarat prin măsuri proporţionale cu impactul materializării riscurilor. În prezent, confruntările cu ameninţările provenite din spaţiul cibernetic la adresa infrastructurilor critice, având în vedere interdependenţa din ce în ce mai ridicată între infrastructurile cibernetice şi infrastructuri, precum cele din sectoarele financiar-bancar, transport, energie şi apărare naţională. Globalitatea spaţiului cibernetic este de natură să amplifice riscurile la adresa acestora afectând în aceeaşi măsură atât sectorul privat, cât şi cel public[[8]](#footnote-8).

Posibilitatea ca sistemele informaţionale computirizate ale unei instituţii să fie insuficient protejate împotriva anumiţi atacuri sau pierderi este numit de către Straub(1998) risc de sistem. Pe de altă parte, putem spune că riscul este considerat ceva subiectiv care se referă la un viitor care există doar în imaginaţie. Conform lui Turban (1996) riscul este defenit ca posibilitatea unei ameninţări materializate.Riscul este în contextul sistemelor informaţionale computerizate, suma ameninţărilor (evenimete care pot cauza daune), vulnerabilităţilor şi valoarea informaţiilor expuse:

**RISC = AMENINŢĂRI+VULNERABILITĂŢI+VALOAREA INFORMAŢIILOR**

Informaţiile stocate electronic au anumită valoare. Un incident care va afecta negativ informaţiile stocate electronic va afecta şi individual instituţia care depinde sau foloseşte informaţiile respective. Reprezentarea schematică sugestivă a conceptelor privind securitatea sistemelor informaţionale şi relaţiile acestea este propusă în standardul CCITSE1 (Common Criteria for Information Technology Security Evaluation).

Pentru evaluarea potenţialului atacurilor posibile este necesar să fie înţelese expertiza, motivaţia şi intenţia potenţialilor atacatorilor. Un atacator care selectează sistemul în funcţie de insecurităţii pe care acesta le prezintă este diferit de un atacator care selectează pentru atac un sistem anume, pentru a comite anumite fapte.

Ameninţările la adresa spaţiului cibernetic se pot clasifica în mai multe moduri, dar cele mai frecvent utilizate sunt cele bazate pe factorii motivaţionali şi impactul asupra societăţii. În acest sens, putem avea în vedere criminalitatea cibernetică, terorismul cibernetic şi războiul cibernetic, având ca sursă atât actori statali, cât şi non-statali.

Principale persoane care generează ameninţări în spaţiul cibernetic sunt:

 - persoane sau grupări de criminalitate organizată care exploatează vulnerabilităţile spaţiului cibernetic în scopul obţinerii de avantaje patrimoniale sau nepatrimoniale;

 - terorişti sau extremişti care utilizează spaţiul cibernetic pentru desfăşurarea şi coordonarea unor atacuri teroriste, activităţi de comunicare, propagandă, recrutare şi instruire, colectare de fonduri etc., în scopuri teroriste;

- state sau actori non-statali care iniţiază sau derulează operaţiuni în spaţiul cibernetic în scopul culegerii de informaţii din domeniile guvernamental, militar, economic sau al materializării altor ameninţări la adresa securităţii naţionale[[9]](#footnote-9).

**Concluzie:** Securitatea informaţională este un domeniu mult prea vast şi cu prea multe domenii conexe pentru a fi detaliat complet undeva. Lumea este în continuă mişcare, cerinţele de securitate şi confidenţialitate cresc pe zi ce trece, ameninţările ţin pasul.

Dependenţa de informaţie este tot mai mare, chiar periculoasă. Există state care depind totalmente de informaţiile oferite de componentele spaţiului cibernetic naţional. Blocarea acestuia timp de cîteva ore poate să conducă la instaurarea haosului în ţara respectivă, afectînd, în bună măsură, şi securitatea sistemului informaţional global. În contextul dat, experţii au declanşat o nouă ofensivă pentru perfecţionarea legislaţiei, întărirea rolului agenţilor de profil şi perfecţionarea produselor pentru prevenirea şi descoperirea delictelor informaţionale şi informatice. Deşi fenomenul infracţionalităţii informaţionale afectează majoritatea instituţiilor publice şi private, cu consecinţe de nebănuit, el capătă accente catastrofale cînd este vorba de siguranţa şi apărarea naţională, unde sistemul informaţional are o importanţă vitală în prelucrarea informaţiilor şi în asigurare fundamentării deciziilor. Iată de ce se impune cu acuitate necesitatea acordării unei atenţii sporite securităţii informaţiilor, în primul rînd prin asigurarea unei corecte clasificări a lor, dar şi prin elaborarea unor strategii coerente de securizare a spaţiului cibernetic.

 În concluzie menționez că noile condiţii ce implică dezvoltarea societăţii informaţionale pe baza utilizării reţelelor informaţionale globale, dezvoltarea schimbului informaţional transfrontalier, globalizarea sistemului economiei mondiale şi creşterea nivelului informatizării necesită scoaterea în evidenţă a factorilor care anterior nu reprezentau ameninţări consi derabile. Aceşti factori fac ca securitatea intereselor naţionale în sfera informaţională să fie un element important al securităţii naţionale a statului.

**Bibliografie:**

1. Bellamy BJ. Vulnerability Identification and Remediation Through Best Security Practices, SANS Institute, 2002.

 2. Grime R.- Implementing Vulnerability Scanning in a Large Organisation, SANS Institute, June 2003.

3. Lundin E., Jonsson E. Survey of Intrusion Detection Research, Technical Report nr. 02-04, 2002.

4. Patriciu Victor-Valeriu, Pietroşanu-Ene Monica, Bica Ion, Cristea Costel-Securitatea informatică în UNIX şi INTERNET, Editura Tehnică, 1998.

5. Patriciu Victor-Valeriu, Pietroşanu-Ene Monica, Bica Ion, Priescu Justin-Semnături electronice şi securitate informatică. Aspecte criptografice, tehnice, juridice şi de standardizare, Editura BIC ALL, 2006.

6. Petersen R.Security Breaches: Notification, Treatment and Prevention, EDUCAUSE review, July/August 2005.

7. Vasilescu Andrei, Rachieru Dan, Vasile Irina, Filip Luminiţa, Vasilescu Elena-Ghid de aplicare a recomandărilor europene referitoare la confidenţialitatea comunicaţiilor, INSCC, decembrie 2005.

8. Walters N. –Into the Breach: Security Breaches and Identity Theft, AARP Public Policy Institute, July 2006.

9. Bragaru T., Briceag V., Malcocui V., Galaicu V. Securitatea informaţiei vis a –vis de securitatea informațională. USM.

<https://www.researchgate.net/publication/340087793_SECURITATEA_INFORMATIEI_VIS-A-VIS_DE_SECURITATEA_INFORMATIONALA>

10. https://ibn.idsi.md/sites/default/files/imag\_file/63-68\_4.pdf SECURITATEA INFORMAŢIONALĂ ÎN ERA TEHNOLOGICĂ Irina Babară, Marin Lupu Academia Militară a Forţelor Armate „Alexandru cel Bun”, revista SECURITATEA INFORMATIONALĂ 2013.

1. Bragaru T., Briceag V., Malcocui V., Galaicu V. Securitatea informaţiei vis a –vis de securitatea informațională. USM.

<https://www.researchgate.net/publication/340087793_SECURITATEA_INFORMATIEI_VIS-A-VIS_DE_SECURITATEA_INFORMATIONALA> [↑](#footnote-ref-1)
2. Bragaru T., Briceag V., Malcocui V., Galaicu V. Securitatea informaţiei vis a –vis de securitatea informațională. USM.

<https://www.researchgate.net/publication/340087793_SECURITATEA_INFORMATIEI_VIS-A-VIS_DE_SECURITATEA_INFORMATIONALA> [↑](#footnote-ref-2)
3. Bragaru T., Briceag V., Malcocui V., Galaicu V. Securitatea informaţiei vis a –vis de securitatea informațională. USM.

<https://www.researchgate.net/publication/340087793_SECURITATEA_INFORMATIEI_VIS-A-VIS_DE_SECURITATEA_INFORMATIONALA> [↑](#footnote-ref-3)
4. https://ibn.idsi.md/sites/default/files/imag\_file/63-68\_4.pdf SECURITATEA INFORMAŢIONALĂ ÎN ERA TEHNOLOGICĂ Irina Babară, Marin Lupu Academia Militară a Forţelor Armate „Alexandru cel Bun”, revista SECURITATEA INFORMATIONALĂ 2013. [↑](#footnote-ref-4)
5. https://ibn.idsi.md/sites/default/files/imag\_file/63-68\_4.pdf SECURITATEA INFORMAŢIONALĂ ÎN ERA TEHNOLOGICĂ Irina Babară, Marin Lupu Academia Militară a Forţelor Armate „Alexandru cel Bun”, revista SECURITATEA INFORMATIONALĂ 2013. [↑](#footnote-ref-5)
6. https://ibn.idsi.md/sites/default/files/imag\_file/63-68\_4.pdf SECURITATEA INFORMAŢIONALĂ ÎN ERA TEHNOLOGICĂ Irina Babară, Marin Lupu Academia Militară a Forţelor Armate „Alexandru cel Bun”, revista SECURITATEA INFORMATIONALĂ 2013. [↑](#footnote-ref-6)
7. https://ibn.idsi.md/sites/default/files/imag\_file/63-68\_4.pdf SECURITATEA INFORMAŢIONALĂ ÎN ERA TEHNOLOGICĂ Irina Babară, Marin Lupu Academia Militară a Forţelor Armate „Alexandru cel Bun”, revista SECURITATEA INFORMATIONALĂ 2013. [↑](#footnote-ref-7)
8. https://ibn.idsi.md/sites/default/files/imag\_file/63-68\_4.pdf SECURITATEA INFORMAŢIONALĂ ÎN ERA TEHNOLOGICĂ Irina Babară, Marin Lupu Academia Militară a Forţelor Armate „Alexandru cel Bun”, revista SECURITATEA INFORMATIONALĂ 2013. [↑](#footnote-ref-8)
9. https://ibn.idsi.md/sites/default/files/imag\_file/63-68\_4.pdf SECURITATEA INFORMAŢIONALĂ ÎN ERA TEHNOLOGICĂ Irina Babară, Marin Lupu Academia Militară a Forţelor Armate „Alexandru cel Bun”, revista SECURITATEA INFORMATIONALĂ 2013. [↑](#footnote-ref-9)