UNIVERSITATEA POLITEHNICA DIN BUCUREŞTI

Școala Doctorală de Inginerie Industrială și Robotică

Nr. Decizie ___/___.___._____

TEZĂ DE DOCTORAT

- REZUMAT –

CERCETĂRI ȘI CONTRIBUȚII PRIVIND IMPLEMENTAREA SISTEMELOR DE CALITATE-RISC ÎN VEDEREA ASIGURĂRII SECURITĂȚII INFORMAȚIONALE ÎN INSTITUȚIILE PUBLICE

Conducător de doctorat: Prof. univ. em. dr. ing. ec. Constantin MILITARU

Autor: drd. Adrian-Viorel Dragomir

COMISIA DE DOCTORAT

Președinte	Prof.univ.dr.ing. Nicolae IONESCU	de la	Universitatea Politehnica București
Conducător de doctorat	Prof.univ.em.dr.ing.ec. Constantin MILITARU	de la	Universitatea Politehnica București
Referent	Conf.univ.dr.ing.mat. Ovidiu BLAJINĂ	de la	Universitatea Politehnica București
Referent	Prof.univ.dr.ing.mat. Adriana Alexandru	de la	Inst. Nat. de Cer. – Dezv. în Informatică
Referent	Conf.univ.dr. Răzvan Grigoraș	de la	Academia Națională de Informații București

BUCUREȘTI
2022

MULȚUMIRI

Doresc pe această cale să îmi exprim întreaga recunoștință și să îi mulțumesc domnului prof. univ. em. dr. ing., dr. ec. Constantin Militaru pentru întregul suport oferit pe parcursul redactării Tezei de doctorat și rapoartelor științifice intermediare. Întreaga cercetare a fost efectuată sub directa îndrumare a domnului profesor, ce mi-a călăuzit pașii pe tot parcursul etapelor pe care le-a presupus acest demers și mi-a susținut decizia de a aborda un domeniu atât de interesant, precum sistemele de management a securității informațiilor în contextul implementării acestora în cadrul instituțiilor publice.

Mulțumesc familiei și în special soției, copiilor, prietenilor și colaboratorilor, pentru răbdarea și încrederea acordată, ce m-au ajutat să duc la bun sfârșit o astfel de activitate susținută.

Doresc pe această cale să aduc mulțumiri conducerii „Facultății de Inginerie Industrială și Robotică" din cadrul „Universității Politehnica din București" pentru eforturile depuse de a îmbunătăți continuu calitatea procesului educațional, pe care l-am găsit aici pe parcursul studiilor doctorale, atât din punct de vedere logistic și operațional, cât și din punct de vedere al nivelului ridicat de calitate a educației formale, ce a reprezentat un real sprijin pentru mine pe întreg parcursul stagiului doctoral.

Mulțumesc de asemenea conducătorilor instituțiilor publice în care mi-am desfășurat timp de doisprezece ani activitatea profesională și șefilor compartimentelor IT și Tehnologia Informațiilor din care cu onoare am făcut parte, datorită cărora am acumulat informații consistente în acest sistem complex dar interesant și în egală măsură competitiv, dar care oferă multe satisfacții profesionale când privești la ce ai lăsat în urmă.

Experiența acumulată pe parcursul anilor de activitate în domeniul abordat în prezenta lucrare în cadrul instituțiilor publice, m-au ajutat să înțeleg în profunzime importanța securității informațiilor și să conștientizez că pentru asigurarea unui climat de securitate nu este suficientă cheltuirea fondurilor publice pe sisteme sau programe complexe, ci este nevoie de măsuri și proceduri de securitate care să reglementeze toate procesele interne cu scopul de a implementa, testa și menține măsuri tehnice și operaționale de securitate a informațiilor în interiorul instituției.

Întreaga activitate de cercetare desfășurată în timpul doctoratului am putut să o materializez cu sprijinul colegilor și colaboratorilor din domeniu IT&C și cu acest prilej doresc să le fiu recunoscător pentru informațiile oferite și întregul lor suport.

CUPRINS

INTRODUCERE

Aproximativ patru miliarde de oameni folosesc Internetul zilnic în contextul exploziei conceptului de IoT (Internet of Things) ce reprezintă conectarea la Internet a unor echipamente din ce în ce mai complexe, IT&C, electrocasnice, rețele sociale, bloguri, platformele digitale, toate reprezentând instrumente ce prin intermediul conectării la Internet permit generarea de conținut de către utilizator.

Securitatea națională este fundamentul funcționării normale a oricărei societăți, în care cetățenii pot dispune de condiții optime de viață și de activitate prin protejarea de riscuri, pericole, şi amenințări de securitate. Se poate spune că securitatea este un bun de care trebuie să beneficieze întregul popor, de aceea toate țările trebuie să asigure condițiile unei vieții normale pentru cetățenii săi.

Riscurile de securitate de la nivel mondial impun schimbarea metodelor de identificare, gestionare și combatere a riscurilor și pericolelor în privința securității, începând de la nivel de individ și până la nivel național și regional. În era globalizării, amenințările de securitate au căpătat valențe transfrontaliere, iar guvernele sunt obligate să găsească soluții inteligente și inovatoare, ori de câte ori se confruntă cu o problemă ce are potențialul afectării stabilității și securității naționale.

Acum câteva decenii securitatea națională era definită printr-o singură componentă, respectiv cea militară, dar în zilele noastre acest concept a căpătat valențe multidimensionale, cele mai importante fiind, cele economice, sociale, umane, politice, diplomatice, energetice și de mediu. Se poate observa la nivel național păstrarea obiectivelor guvernamentale principale în ceea ce privește managementul calitate-risc în acest domeniu, respectiv, creșterea nivelului de securitate, minimizarea riscurilor și amenințărilor de securitate a informațiilor la nivelul administrației publice, ținând cont că instituțiile publice românești continuă procesele de dezvoltare și modernizare în vederea alinierii la standardele Uniunii Europene.

La nivelul țării noastre s-a schimbat mult paradigma informațională în ultimele 3 decenii, începând să utilizeze cu precădere tehnologia informației în mai toate domeniile de activitate și cu precădere în mediul guvernamental. Informațiile, care până atunci aveau ca suport hârtia, au început să se transforme în format electronic. Astfel, în ultimii ani infrastructurile informaționale s-au dezvoltat simțitor, ducând la interconectarea globală ce a atras după sine și riscurile specifice digitalizării.

Indiferent de denumirea abordării alese, este întotdeauna important să se identifice și să se conștientizeze amenințările la adresa securității informațiilor, flagel care poate exista la nivelul fiecărei țări în parte, să se selecteze, să se implementeze și să se mențină în mod consecvent politici, strategii, procese și măsuri de securitate a informațiilor adecvate, atât la nivelul instituțiilor de stat cât și al celor private.

În cele 5 capitole ale tezei de doctorat este realizat un studiu asupra tendințelor actuale în ceea ce privește implementarea Sistemelor de management ale securității informațiilor în cadrul instituțiilor publice cu scopul creșterii gradului de securitate a informațiilor din aceste entități.

CAPITOLUL 1
STADIUL ACTUAL AL CERCETĂRILOR PRIVIND SECURITATEA INFORMAȚIONALĂ

1.1.ROLUL ȘI LOCUL SECURITĂȚII INFORMAȚIILOR LA NIVEL CONCEPTUAL

În capitolul I am realizat **o analiză a situației actuale cu privire la asigurarea securității informațiilor prin intermediul managementului calitate-risc** la nivel național, european și internațional.

În sensul cercetării de față informația va fi definită și utilizată din prisma conceptului de securitate în general și de securitate informațională în particular, a cărei definiție o regăsim la **art.15 lit.a) din Legea nr. 182/2002 privind protecția informaţiilor clasificate**, capitolul Dispoziții generale – Definiții, respectiv „informații - orice documente, date, obiecte sau activităţi, indiferent de suport, formă, mod de exprimare sau de punere în circulație.”[1]

Informațiile stau la baza securității naționale și elaborarea documentelor specifice informațiilor se gestionează prin intermediul sistemelor informaționale, ce se regăsesc în arhitectura tuturor organelor de conducere a statului.

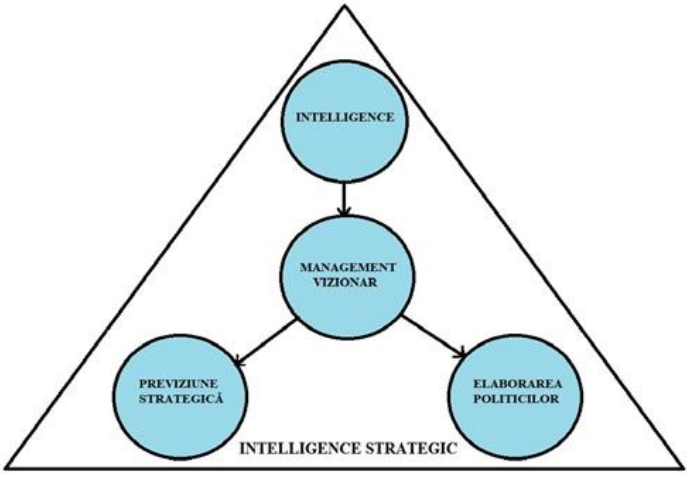

Fig. 1.1. Principiile ce stau la baza conceptului de intelligence strategic (propunere autor)

1.1.1.Delimitarea ariei de acoperire a securității informațiilor în mediul on-line

Vulnerabilitatea în domeniul informațiilor din mediul on-line este un defect al unui sistem prin intermediul căruia se gestionează informații, care poate lăsa porți deschise atacului și se poate referi la orice tip de slăbiciune a unui sistem informațional, a unui set de proceduri sau în orice context care expune securitatea informației oricărui tip de amenințări.

Vulnerabilitățile informațiilor din mediul on-line sunt definite ca puncte nevralgice sau slăbiciuni ce se strecoară în procesul de design sau în cel de construire a sistemelor hardware, software, a rețelelor informaționale sau a procedurilor de securitate, prin intermediul cărora se gestionează informațiile. Pe scurt, „vulnerabilitatea este o slăbiciune care permite o acțiune neautorizată”.[2]

Sistemul este unul dintre conceptele de bază atunci când vorbim despre informații, dar este adesea folosit și în multe domenii din știință. Fiind un concept primar foarte comun, acesta nu a fost definit foarte strict, într-un mod general acceptat, dar, prin descrierea caracteristicilor sale principale, conceptul poate fi înțeles într-un mod intuitiv.

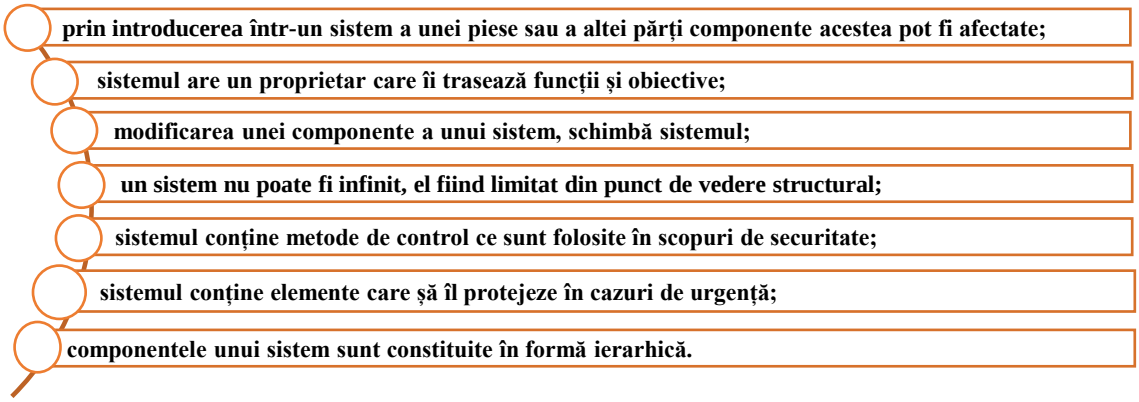

Fig. 1.2. Caracteristicile principale ale sistemelor (propunere autor)

Obiectivele unui sistem de securitate pot fi determinate prin analizarea amănunțită a obiectivelor sistemului în general pentru care trebuie asigurată securitatea și a modului de interacțiune a acestuia cu mediul on-line pentru atingerea scopului pentru care a fost creat. Orice sistem informațional ce este conectat în mediul virtual are nevoie de securitate, ceea ce justifică obiectivele comune ale celor două tipuri de sisteme.

1.1.2. Analiza aspectelor tehnice și juridice ale cyberspațiului

Cyberspațiul sau **spațiul cibernetic** este definit prin orice interacțiune a omului cu mediul on-line ce a devenit o obișnuință pentru o foarte mare parte din populație. Spațiul cibernetic poate fi caracterizat printr-o prezență universală și în majoritatea aspectelor vieții de zi cu zi, ce se pot desfășura în mediul on-line.

Una din componentele cele mai importante ale cyberspațiului este **Internetul**, rețeaua prin intermediul căreia se interconectează între ele majoritatea celorlalte rețele, ce pot avea diferite tipuri sau structuri, fiind publice sau private și gestionate în aproape toate țările lumii.

Amenințările cibernetice au devenit impedimente zilnice și obișnuite în viețile noastre, iar majoritatea specialiștilor vorbesc deja despre acest flagel ca fiind similar unui război cibernetic, cel mai bun exemplu în acest sens fiind Statele Unite ale Americii, care, de mai multă vreme a încadrat în legislația specifică atacurile cibernetice în rândul atacurilor teroriste.

1.1.3.Unele aspecte privind exploatarea malițioasă a cyberspațiului

În contextul actual caracterizat de vulnerabilități majore din punct de vedere al securității, informația a devenit o valoare inestimabilă pentru orice entitate, fiind surclasate, poate, doar de resursele umane. Fiecare aspect al societății este influențat de mediul on-line, căci majoritatea infrastructurilor sunt interconectate. Prin această afirmație nu susținem ipoteza că toate aspectele vieții au legătură directă cu mediul on-line, ci că orice individ sau entitate, indiferent dacă este activ sau nu în mediul virtual, poate fi afectat de acest aspect.

Din perspectiva oricărui tip de entitate, publică sau privată, informația este un bun de mare preț, ceea ce a impus securitatea informațiilor ca o activitate de o importanță deosebită pentru acestea, fie că derulează afaceri electronice fie că servesc interesul publicului larg.

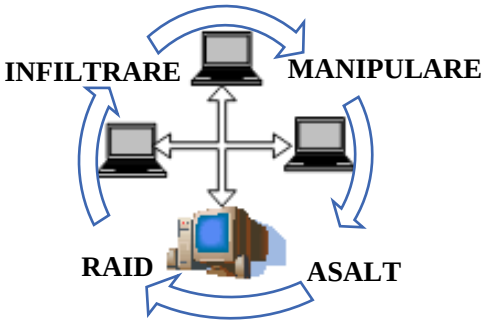

Figura 1.4. Secvențele unui atac asupra informațiilor din rețele informaționale (propunere autor)

Securitatea informațiilor joacă un rol de bază în managementul securității sistemelor informaționale, importanța sa fiind luată în considerare tot mai des în ultima perioadă, de

entitățile publice sau private după ce au văzut experiențele negative ale proprietarilor site-urilor care nu și-au întărit securitatea cibernetică și au avut probleme datorate exploatării vulnerabilităților de către hackeri, rezultatul fiind pătarea reputației și pierderi financiare mari.

1.2. CERCETĂRI PRIVIND ASIGURAREA SECURITĂȚII INFORMAȚIONALE

De-a lungul timpului **tehnologia în domeniul informațiilor** a cunoscut o dezvoltare galopantă, iar progresele înregistrate în domeniu au atras după sine implementarea acestor tehnologii în toate domeniile societale. În prezent, existența și funcționarea societății umane se află în strânsă legătură cu tehnologia informațiilor, dacă nu chiar dependentă de funcționarea la parametri normali a infrastructurilor informaționale în anumite sectoare critice.

A**tacurile cibernetice** ce au ca scop furtul de informații, ca amenințare la adresa securității globale, sunt prezentate în strânsă legătură cu crima organizată, traficul ilicit și atacurile teroriste. Cauzele atacurilor la adresa rețelelor informaționale pot avea rațiuni financiare, respectiv finanțarea activităților de crimă organizată și terorism, sau de facilitare a producerii acestor tipuri de atac, aici referindu-ne la atacurile teroriste care au loc în corelare cu exploatarea vulnerabilităților sistemelor prin intermediul cărora se gestionează informațiile.

Tehnologiile informaționale utilizate în scopurile pentru care au fost proiectate inițial, ce respectă integritatea și securitatea informațională și principiile generale de bună conduită, cum ar fi responsabilitatea, vigilența și respectul față de ceilalți reprezintă modele de urmat privind păstrarea securității și a unui climat ce inspiră siguranță.

Spațiul cibernetic, este mediul care găzduiește cea mai mare parte a informațiilor în zilele noastre și este sinonim cu termeni precum „realitate virtuală, mediu on-line, spațiu digital, care alcătuiesc împreună un aparat conceptual”[3].

1.2.1.Metode de asigurare a securității informațiilor în mediul online

Importanța asigurării securității informațiilor derivă din faptul că astăzi, majoritatea informațiilor cu caracter confidențial sau clasificat precum, informațiile cu privire la sistemele de apărare ale unui stat și elementele de bază ale acestora, tehnologii de fabricație, efectivele și dispozitivele militare, date referitoare la sistemele de comunicații, hărți, date referitoare la alimentarea cu energie electrică, apă, gaze, date științifice, tehnologice, economice, sunt stocate pe infrastructuri informatice.

În vederea asigurării securității informațiilor și îmbunătățirii politicilor privind lupta împotriva criminalității informaționale, Parlamentul și Comisia Europeană au creat strategii și acte normative, pentru a trata acest flagel al secolului XXI. Astfel, la nivelul Parlamentului European a fost adoptată „Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune” în anul 2016, ce este cunoscută și sub numele de **Directiva NIS**.

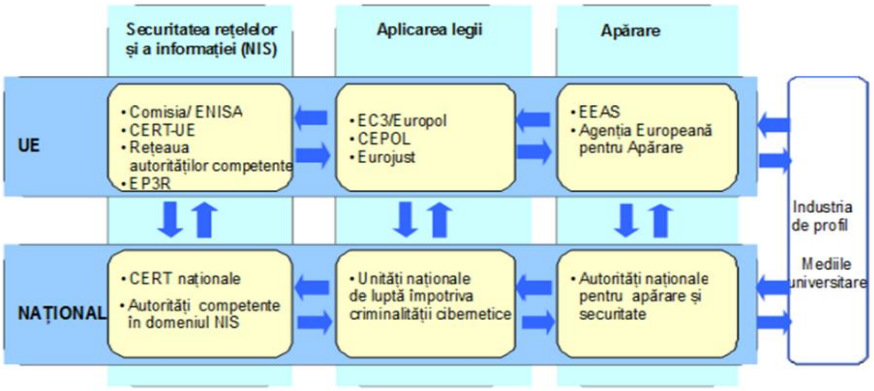

Fig. 1.6. Pilonii principali din cadrul Directivei NIS (sursa: Agenția Uniunii Europene pentru Securitate Cibernetică-ENISA)

1.2.2.Importanța asigurării securității rețelelor de comunicații pentru protejarea informațiilor

Rețeaua informațională este un grup interconectat de echipamente de procesare, echipamente de comutare și ramuri de interconectare, iar asigurarea securității unei rețele de comunicații se face atât prin protecție la nivel fizic, cât și prin protecție la nivel informațional.

Trebuie menționat că o rețea nu trebuie să fie conectată la Internet pentru a funcționa, dimpotrivă, la ora actuală rețelele importante nu sunt conectate la Internet pentru a nu fi vulnerabile la atacuri venite din zona Internetului.

Securitatea rețelelor informaționale este ramura „responsabilă cu designul, implementarea și funcționarea rețelelor astfel încât securitatea informației să își atingă scopul, într-o rețea interconectată la nivel organizațional, între organizații și între organizații și utilizatori”[4].

1.2.3.Securitatea informațiilor pe Internet

Securitatea rețelei Internet se referă la „protejarea serviciilor legate de Internet și sistemele tehnologiei de comunicație a informațiilor, ca o extensie a securității rețelei în organizații și la domiciliu, pentru a atinge scopul de securitate”[5].

Orice persoană sau entitate dorește să se simtă în siguranță atunci când navighează pe Internet, din toate punctele de vedere, de la cel personal, financiar, informațional, la cel al imaginii sale în zona publică.

Securitatea Internetului este activitatea responsabilă cu funcționarea, disponibilitatea și fiabilitatea serviciilor ce se accesează prin intermediul Internetului. Securitatea de pe Internet se deosebește de securitatea rețelelor interne în principal din cauze cantitative, prin faptul că Internetul însumează miliarde de utilizatori, în timp ce o rețea internă poate avea un număr mult mai mic de utilizatori.

1.2.4.Securitatea tehnologiei prin intermediul căreia se gestionează informațiile

Definirea acestei componente a securității informațiilor vine din limba engleză - information communications technology security - și se referă la supravegherea securității echipamentelor sau programelor prin intermediul cărora se procesează, stochează sau transmit informațiile, precum și a modului în care aceste device-urile sau soft-uri sunt fabricate, astfel încât acestea să respecte standardele în materie de siguranță a informațiilor.

Atacurile cibernetice sunt adesea folosite pentru a avea acces la fluxul de informații privitoare la tehnologie sau planuri de proiectare din diverse domenii, de la tehnica militară până la industria civilă, pentru a întrerupe sau a perturba funcționarea normală a infrastructurii, pentru a opri comunicarea și transmiterea de mesaje publice și pentru a influența procesele decizionale.

1.3.CERCETĂRI PRIVIND ASIGURAREA SECURITĂȚII INFORMAȚIILOR GESTIONATE DE INFRASTRUCTURILE CRITICE

Puterea unui stat este întotdeauna relativă, nu poate fi stabilită cu exactitate, ea fiind evaluată în funcție de puterea instituțiilor naționale, de nivelul rezervelor financiare ale statului și de puterea de cumpărare a cetățenilor țării, dar în același timp trebuie precizat că la bazele puterii stau informațiile. Puterea unui stat este alcătuită dintr-o serie de elemente ale instituțiilor naționale, elemente identificate de Hans Morgenthau în cartea sa – „Politica între națiuni - lupta pentru putere și pace”[6].

Infrastructurile critice ale oricărui stat au nevoie de asigurarea unui mediu de securitate puternic, ce are ca scop declarat protejarea informațiilor care sunt în proprietatea sau doar operate de acestea. Securitatea infrastructurilor critice trebuie să fie asigurată de către entitățile ce sunt desemnate în acest sens de organele abilitate ale statului.

În anul 2010 România a implementat prevederile UE privind protecția infrastructurilor critice, prin transpunerea prevederilor „Directivei Europene nr. 2008/114/CE a Consiliului din

anul 2008, privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora în legislația națională", ce s-a realizat prin adoptarea la nivelul Guvernului României a „Ordonanței de Urgență nr. 98 din 2010 privind identificarea, desemnarea și protecția infrastructurilor critice din România".

Elementele ce stau la baza puterii naționale ale statului român sunt: populația, informațiile, poziționarea pe harta geo-politică, bogățiile naturale, caracteristicile poporului, nivelul guvernării, moralul națiunii capacitatea economică și nivelul de înzestrare și pregătire a armatei.

Când ne referim la infrastructură critică națională trebuie să avem în vedere faptul că aceasta constituie o condiție esențială a vieții, stabilitatea și funcționarea infrastructurii critice putând influența decisiv orice altă activitate socială sau economică. În toate conflictele militare ce au avut loc în istorie, infrastructurile critice au fost primele vizate de atacuri, dar, în secolul XXI riscul atacării infrastructurilor critice a trecut în dimensiunea virtuală, ne mai fiind nevoie de distrugerea fizică a acestora.

1.4.TIPURILE DE ATACATORI AI SISTEMELOR INFORMAȚIONALE ȘI SCOPURILE URMĂRITE

În literatura de specialitate am identificat șase **categorii de atacatori ai sistemelor informaționale**, definiți în funcție de obiectivele atacurilor și de ceea ce îi motivează pentru a ataca, după cum urmează: **hackerul, spionul, teroristul, atacatorul cu scop economic, criminalul de profesie și vandalul**.[7]

Infractorii cibernetici sunt denumiți generic **hackeri** și sunt „acele persoane care încearcă să obțină, în mod ilegal, controlul unui sistem de securitate, computer sau rețea, cu scopul de a avea acces la informații confidențiale sau avantaje materiale"[8]. Interesant este faptul că, la origine, termenul de hacker nu a avut din totdeauna o conotație negativă, referindu-se la începuturile erei tehnologice la „programator sau utilizator"[9].

Când se analizăm scopurile atacurilor cibernetice, se observă că atacurile ce au ca obiectiv spionajul economic și politic sunt de obicei asociate statelor, iar atacurile cu scop infracțional și terorist au legătură cu actorii non-statali.

Spionajul informațional și ne referim aici preponderent la cel din domeniul comercial, unde atacurile sunt îndreptate către marile companii și corporații, are ca scop "obținerea prin mijloace nelegitime sau divulgarea, transferul și folosirea fără drept, ori fără altă justificare legală a unui secret comercial sau industrial, cu intenția de a cauza un prejudiciu economic persoanei care deține dreptul asupra secretului sau de a obține pentru sine sau pentru o terță parte avantaje economice ilicite"[10].

Războiul informațional se consideră a fi următorul tip de război al secolului nostru, atacurile asupra informațiilor fiind extrem de eficiente în cazul unui astfel de conflict, acestea provocând panică și distrugeri și facilitând superioritatea atacatorului.

Spionajul electronic filtrează informațiile fiind concentrat exclusiv pe țintele importante, informațiile obținute fiind exact cele dorite. În spionajul clasic, când se depistează sursa scurgerii de informații, agentul sau rețeaua sunt depistați și interogați, putându-se afla apartenența acestora vizavi de o țară, declanșându-se astfel un scandal diplomatic între cele două țări implicate. Spre deosebire, spionajul electronic chiar dacă este depistat nu se poate afirma cu exactitate țara responsabilă, eliminând din start astfel de acuze de spionaj, pe care le pot declara nefondate din lipsă de dovezi incriminatorii.

Criminalitatea informațională este o problemă internațională din simplul fapt că majoritatea atacurilor din on-line au drept autori persoane din afara granițelor, lucru ce derivă din caracteristicile spațiului virtual, un spațiu lipsit de frontiere. Prin urmare, statul în care a avut loc incidentul respectiv este pus în imposibilitatea de a depista și trage la răspundere

autorul. Este necesară o „legislație valabilă în toate țările lumii”[11], pentru a putea combate eficient acest gen de atacuri.

1.5. PRINCIPIILE STRATEGIEI DE SECURITATE A INFORMAȚIILOR ÎN UNIUNEA EUROPEANĂ

Deopotrivă, Internetul și întreg spațiul virtual, au avut în ultima perioadă o influență definitorie asupra majorității componentelor vitale ale societății. Viața cotidiană, drepturile fundamentale ale omului, interacțiunea socială și finanțele fiecărei persoane depind în mare măsură de tehnologia informațiilor și comunicațiilor și de funcționarea permanentă a acestora, deoarece defecțiunile sau nefuncționarea acestor sisteme poate crea dezechilibre în societate, sau chiar dezastre.

Statul de drept și drepturile omului trebuie protejate în spațiul virtual în egală măsură de statele membre UE și de entitățile ce au atribuții legale în protejarea acestora, indiferent dacă au finanțare de stat sau privată. Libertățile și bunăstarea fiecărui cetățean sunt legate intrinsec de existența unui Internet protejat și progresist, ce poate avea aceste calități dacă companiile private din acest domeniu aduc în permanență inovații ce să fie sprijinite de societatea civilă, pentru ca acesta să continue să crească.

Tehnologia informațiilor și comunicațiilor, o dată cu dezvoltarea sa masivă, a fost transformată în principalul mijloc de creștere economică și principala resursă pentru dezvoltarea diferitelor sectoare ale economiei. TIC este în prezent fundamentul pentru susținerea tuturor sistemelor informaționale complexe, prin intermediul cărora este asigurată funcționarea în parametrii optimi a economiilor naționale în sectoare cheie și infrastructuri critice precum energia, finanțele, sănătatea și transporturile.

Strategia europeană de securitate cibernetică, în vigoare din anul 2013, statuează principiile ce ghidează politicile de securitate cibernetică în statele membre și în relația acestora cu celelalte țări la nivel internațional. Conform acestui document strategic, valorile fundamentale europene trebuie să fie aplicate în mediul material în egală măsură cu cel virtual.

Viziunea UE din Strategia de securitate cibernetică se articulează pe cinci mari priorități, care abordează o serie de provocări de securitate informațională pe care le detaliem în cele ce urmează și le menționăm în figura 1.11:

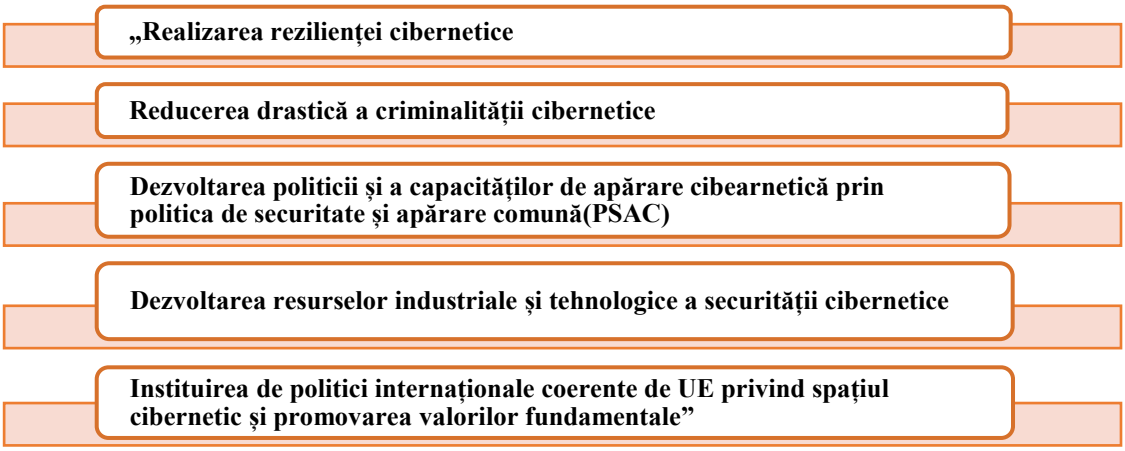

Fig. 1.11. Prioritățile strategice ale UE în privința securității cibernetice (sursa: Strategia europeană de securitate cibernetică [12])

În luna decembrie a anului 2020, Comisia Europeană a publicat spre aprobare o nouă versiune îmbunătățită a Strategiei de securitate cibernetică a Uniunii Europene ce va modifica semnificativ prevederile Strategiei în vigoare din anul 2016, iar statele membre vor trebui să adopte măsuri de implementare a noilor concepte de securitate informațională cuprinse în noua variantă.

Scopul noii strategii europene de securitate cibernetică este consolidarea relațiilor de cooperare a entităților responsabile cu securitatea din mediul guvernamental cu organizațiile neguvernamentale și mediul academic, integrarea tuturor centrelor de coordonare existente pentru a coopera și de a întreprinde acțiuni pentru consolidarea cunoștințelor cu privire la riscurile de securitate a informațiilor, prin planuri de stimulare și conlucrare între mediile militar-civile și public-private.

1.6. VULNERABILITĂȚILE INFORMAȚIILOR DIN MEDIUL ON-LINE ȘI MODALITĂȚI DE REMEDIERE

În ultimele decenii, societatea a utilizat din ce în ce mai mult informația în format electronic, modalitate ce a câștigat din ce în ce mai mult teren pentru că lumea are nevoie de informație în mișcare și în timp real. La ora actuală există foarte multe informații sensibile, confidențiale sau secrete ce sunt procesate, transferate sau stocate în mediul electronic, care trebuie protejate împotriva răuvoitorilor.

Majoritatea entităților, fie că sunt guvernamentale sau private, își desfășoară activitățile zilnice cu ajutorul tehnologiei informației, iar nefuncționarea acesteia sau modificarea datelor acestora poate implica grave prejudicii financiare sau reputaționale. Vulnerabilitățile care pot apărea într-o rețea informațională pot fi de mai multe tipuri, după cum urmează: **a) Culegerea de informații privind profilul țintei (target fingerprinting), b) Coduri răuvoitoare, c) Refuzul serviciului, d) Compromiterea conturilor, e) Acces prin tentative de pătrundere, f) Accesul neautorizat la informații, g) Modificări ilicite de informații, h) Accesul neautorizat la sistemele de comunicații, i) Spam.**

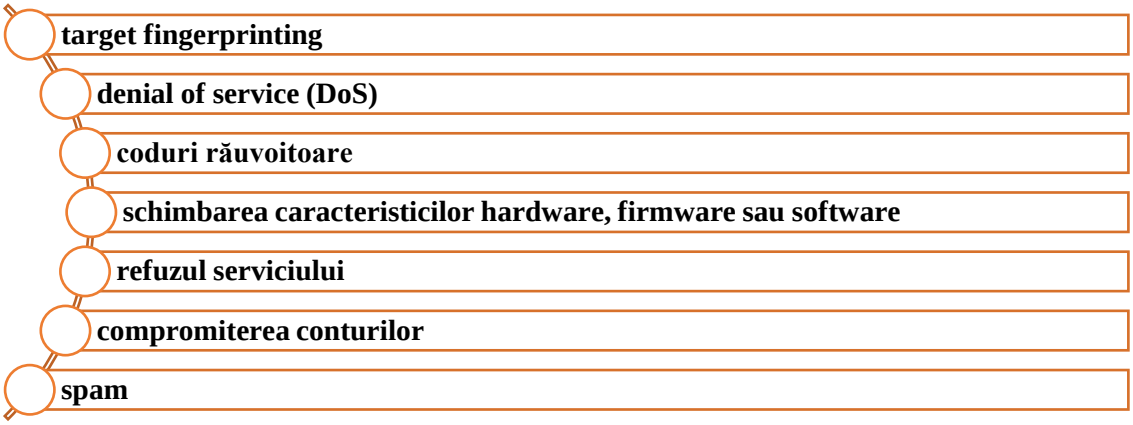

Fig. 1.12. Vulnerabilitățile informațiilor din mediul on-line (propunere autor)

Pentru rezolvarea acestor probleme a luat naștere echipele tehnice de tip CERT (Computer Emergency Response Team).

1.6.1. Comunitatea CERT și acțiunile specifice în domeniul securității informațiilor

Un grup de experți ce au ca responsabilități răspunsul la incidentele de securitate a informației poartă denumirea de **Computer Emergency Response Team (CERT)**. Aceste entități mai sunt denumite și **Computer Security Incident Response Team (CSIRT)**, cele două denumiri reprezentând în mare același tip de entitate, diferențe dintre cele două fiind minore. Termenul - CERT a fost înregistrat în registrul mărcilor înregistrate, fiind astfel protejat de legile copyright-ului. [13]

Responsabilitățile principale ale unui CERT/CSIRT sunt acțiunile proactive și reactive cu scopul de a proteja securitatea informațiilor unei organizații. CERT-urile nu pot avea responsabilități similare sau standardizate, căci fiecare echipa desfășoară activităţi în funcție de nevoile identificate la nivelul fiecărui client. Obiectivele tehnice ale unui CERT trebuie să se muleze pe obiectivele generale și specifice ale organizațiilor beneficiare de servicii de securitate, oricare ar fi tipul de servicii ales de aceștia din multitudinea acestui domeniu.

1.6.2. Aspecte teoretice privind auditul de securitate a informațiilor

Auditul sistemelor informaționale este un proces prin care o echipă formată din experți în domeniu fac **o analiză independentă și obiectivă** asupra nivelului de securitate a unui sistem informațional. Aceste activități trebuie să se desfășoare cu respectarea regulilor și obiectivelor impuse de standardele universal de audit acceptate în acest domeniu.

Totodată trebuie să se stabilească **obiective foarte bine definite ale auditului**, cum ar fi conformitatea cu anumite sisteme de management al securității informaționale, sau pur și simplu analiza protecției oferite sistemului informațional prin intermediul unui dispozitiv de protecție, exemplu în acest sens fiind auditul echipamentelor de tip firewall din cadrul unui sistem informațional.

Auditul de securitate a informațiilor bazat pe evaluarea riscurilor este mai complet și mai eficient pentru managementul organizației decât un audit clasic de sistem, care realizează doar o radiografie multicriterială a acestuia. Din cauza importanței informațiilor pentru orice tip de entitate, publică sau privată, evaluarea riscurilor de securitate a informațiilor trebuie considerată un obiectiv de importanță strategică, iar managementul trebuie să actualizeze permanent aceste evaluări și să verifice permanent controalele de securitate.

1.6.3. Analiza aspectelor generale privind managementului riscurilor de securitate a informațiilor

Domeniul analizei de risc a securității informațiilor reprezintă o preocupare curentă a tuturor entităților ce și-au creat un scop din protejarea securității, optimizarea funcționării acestora din punct de vedere al managementului riscului le ajută să-și crească nivelul de performanță.

Definițiile referitoare la risc pe care le-am identificat pe parcursul cercetării bibliografice se concentrează pe gestiunea ameninţărilor, ca o combinație a probabilității unui eveniment și consecințele sale, iar tehnicile de răspuns ce sunt utilizate în general pentru tratarea acestor se bazează pe caracteristica negativa a riscurilor. Dintre aceste definiții amintim pe cea dată în „Dicționarul Explicativ al Limbii Române", respectiv, „posibilitatea de a ajunge într-o primejdie, de a avea de înfruntat un necaz sau de suportat o pagubă, pericol posibil"[14] și pe cea din „Dicționarul de Ergonomie", unde prin risc se poate înțelege și posibilitatea de a obține un câştig, respectiv, „o măsură a unei eventuale neconcordante între rezultatele posibile - favorabile sau nefavorabile - și cele preconizate într-o acțiune viitoare supusă influenței unor factori întâmplători". [15]

În era digitală atât entitățile publice cât și cele private utilizează sisteme informaționale pentru gestionarea informaților, iar **managementul riscului de securitate** reprezintă una din modalitățile principale de protejare a informaţiilor organizaţiilor și implicit a activității de bază a acestora, de riscurile de securitate corelate sistemelor informaționale.

„Pentru a asigura o oarecare uniformizare privind modalitatea de gestionare a riscurilor există o serie de standarde aplicabile la nivelul oricărei organizaţii, indiferent de domeniul de activitate sau tipul de risc, printre care amintim:

- SR ISO 31000:2010 – „Managementul riscului. Principii si linii directoare";
- SR EN 31010:2010 – „Managementul riscului. Tehnici de evaluare a riscurilor";
- SR GHID ISO 73:2010 – „Managementul riscului. Vocabular";
- SR BS 31100:2013 – „Managementul riscului. Cod de practica şi îndrumare pentru implementarea standardului SR ISO 31000" [16].

Pentru a detalia cât mai sugestiv care sunt funcțiunile managementului riscurilor de securitate a informațiilor, prezentăm în cele ce urmează sub formă grafică în figura 1.15 procesul de realizare activităților ce trebuie întreprinse pentru implementare:

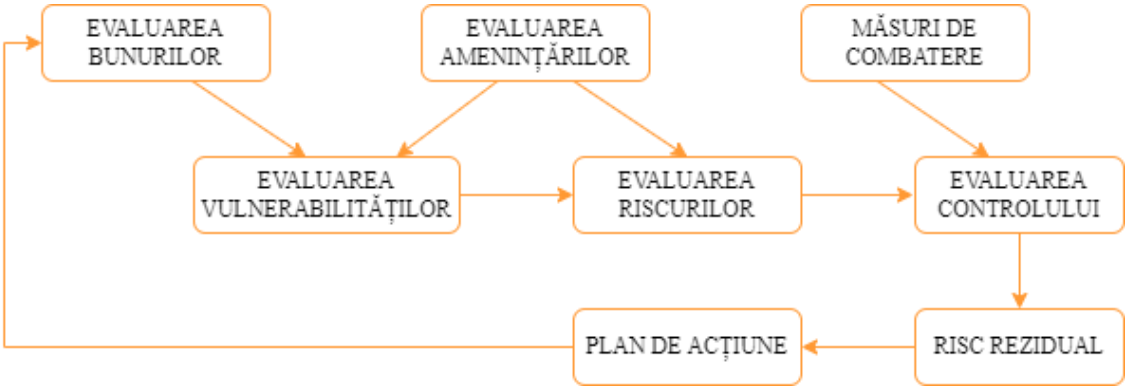

Fig. 1.15. Procesul de realizare a managementului riscurilor de securitate (propunere autor)

Între modelele consacrate de management al riscurilor, ce poate fi implementat atât în instituții de stat, în medii universitare cât și în entități private, deoarece conține modalități complete de evaluare a riscurilor de securitate din punct de vedere al metodologiei utilizate sau a ariei de aplicabilitate, am ales pentru studiu unul dintre cele mai consacrate și complete modele de management a riscurilor, respectiv cel descris în cadrul **Standardului NIST 800-37** al Departamentului de Comerț al SUA.[17]

În figura 1.16 de mai jos prezentăm legătura dintre evaluările de risc ce se bazează pe analiza amenințărilor și evaluările vulnerabilităților în interiorul unui model de sistem de management al riscurilor descris în Standardul NIST 800-37:

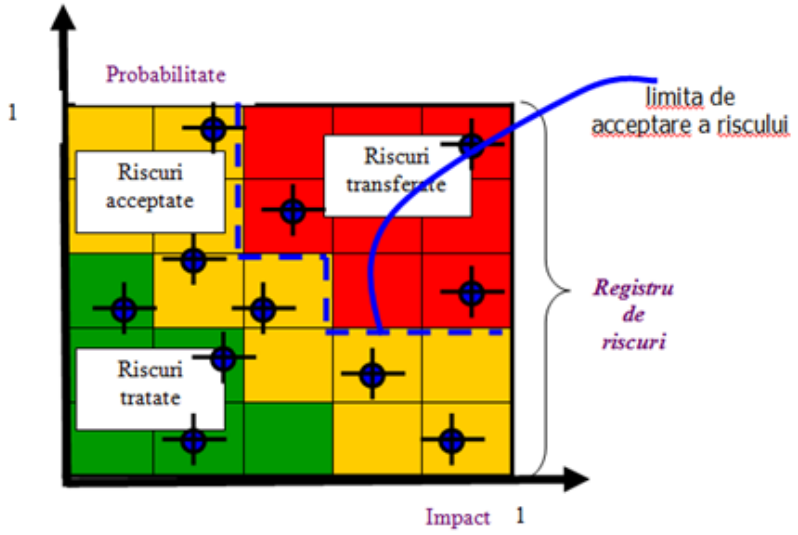

Fig. 1.16. Matricea riscurilor (sursa: Standardul NIST 800-37)

Se poate observa că o amenințare are semnificație practică doar dacă este o

În documentele standardului NIST 800-37 am identificat noțiuni cu privire la amenințare, risc și pericol ce se calculează pe o scară a gravității graduală, crescătoare, conform relației de calcul a riscului, prezentată în figura 1.17:

$$R = \frac{A \cdot V}{C} \cdot P \cdot I$$

unde: **R** reprezintă nivelul riscului de securitate; **A** amploarea amenințării; **V** gradul de vulnerabilitate; **C** eficiența măsurilor de contracarare; **P** probabilitatea de manifestare; **I** impactul produs.

Fig. 1.17. Relația de calcul a riscului (sursa: Standardul NIST 800-37)

1.6.4.Dimensiuni ale educației de securitate pentru reducerea erorilor umane legate de securitatea informațională

Asigurarea securității informațiilor este imposibilă în condițiile unei culturi de securitate generale precare sau a lipsei unei educații de securitate susținute și continue. Dacă, în cazul culturii de securitate, avem de-a face cu un cumul de precondiții și circumstanțe care țin de factorii sociali, culturali și istorici care se vor fi manifestat la nivelul național sau regional, educația de securitate trebuie să fie un obiectiv în permanentă atenție pentru toate organizațiile guvernamentale, de apărare și siguranță națională, dar și pentru celelalte tipuri de organizații de stat sau private.

Astfel, conducerile acestor organizații trebuie să asigure instruirea periodică a tuturor utilizatorilor cu privire la obligațiile pe care le au în ceea ce privește securitatea informațiilor, înainte de a le permite accesul la acestea.

Aceste instruiri trebuie să certifice faptul că angajații au înțeles și au deprinderi solide în aplicarea regulilor de securitate și că trebuie să solicite consultanță și ajutor la orice problemă care poate avea conotații legate de securitatea informațiilor pe care le exploatează.

În cadrul politicilor de securitate a informațiilor unei organizații este necesară prevederea unei secțiuni speciale dedicate educației de securitate, care să cuprindă cerințe complete și detaliate asupra programului de cunoaștere și protejare a securității informațiilor din cadrul organizației. Această secțiune trebuie să includă, printre altele:

- roluri și responsabilități;
- elemente programatice pentru dezvoltarea educației de securitate a informațiilor;
- măsuri de ducere la îndeplinire a programului de asigurare a educației de securitate a informațiilor;
- modalitatea de actualizare a acestui plan și de comensurare a efectelor acestuia.

Educația în domeniul securității informațiilor nu poate fi însă abordată doar la nivelul programelor de instruire și al responsabilităților personalului implicat în exploatarea resurselor informaționale ci și pe palierul mecanismelor și conceptelor psiho-sociale, aplicate asupra utilizatorilor acestora. Cel mai bun argument pentru această abordare este ingineria socială, foarte des utilizată de atacatori pentru a depăși barierele de securitate instalate de administratorii de sisteme informaționale. [18]

Astfel, formarea și educarea în domeniul securității informațiilor se transformă într-un obiectiv important, ce trebuie atins la nivelul oricărei entități și de orice angajat, indiferent de nivelul la care își desfășoară activitatea la un anumit moment al carierei lui.

1.7. ACTIVITĂȚI CE DUC LA ASIGURAREA REZILIENȚEI INFORMAȚIONALE

Rolul vital pe care îl joacă securitatea informațională în protejarea confidențialității informațiilor iese în evidență mai mult ca niciodată în aceste vremuri, căci din ce în ce mai mult infrastructurile critice trebuie să își gestioneze informațiile prin mediul on-line, ceea ce le face vulnerabile la atacuri digitale.

Reziliența informațională poate fi definită ca „abilitatea de a rezista în ciuda amenințărilor la adresa infrastructurii informaționale și a infrastructurii de comunicare”[19]. Analizând funcțiile critice și infrastructura putem observa dependența acestora de buna funcționare a sistemelor cibernetice, ale căror vulnerabilități au fost analizate și diminuate prin intermediul politicilor și procedurilor de securitate ale standardelor internaționale, iar pe baza riscurilor și amenințărilor inventariate în cadrul entităților se pot lua măsuri de îmbunătățire a rezilienței.

Îmbunătățirea rezilienței informaționale se realizează prin mecanismele de prevenire, detectare, atenuare și redresare[20], stabilite la nivel tehnic și decizional din cardul unei entități, așa cum am ilustrat în figura 1.18, astfel încât infrastructura informațională să fie capabilă să își mențină capacitatea de a funcționa pe timpul sau după ce este supusă unui atac:

Fig. 1.18. Reziliența informațională (propunere autor)

În contextul actual caracterizat de amenințări hibride la adresa securității informațiilor, este de interes să amintim că instituțiile publice trebuie să se concentreze pe latura umană a securității informațiilor prin implementarea de controale la nivel tehnic, aceasta activitate fiind definitorie pentru asigurarea securității. Acest aspect este deseori uitat de managementul instituțiilor, atitudine ce duce la lipsa de conștientizare a angajaților și la o slabă cultură generală în ceea ce privește securitatea informațiilor.

Din perspectivă teoretică, pentru a asigura securitatea informațiilor în mediul on-line, instituțiile publice trebuie să respecte politicile de securitate și procedurile operaționale pentru a putea fi reziliente. În cele ce urmează vom prezenta câteva aspecte importante ce trebuie urmărite de aceste entități, pentru a micșora riscurile ce pot afecta starea de securitate[21]:

a) Schimbul de informații de securitate

b) Asigurarea informațiilor;

c) Forța de muncă specializată în securitatea informațiilor;

d) Auto-apărarea securității informațiilor;

e) Lanțul de aprovizionare a securității informațiilor;

f) Securitatea informațională transfrontalieră;

g) Conștientizarea, educația și formarea;

Instituțiile publice trebuie să dispună măsuri care să vizeze proprii angajați, conștientizarea acestora cu privire la riscurile unui atac cibernetic îndreptat împotriva informațiilor pe care le gestionează și urmările negative ale acestora. În aceeași măsură, se dispun măsuri cu privire la educarea angajaților și formarea acestora în utilizarea calculatorului, îndeosebi pe Internet, astfel încât să nu fie expuși și vulnerabili.

Prevenirea are ca scop reducerea dependenței cibernetice și reducerea vulnerabilităților sistemelor informaționale. De remarcat că toate aceste activități ce se desfășoară cu scopul de a preveni, sunt programate și gândite în avans prin implementarea politicilor și procedurilor operaționale de securitate a informațiilor, pentru a se petrece înainte de a surveni un atac cibernetic

Politicile de securitate a informațiilor vor include și modalități de atenuare a atacurilor, activitate ce se referă la dezvoltarea unei capacități de rezistență împotriva atacurilor asupra informațiilor unei instituții publice.

Plus valoarea implementărilor de sisteme de management ale securității informațiilor la nivelul instituțiilor publice este generată de experiențele anterioare ale experților din alte entități similare și a celor ce au participat la gândirea acestor sisteme de management cu privire la protejarea sistemelor informaționale sau a celor metodologice prin intermediul cărora se gestionează sau stochează informațiile.

Prin implementarea unui sistem de management al securității informațiilor se pot elabora strategii și politici de securitate a informațiilor complete și adaptate nevoilor actuale, care pot cuprinde pe lângă norme metodologice și rolurile specifice fiecărui expert ce este implicat în implementarea sistemului, responsabilitățile și relațiile dintre toți experții ce au responsabilități în protejarea acestor sisteme.

CAPITOLUL 2
OBIECTIVELE TEZEI DE DOCTORAT

2.1. CONCLUZII PRELIMINARE ÎN URMA CERCETĂRII BIBLIOGRAFICE A TEMEI TEZEI DE DOCTORAT

În cadrul cercetării bibliografice efectuate în cadrul tezei de doctorat am aprofundat opiniilor autorilor de cărți și articole științifice cu aceeași temă și în acest scop am utilizat metode calitative ce au constat în analiza studiilor comparative și a studiilor de caz identificate în bibliografia studiată și metode cantitative ce au fost folosite pentru verificarea ipotezelor identificate în cadrul cercetărilor calitative.

Ipoteza principală de la care a pornit această cercetare, ca urmare a abordării critice a literaturii de specialitate în domeniu și a asimilării nivelului prezent al cercetărilor, dar și în baza cunoașterii practice a fenomenului securității informațiilor, este: **implementarea sistemelor de management al securității informaționale, împreună cu sistemele de management al riscului și celelalte măsuri tehnice de asigurare a securității pot contribui la eficientizarea răspunsului instituțiilor de stat la amenințările actuale în ceea ce privește securitatea informațiilor.**

Implementarea unui sistem de management al securității informațiilor în cadrul instituțiilor publice implică punerea în aplicare de politici de securitate necesare atingerii obiectivelor specifice domeniului securității informațiilor, ce trebuie să respecte normele standardelor internaționale în vigoare și cerințele legale aplicabile activității pe care o desfășoară. O componentă importantă a SMSI constă în formarea/educarea funcționarilor publici în ceea ce privește păstrarea unui climat de securitate prin respectarea măsurilor de securitate adoptate de managementul instituțiilor unde se implementează.

2.2. DELIMITAREA DOMENIULUI DE CERCETARE

În urmă cercetării bibliografice am tras concluzia că în cazul entităților de stat, pentru asigurarea unui răspuns adecvat la factorii de risc ce pot afecta starea de securitate a informațiilor nu este suficientă doar achiziția și instalarea de echipamente și/sau softuri de securitate informațională, ci trebuie adoptate politici, măsuri, reguli și proceduri operaționale de securitate și activități de formare și conștientizare a personalului/utilizatorilor cu privire la amenințările de securitate. Aceste unelte de securitate se pot implementa prin intermediul unui **Sistem de management a securității informaționale**, prin intermediul căruia se poate crea cadrul general și asigura premisele pentru menținerea stării de securitate a informațiilor.

Considerăm că este necesar ca un sistem de management al securității informațiilor, ce se implementează la nivelul unei instituții publice, să fie auditat de o entitate terță care să asigure managementul de faptul că este bine implementat și tratează o plajă cât mai mare de riscuri. Un astfel de audit trebuie făcut de o entitate acreditată de autoritățile de standardizare recunoscute la nivel internațional, pentru a avea expertiza necesară în certificarea calității sistemului de management ce a fost implementat.

Datorită complexității și sensibilității acestui domeniu și pentru asigurarea conformității sistemului de management, s-a constatat necesară asigurarea faptului că după implementare SMSI este viabil și bine croit pe nevoile de securitate ale entității, acest lucru fiind posibil prin certificarea sistemului de management în baza cerințelor și condițiilor unui standard internațional recunoscut la nivel internațional. În urma cercetării bibliografice am constatat că cel mai potrivit standard pentru certificarea unui SMSI implementat în instituții publice este SR/EN ISO/IEC 27001:2018.

2.3.OBIECTIVELE CERCETĂRII ȘTIINȚIFICE DIN CADRUL TEMEI TEZEI DE DOCTORAT

În urma cercetării bibliografice efectuate în cadrul tezei de doctorat, pornind de la ipoteza principală a cercetării, conturată pe impactul pozitiv pe care îl pot avea sistemele de management al securității informaționale asupra nivelului de securitate a informațiilor în cadrul instituțiilor publice, se profilează obiectivul principal al tezei de doctorat din care decurg obiectivele specifice corespunzătoare, pe care le prezentăm în cele ce urmează.

Obiectivul principal este identificarea celor mai bune metode și exemple de bune practici privind implementarea unui sistem de management a securității informațiilor și certificarea acestuia conform unui standard recunoscut la nivel internațional în cadrul instituțiilor publice.

Scopul acestui demers este creșterea gradului de securitate a informațiilor și micșorarea riscurilor în acest domeniu.

Pentru realizarea acestui obiectiv principal, propunem abordarea unor aspecte teoretice și practice, mai puțin dezvoltate și testate la nivelul entităților publice prin care să se trateze particularitățile implementării SMSI în acest tip de organizaţie, fapt ce prezintă o importanță majoră pentru domeniul cercetat.

Obiectivele specifice pe care le propunem în vederea atingerii obiectivului principal și a confirmării ipotezei sunt împărțite în:

1. Obiective teoretice ale tezei de doctorat:

- ❖ analiza teoretică și comparativ-critică a stadiului actual al cercetărilor cu privire la securitatea informațională;
- ❖ stabilirea rolului și importanței securității informațiilor în instituțiile publice;
- ❖ cercetarea metodelor, modalităților și sistemelor prin care se poate asigura securitatea informațiilor la nivelul instituțiilor publice;
- ❖ analiza teoretică sistemelor de management a securității informaționale și certificarea acestora conform standardului internațional SR EN ISO/IEC 27001:2018
- ❖ identificarea particularităților aplicabilității SMSI în contextul implementării în instituții de stat;

2. Obiective practice ale tezei de doctorat

- ❖ proiectarea unui model de implementare practică a SMSI și certificarea acestuia conform standardului internațional SR EN ISO/IEC 27001:2018 la nivelul Autorității Electorale Permanente din România;
- ❖ propunerea unui set de măsuri ce pot face parte din Politica de securitate ce se va adopta în cadrul SMSI al AEP;
- ❖ stabilirea procedurilor, documentelor și politicilor ce vor trebui adoptate de AEP în cadrul SMSI;
- ❖ identificarea riscurilor de securitate a informațiilor de la nivelul AEP în vederea tratării acestora;
- ❖ propunerea planului de acțiune pentru implementarea SMSI la nivelul AEP ce va conține fazele acestuia, termenele de implementare, responsabilii și livrabilele.

În cadrul modelului de analiză pe care îl vom prezenta detaliat în capitolul ce va conține contribuțiile practice privind implementarea SMSI, vom prezenta o serie de obiective de securitate tangibile, documente și proceduri operaționale de securitate, care vor avea rolul de a trata sau acoperi într-o măsură cât mai mare riscurile de securitate informațională la care este expusă instituția, în vederea îndeplinirii atribuțiilor specifice și creșterii prestigiului AEP la toate nivelurile de reprezentare.

CAPITOLUL 3

CERCETĂRI ȘI CONTRIBUȚII TEORETICE PRIVIND IMPLEMENTAREA SISTEMELOR DE MANAGEMENT A SECURITĂȚII INFORMAȚIILOR CONFORM ISO/IEC 27001:2018 LA NIVELUL INSTITUȚIILOR PUBLICE

Era informațională are același efect asupra umanității ca și descoperirea materialelor de bază, atât de utile oamenilor precum petrolul, focul și fierul. Acest efect crește exponențial odată cu dezvoltarea tehnologiei și cu posibilitatea accesului facil la informații pe căi multiple. În acest mediu dinamic, dezvoltarea activităților de securizare a informațiilor, în vederea păstrării acestora în bune condiții și cu cât mai puține riscuri, necesită existența unui sistem informațional funcțional, ținut la zi din punct de vedere tehnologic și protejat împotriva amenințărilor de securitate.

Atunci când analizăm **echilibrul cost/beneficiu** din punct de vedere reputațional sau social în cazul instituțiilor publice, putem spune că investițiile în o mai bună securitate a echipamentelor și rețelelor pentru protejarea informațiilor generează costuri mari, pe care de cele mai multe ori instituțiile nu și le permit, iar beneficiile sociale care nu se reflectă în mod direct și adecvat în imaginea generală a acestora în fața publicului larg.

Prin urmare, se constată nevoia ca la nivelul instituțiilor publice, pe lângă implementarea de soluții operaționale de securitate a informațiilor, să se adopte și alte tipuri de măsuri de securitate, prin intermediul sistemelor de management al securității informațiilor.

Implementarea unui sistem de management al securității informației (SMSI) bine structurat, conceput în conformitate cu standardele internaționale, poate sta la baza unei strategii adecvate de securitate, în special în aceste vremuri în care amenințările și securitatea informațiilor în general, sunt probleme predominante de care se lovește orice tip de entitate publică sau privată.

Un aspect important al securității informațiilor este stabilirea politicii de securitate, care este documentul care specifică măsurile de securitate a informațiilor și care trebuie să facă obiectul unor revizuiri și evaluări la anumite termene clare.

Pentru a putea avea certitudinea faptului că SMSI a fost bine implementat și conferă premisele asigurării securității informațiilor, acesta trebuie verificat, auditat și certificat conform unui standard recunoscut la nivel mondial în acest domeniu, ce stabilește cadrul general prin care se asigură garanția că SMSI respectă cele mai înalte standarde de calitate. Astfel în cadrul cercetării am analizat „**ISO - International Organization for Standardization**” sau „Organizația Internațională de Standardizare, este o organizație internațională independentă, neguvernamentală, a cărei membri fac parte din 167 de organisme naționale de standardizare, ce are ca scop dezvoltarea de standarde internaționale ce pot fi adoptate voluntar, bazate pe consens, relevante pentru piață, care sprijină inovația și oferă soluții la provocările globale”.[22]

În sensul lucrării de față, am identificat ca fiind relevantă pentru cercetare implementarea „**Standardului SR EN ISO/IEC 27001:2018 – Tehnologia informației, Tehnici de securitate, Sisteme de management al securității informației, Cerințe**”[23], ce face parte din seria de standarde 27000 și a fost aprobat în ianuarie 2018 de Asociația de Standardizare din România, fiind identic cu versiunea europeană a standardului. Această serie de standarde este compusă din „ISO/IEC 27001 Cerințele SMSI; ISO/IEC 27002 Catalogul măsurilor de control; ISO/IEC 2700x Standarde de implementare; ISO/IEC 2701x Standarde sectoriale;

ISO/IEC 2703x Standarde de control”[24], iar în figura 3.1 prezentăm lista acestora și relațiile dintre ele, așa cum le prezintă Organizația Internațională de Standardizare:

Standardul ISO 27001:2018 folosește ca fundament principiile clasice ale securității informațiilor, respectiv confidențialitatea, integritatea și disponibilitatea informațiilor, care definesc în general starea de securitate informațională. Implementarea acestui standard asigură premisele unei securități a informațiilor pe termen lung, bazată pe implementarea politicilor, procedurilor și metodelor de securitate concepute pentru a proteja informațiile și resursele instituțiilor. Minimizând riscurile, se asigură faptul că sistemul de management este bine implementat la nivelul instituției, răspunde tuturor nevoilor beneficiarilor de servicii ale acesteia și respectă legislația în vigoare.

Organizațiile de stat pot învăța să răspundă riscurilor de securitate prin implementarea și menţinerea un sistem de management al securității informației, căci astfel vor adopta măsurile de securitate prevăzute în cadrul standardului ISO 27001:2018, ce conțin planuri de tratare a acestor riscuri. Aceste planuri ce se creează la nivelul entității ajută managementul instituției să aleagă tipurile de controale corespunzătoare contextului în care instituția își desfășoară activitatea.

„Standardul ISO 27001:2018 are în prezent exemplificate un număr de 114 măsuri de control și obiective de securitate care sunt repartizate în 14 grupe”[25], pe care le detaliem așa cum sunt ele prezentate în cadrul standardului, în tabelul 3.1:

Tabelul 3.1. Grupele măsurilor de control din standardul 27001:2018 (sursa: https://www.itgovernance.co.uk/)

Codificarea grupelor	**Denumirea grupelor**	**Numărul măsurilor de control**
A.5	Politici de securitate a informației	2
A.6	Organizarea securității informației	7
A.7	Securitatea resurselor umane aplicabilă oricând înainte, în timpul sau după angajare	6
A.8	Managementul resurselor	10
A.9	Controlul accesului	14
A.10	Criptografie	2
A.11	Securitatea fizică și cea a mediului	15
A.12	Operațiuni de securitate	14
A.13	Securitatea comunicațiilor	7
A.14	Achiziții de sistem, dezvoltare și întreținere	13
A.15	Relațiile cu furnizorii	5
A.16	Managementul incidentelor de securitate a informației	7
A.17	Aspectele privind securitatea informațiilor în managementul continuității afacerii	4
A.18	Conformitatea cu cerințele interne - politicile și cu cerințele externe - legile	8

ISO 27001:2018 impune unei instituții publice folosirea strategiei de management ce utilizează abordarea orientată spre procese. Când se folosește această abordare, înseamnă că managementul controlează procesele, interacțiunile dintre aceste procese și rezultatele care reies din acestea.

Standardul sugerează structurarea fiecărui proces din cadrul SMSI prin folosirea modelului Planifica-Executa-Verifica-Acționează (PDCA), a cărei reprezentare grafică o regăsim în figura 3.3, iar fiecare proces din cadrul modelului reprezintă:

- „planificarea obiectivelor împreună cu obiectivele specifice de securitate a informațiilor;
- Transpunerea planului în practică, administrat și menținut;
- verificarea, măsurarea, auditarea și evaluarea bazate pe măsurarea eficienței proceselor prin intermediul indicatorilor de performanță;
- acționarea pentru implementarea celor mai adecvate soluții de îmbunătățire a eficienței proceselor"[26].

Fig.3.3. Modelul PDCA (sursa: Ministerul Dezvoltării, Lucrărilor Publice și Administrației)

Analiza riscurilor este o activitate de sprijin a securității informațiilor, iar importanța acestui proces derivă chiar din definiția ISO 27001:2018, respectiv identificarea incidentelor care pot apărea în activitățile instituționale și a celor mai utile moduri de abordare a acestora.

Certificarea SMSI în conformitate cu cerințele ISO 27001:2018 se poate aplica în egală măsură oricărei instituții publice care are printre obiectivele generale crearea unei imagini pozitive pentru publicul larg prin păstrarea unei stări de securitate a informațiilor. Acest deziderat se pot duce la îndeplinire prin:

- comunicarea publică a politicii de securitate a informațiilor;
- instruirea personalului în domeniul protejării securității informațiilor;
- creșterea încrederii tuturor entităților de stat sau private, prin dovezi certificate ce arată capacitatea de protejare a informațiile, cu privire la confidențialitatea, integritatea și disponibilitatea acestora.

Implementarea unui SMSI la nivelul unei entități publice va ajuta atât conducerea cât și angajații acesteia la asigurarea premiselor și mijloacelor prin care aceasta să fie percepută ca o instituție publică digitalizată, ce utilizează tehnologii inovative, cu o bună reputație pe plan european și internațional, demnă de încredere în fața cetățenilor a căror interese le reprezintă, pentru că astfel demonstrează furnizarea de servicii de calitate și prin care asigură îndeplinirea misiunii instituției.

Printre scopurile de bază pe care instituțiile publice le pot urmări prin certificarea ISO 27001:2018 enumerăm măsuri de protejare a datelor personale ale angajaților sau ale instituțiilor cu care fac schimb de date sau informații, precum și a cetățenilor care beneficiază de serviciile oferite de acestea, gestionarea riscurilor de securitate a informațiilor, respectarea reglementărilor europene în domeniul protecției datelor cu caracter personal și îmbunătățirea imaginii organizației în public.

CAPITOLUL 4
CERCETĂRI ȘI CONTRIBUȚII PRACTICE PRIVIND IMPLEMENTAREA UNUI SISTEM DE MANAGEMENT AL SECURITĂȚII INFORMAȚIILOR ȘI CERTIFICAREA ACESTUIA CONFORM SR/EN ISO 27001:2018 LA NIVELUL AUTORITĂȚII ELECTORALE PERMANENTE

4.1. PREZENTAREA AUTORITĂȚII ELECTORALE PERMANENTE ȘI A CATEGORIILOR DE INFORMAȚII PE CARE LE GESTIONEAZĂ

Pentru a prezenta cât mai în detaliu cum se poate implementa un model de sistem de management al securității informaționale în cadrul unei instituții publice, am considerat necesară prezentarea unui model practic, un studiu de caz prin care să se transpună latura teoretică, destul de abstractă în ceea ce privește activitățile ce trebuie derulate, în zona practică, adică crearea unui model practic de implementare a SMSI, similar consultanței inițiale unui astfel de demers și apoi pașii de urmat pentru certificarea acestuia conform standardului ISO 27001:2018.

În scopul realizării acestui demers, am ales pentru analiză practică și studiu de caz o instituție publică reprezentativă a statului român, respectiv Autoritatea Electorală Permanentă. Am făcut această alegere deoarece instituția reprezintă garantul respectării principiilor de bază ale democrației din România, ceea ce implică un grad mare securitate a informațiilor pe care acesta le gestionează.

Pe parcursul **cercetării bibliografice** realizate în cadrul lucrării de doctorat am constatat că pentru asigurarea securității informațiilor unei astfel de instituții importante este nevoie de un grad ridicat de sofisticare a rezultatelor cercetărilor practice. Această alegere a implicat nevoia cunoașterii aprofundate a mecanismelor operaționale, juridice și tehnice ale instituției, cunoașterea categoriilor de informații, a echipamentelor prin care se procesează sau stochează acestea și a modalităților și fluxurilor prin care acestea circulă în interiorul și în afara acesteia.

„**Autoritatea Electorală Permanentă** este o instituție administrativă autonomă cu personalitate juridică și cu competență generală în materie electorală, care are misiunea de a asigura organizarea și desfășurarea alegerilor și a referendumurilor, precum și finanţarea partidelor politice şi a campaniilor electorale, cu respectarea **Constituţiei**, a legii şi a standardelor internaţionale și europene în materie.”[27].

Astfel, **obiectivele în ceea ce privește digitalizarea și debirocratizarea Autorității Electorale Permanente** se pot atinge prin intermediul departamentului de resort IT&C, ce deține toate pârghiile pentru transferul cât mai multor informații gestionate de instituție către mediul on-line, fapt ce ar conduce la tranziția către e-guvernare, interoperabilitatea facilă și în timp real, pentru schimbul de informații cu alte sisteme informaționale ale entităților administrației publice.

Pentru atingerea acestor obiective, la nivelul instituției funcționează o suită de sisteme și aplicații informatice ce sunt utilizate ce suport operațional pentru toate procesele și informațiile pe care structurile din cadrul instituției le au ca și atribuții legale.

Infrastructura internă IT&C a Autorității Electorale Permanente susține pe de o parte desfășurarea activităților zilnice ale tuturor angajaților, respectiv, infrastructura de rețea, echipamentele necesare pentru lucrul de birou, accesul la Internet, intranet, schimb de fișiere și lucru în comun, comunicare internă și externă pe email și pe de altă parte toate aplicațiile informatice dezvoltate cu resurse proprii sau achiziționate de pe piață, necesare instituției pentru desfășurarea activităților operaționale.

Infrastructura hardware ce susține sistemul informațional al Autorității Electorale Permanente, funcționează într-un centru de date aflat în sediul central al instituției, ce conține și echipamente cu rol de back-up și recuperare de date în caz de dezastru, ce este situat într-un spațiu securizat din cadrul clădirii. Schema logică a arhitecturii sistemului o prezentăm sub formă grafică în figura 4.1:

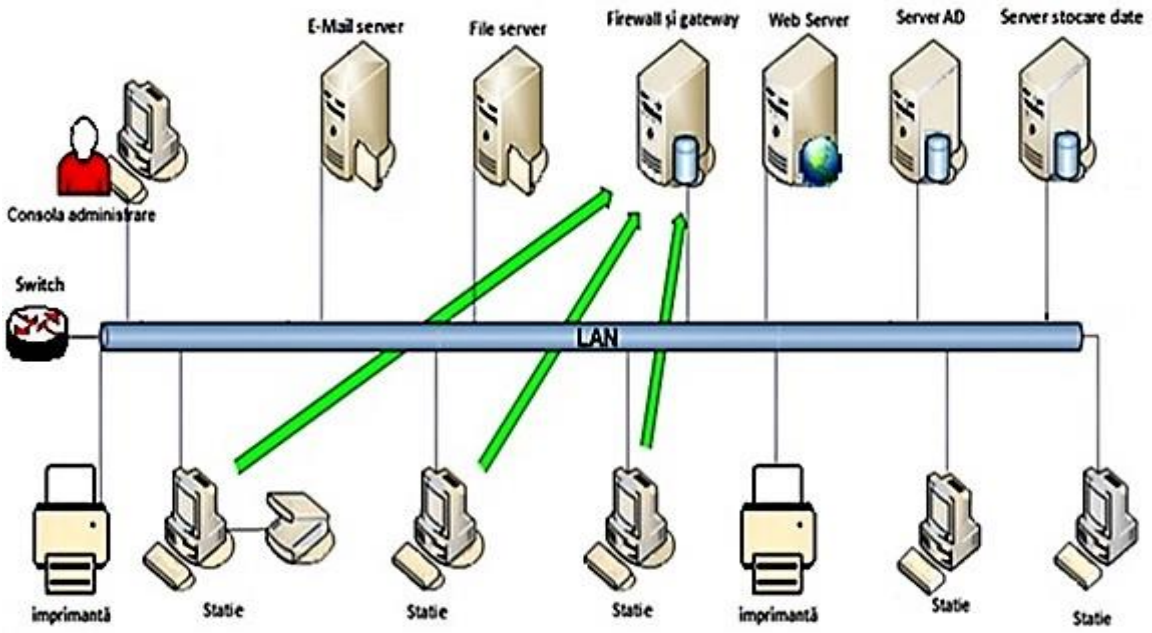

Fig. 4.1. Arhitectura rețelei de comunicații din sediul central al AEP (sursa: documentația tehnică a rețelei interne AEP)

O componentă foarte importantă din sistemul informațional al instituției este „**Sistemul Informatic Registrul Electoral (SIRE)**”, fiind reprezentat de un portal informatic complex ce a fost creat în scopul asigurării unei evidențe corecte și transparente a alegătorilor români și arondarea acestora pe secții de votare în România și din străinătate.

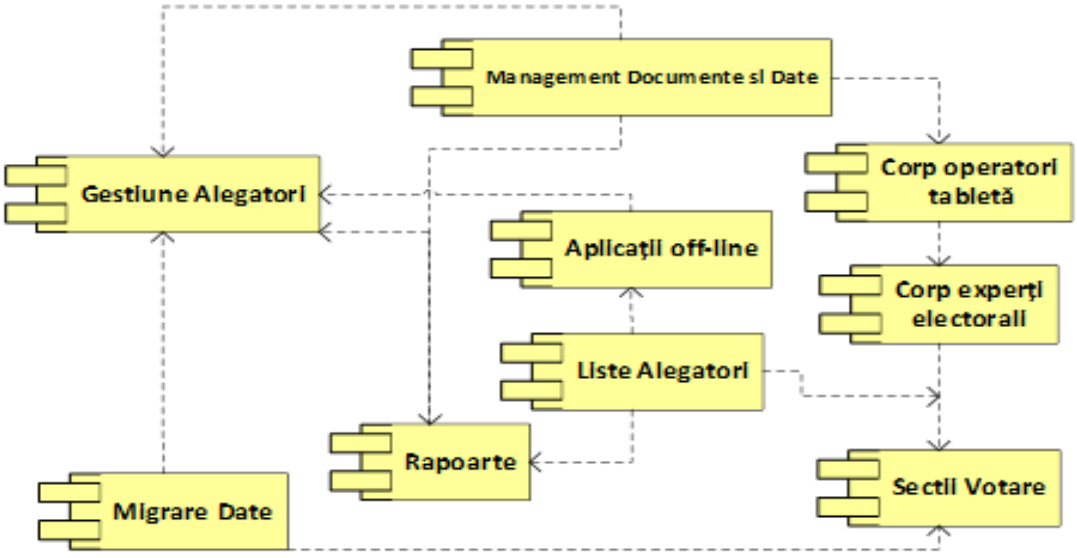

Fig.4.2. Arhitectura logică a SIRE (sursa: documentația tehnică SIRE)

4.2.CONTRIBUȚII PRACTICE PRIVIND IMPLEMENTAREA UNUI SISTEM DE MANAGEMENT A SECURITĂȚII INFORMAȚIONALE LA NIVELUL AUTORITĂȚII ELECTORALE PERMANENTE

Din analiza rezultatelor cercetării științifice au rezultat o serie de riscuri de securitate a informațiilor gestionate la nivelul Autorității Electorale Permanente ce pot reprezenta provocări reputaționale majore pentru conducerea instituției în contextul geo-politic actual, iar metodei practice pe care am propus-o în cadrul lucrării pentru menținerea unui climat de securitate informațională este crearea, implementarea și îmbunătățirea în mod continuu a unui sistem de management a securității informațiilor și certificarea acestuia conform regulilor „Standardului SR EN ISO/IEC 27001:2018 privind tehnologia informației – tehnici de securitate – sisteme de management al securității informației".

Vom prezenta explicit și detaliat în cadrul analizei beneficiile implementării unui SMSI personalizat în mod individual pentru nevoile AEP, care să fie conforme cu cerințele impuse de standardul ISO 27001:2018, în vederea certificării de către un organism de certificare acreditat.

Pentru a parcurge etapele ce sunt necesare la nivelul AEP în vederea implementării SMSI, este necesară parcurgerea următorilor pași:

- ❖ planificarea, pregătirea elementelor ce vor intra sub incidența SMSI;
- ❖ derularea activităților de implementare a SMSI la nivelul instituției;
- ❖ certificarea SMSI ce a fost implementat la nivelul AEP conform standardului ISO 27001:2018;
- ❖ menținerea prin respectarea măsurilor de securitate adoptate prin SMSI și auditarea internă sau externă periodică a acestuia.

În paralel cu implementarea SMSI și certificarea acestuia conform standardului ISO 27001:2018, pot fi utilizate sau implementate și alte standarde interne sau internaționale și sisteme de management, care au principii sau domeniu de aplicare asemănător și care se adresează îmbunătățirii sau menținerii stării de securitate informațională.

4.2.1. Componentele și etapele implementării SMSI la nivelul Autorității Electorale Permanente în vederea certificării ISO/IEC 27001

În vederea implementării SMSI, la nivelul AEP trebuie să se adopte măsuri tehnice și organizatorice care mai sunt cunoscute în acest domeniu și sub denumirea prescurtată de „MTO", în vederea realizării și menținerii unui climat de securitate a informațiilor pentru atingerea nivelului necesar de protecție ce este solicitat pentru certificarea sistemului în conformitate cu standardul ISO 27001:2018.

La nivelul AEP, pentru îndeplinirea acestui obiectiv major, trebuie efectuată o analiză aprofundată a legislației românești și comunitare ce guvernează activitatea AEP, a uzanțelor în domeniu și a documentelor oficiale disponibile în mediul public cu privire la standardul ISO 27001:2018, și a atribuțiilor Departamentului Informatizarea Proceselor Electorale din cadrul instituției ce are ca sarcina asigurării securității informaționale a Autorității.

Primul pas procedural al acestui proces este realizarea unui **audit al sistemului IT&C** ce se află în proprietatea sau administrarea instituției, ce va avea rolul de a constata stadiul actual al securității informaționale la nivelul AEP și de a identifica demersurile ce trebuie întreprinse la nivelul echipamentelor și a software-ului, raportat la cerințele standardului, în vederea atingerii obiectivelor specifice ale structurii și implicit ale instituției.

4.2.2.Determinarea domeniului de aplicare al sistemului de management al securității informațiilor în cadrul Autorității Electorale Permanente

În timpul implementării SMSI, una dintre primele sarcini este determinarea exactă a **domeniului de aplicare a sistemului de management** și analiza cerințelor și a situației instituției și a părților interesate de acest proces.

În conformitate cu standardul, domeniul de aplicare trebuie foarte bine documentat și pe lângă procesele și diviziunile acoperite de SMSI, trebuie să cuprindă și o analiză a cerințelor

funcționale ale sistemului de securitate a informațiilor, ce trebuie făcută în funcție de situația în care se află instituția la data efectuării acesteia.

La nivelul Autorității Electorale Permanente, în urma studierii organigramei și a actelor normative ce statuează organizarea instituției și obligațiile legale ale acesteia, propunerea privind domeniul de aplicare a SMSI ar putea fi **Departamentul de Informatizare a Proceselor Electorale (DIPE)**, care este structura ce poate implementa, urmări și îmbunătăți permanent SMSI al instituției, așa cum reiese din atribuțiile conferite prin Regulamentul de Organizare și Funcționare al AEP, aprobat prin Hotărârea nr. 4/2020 a Birourilor Permanente ale Camerei Deputaților și Senatului[28], prin care i-au fost atribuite responsabilități în domeniul managementului, administrării și securității informaționale a componentelor IT&C din proprietatea instituției.

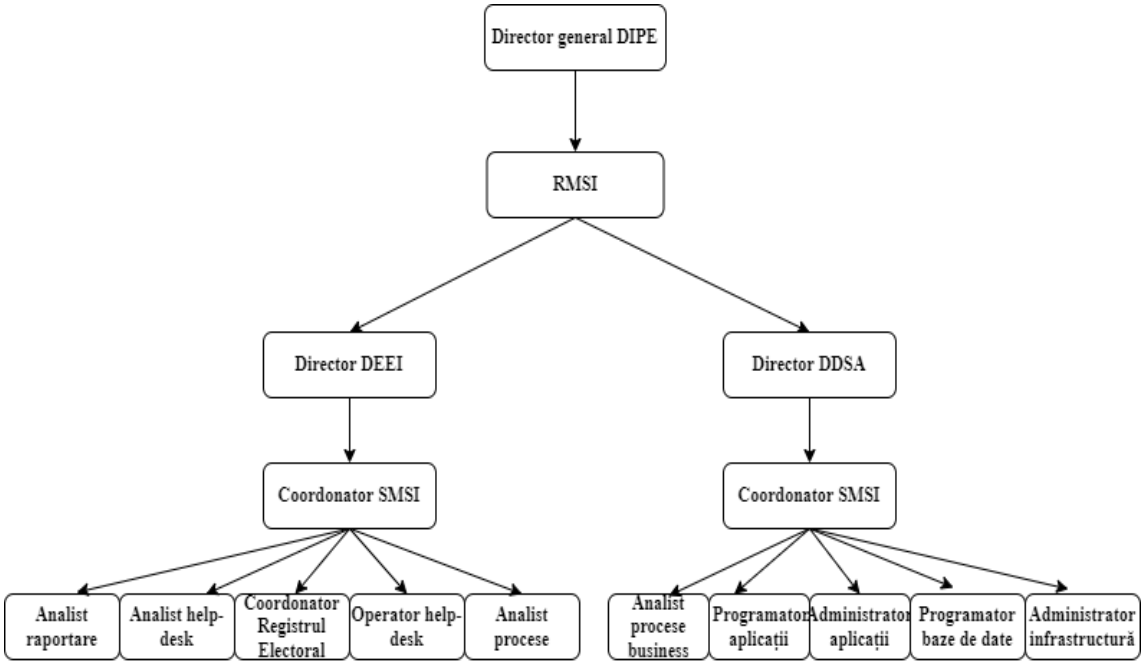

Fig. 4.8. Organigrama DIPE restructurată în funcție de nevoile SMSI (propunere autor)

După creare, documentul privind domeniul de aplicare la nivelul AEP, va fi pus la dispoziția conducerii și managementului tuturor departamentelor spre analiză și verificare, acesta fiind singura modalitate prin care toate părțile interesate pot verifica dacă domeniul de aplicare SMSI acoperă toate procesele, infrastructura, subiectele sau cerințele relevante pentru întreaga instituție.

Un alt document important ce face parte din sistemul de management este Declarația de aplicabilitate, document obligatoriu prevăzut de standardul ISO 27001:2018. Declarația detaliază și explică deciziile de punere în aplicare a controalelor - adică se verifică dacă fiecare control propus la nivelul instituției este util și dacă va fi utilizat sau nu în cadrul SMSI, inclusiv justificarea corespunzătoare a fiecărei verificări.

4.2.3.Analiza situației actuale și a cerințelor operaționale la nivelul Autorității Electorale Permanente

Scopul unei analize a situației existente la nivelul AEP este de a plasa SMSI în mediul general în care autoritatea își desfășoară activitatea, pe baza domeniului de aplicare definit în pașii anteriori de implementare și aprobat de conducerea instituției. După stabilirea relațiilor organizaționale interne și externe, în cadrul analizei trebuie stabilite relațiile tehnice dintre aplicațiile informaționale gestionate de AEP, ce sunt relevante pentru implementarea SMSI.

Analiza va trebui să includă, de asemenea, și condițiile specifice tipice pentru domeniul de activitate al AEP, având în vedere importanța sistemelor informaționale pe care instituția le

gestionează, ce este justificată de utilizarea acestora în cadrul tuturor proceselor electorale din România și Europa.

De asemenea, pentru o bună fundamentare a componentelor SMSI se va analiza cu atenție contextul extern în care își desfășoară activitatea AEP, cum ar fi tipul și profilul furnizorilor și prestatorilor de servicii importanți, care sunt partenerii strategici ai instituției și orice alte organizații relevante cu care există relații de colaborare.

Persoanele ce vor fi responsabile cu implementarea SMSI vor trebui să aibă o imagine foarte clară asupra securității informaționale și a implicațiilor pe care aceasta le are în legătură cu activitățile de bază ale instituției, precum și a celor incidente tuturor părților interesate.

4.2.4. Management, roluri și responsabilități în ceea ce privește SMSI la nivelul Autorității Electorale Permanente

Un sistem de management al securității informațiilor de succes trebuie implementat pe verticală după modelul „de sus în jos", cu implicarea și sprijinul managementului superior, care este factorul-cheie pentru succesul procesului de implementare al sistemului de management și certificarea acestuia conform standardului ISO 27001:2018.[29].

Rolul cel mai important din prisma implementării SMSI îl are chiar managementul superior al Autorității Electorale Permanente, ce trebuie să se implice activ în ceea ce privește luarea deciziei de implementare a sistemului și ulterior să susțină și să aprobe toate demersurile, documentele și activitățile ce se creează pe tot parcursul implementării și certificării conform normelor ISO.

În cazul în care conducerea AEP va accepta propunerea privind stabilirea domeniului de aplicare a SMSI la nivelul Departamentul de Informatizare a Proceselor Electorale, atunci managementul întregului proces de implementare va trebui să fie asigurat acest departament.

În acest context, conducerea DIPE împreună cu managementul superior al AEP vor trebui să atribuie responsabilitatea și autoritatea de management către un responsabil cu sistemul de management al securității informațiilor. Acesta va reprezenta rolul cel mai important în cadrul procesului de implementare a sistemului, deoarece poartă responsabilitatea implementării cu succes a sistemului de management a securității informațiilor la nivelul instituției.

Ținând cont de structura organizatorică instituțională existentă în prezent în cadrul AEP, în vederea implementării SMSI propunem ca instrument de management al proiectului implementarea unei **matrice de tip RASCI**, ce va avea ca scop realizarea cu succes a identificării corecte și complete a tuturor responsabilităților și respectarea acestora la nivelul întregului personal. Acest concept mai este cunoscut și sub numele de matrice de alocare a responsabilităților.

Responsabilitatea pentru susținerea și respectarea politicilor de securitate va aparține întregii instituții, sub îndrumarea și asistența personalului de conducere, care încurajează angajamentul întregului personal de abordare a SMSI ca parte a competențelor profesionale.

Standardul ISO 27001:2018 stabilește responsabilitățile pe care trebuie să și le asume oricare dintre membrii echipei de implementare, pentru a asigura respectarea condițiilor prevăzute în cadrul acestuia, care includ:

- stabilirea unor obiective de politica de securitate care trebuie sa fie compatibile cu politicile strategice si obiectivele generale ale instituției;
- respectarea condițiilor general valabile și a obiectivelor specifice privind implementarea SMSI.
- respectarea măsurilor de securitate a informațiilor în activitatea de zi cu zi a instituției;
- asigurarea resurselor pentru implementarea SMSI;

- ❖ definirea responsabilităților în fișa postului pentru funcționarii publici care vor pune în aplicare măsuri de securitate pentru a-și îndeplini îndatoririle.

4.2.5.Politicile de securitate a informației ce trebuie adoptate la nivelul Autorității Electorale Permanente

O politica de securitate a informației reprezintă asigurarea managementului în privința analizei și tratării problemelor de securitate ale informației la nivelul instituției. Aceasta oferă direcții și suport operațional la problemele de securitate informațională conform regulamentelor instituției, legile și normativelor tehnice în vigoare.

La nivelul AEP, în cadrul activităților SMSI se va elabora un document de politică de securitate a informației, prin care se va asigura informarea angajaților și a entităților externe interesate, cu privire la obligația de a respecta cerințele de securitate a informației și se va declara angajamentul instituției de îmbunătățire continuă a SMSI.

Politica va include principiile și obiectivele generale în ceea ce privește securitatea informațiilor, în scopul implementării cu succes al SMSI și se va aplica tuturor activităților AEP ce au legătură cu informația, sistemele informatice, rețeaua și infrastructura fizică.

Politica de securitate a informațiilor trebuie să conțină măsuri cu privire la managementul resurselor IT&C deținute de AEP. Protecția activelor trebuie obținută și menținută și din acest motiv trebuie să existe un registru al tuturor activelor prin care se gestionează informații din proprietatea instituției.

Echipamentele și programele de calculator aflate în proprietatea AEP și în utilizarea angajaților instituției, ce vor intra sub incidența politicilor de securitate adoptate în cadrul SMSI vor fi înregistrate într-un registru special, ce va face parte din înregistrările sistemului și va conține toate datele despre origine, achiziție, locul principal de utilizare și starea acestora la predarea către utilizator, sau la orice schimbare survenită asupra oricăruia dintre datele menționate anterior sau a stării de securitate constatată în cadrul controalelor asupra sistemului.

4.2.6.Gestionarea și managementul riscurilor în cadrul SMSI la nivelul Autorității Electorale Permanente

Managementul riscului este activitatea prin care se analizează tot ceea ce s-ar putea întâmpla negativ în cadrul SMSI al AEP, precum și impactul potențial al acestor evenimente din toate punctele de vedere pentru prevenirea eventualelor prejudicii materiale, financiare sau reputaţionale. Scopul principal al managementului riscurilor în cadrul instituției este de a reduce riscurile identificate de fiecare departament la un nivel acceptabil. Definirea nivelului de acceptabilitate a riscurilor va trebui decis și definit de către persoanele ce au primit această responsabilitate din partea conducerii instituției.

În cadrul cercetării bibliografice pentru teza de doctorat am identificat mai multe particularități ale modului în care trebuie abordate riscurile ce au fost identificate și evaluate în cadrul SMSI la nivelul unei instituții publice. Una din cele mai importante particularități față de mediul privat este obligativitatea instituțiilor publice de a-și organiza activitatea de management al riscurilor conform standardelor și regulilor impuse de „Ordinul Secretarului General al Guvernului nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităților publice”, ce reprezintă legislația primară incidentă acestui domeniu.

Pentru o implementare corectă am identificat nevoia unor evaluări ciclice și obiective, menite să contribuie la identificarea sistematică, evaluarea și prezentarea transparentă a riscurilor în contextul securității informațiilor și să asigure o îmbunătățire acceptabilă și pe termen lung a nivelului de securitate în cadrul domeniului de aplicare ce va fi stabilit și adoptat la nivelul instituției.

Pentru asigurarea implementării managementului riscurilor la nivelul Autorității Electorale Permanente, a fost înființată „**Comisia de monitorizare (CM) a Sistemului de Control Intern Managerial (SCIM)**”, prin Ordin al Președintelui instituției, ce are printre atribuții obligația implementării, modificării și asigurării funcționării managementului

riscurilor, respectiv, identificarea, evaluarea, analiza și monitorizarea riscurilor identificate la nivelul instituției.

Toate activitățile de management al riscurilor în cadrul AEP se desfășoară în conformitate cu procedura de sistem „PS.08 - Procedura privind managementul riscului”, ce descrie procesul specific prin care se implementează la nivelul instituției „Standardul 8 – Managementul Riscului din Codul controlului intern managerial al entităților publice, aprobat prin Ordinul SGG nr. 600/2018”.

În concluzie, putem spune că pentru implementarea Sistemului de management al securității informațiilor la nivelul DIPE, întreg aparatul Autorității Electorale Permanente va trebui să reanalizeze în profunzime principiile ce stau la baza activităților de evaluare a riscurilor de securitate a informațiilor, definind totodată noi riscuri specifice acestui domeniu și criterii pentru procedurile de acceptare și evaluare ale acestora în conformitate cu documentele și cerințele ce stau la baza sistemului, așa cum sunt ele prezentate în cadrul standardului ISO 27001:2018.

4.2.7.Proceduri, documente și politici propuse spre adoptare în cadrul SMSI la nivelul Autorității Electorale Permanente

La nivelul Autorității Electorale Permanente, trebuie create și implementate politici și proceduri de securitate informațională, detaliate pentru fiecare control care va fi definit la nivelul SMSI, acestea fiind cerințe exprese ale standardului ISO 27001:2018.

Procedurile și politicile de securitate a informațiilor, ce se vor crea în cadrul SMSI la nivelul AEP se vor transmite tuturor angajaților ce vor avea atribuții în legătură cu activitățile pentru care acestea au fost create, spre a fi luate la cunoștință și folosite, astfel încât fiecare să își cunoască responsabilitățile subsumate domeniului și managementul să se poată controla în cele mai bune condiții activitățile individuale.

Pentru a identifica ce proceduri trebuie documentate la nivelul instituției, se va consulta „Declarația de aplicabilitate” - SOA, document ce detaliază și explică deciziile de punere în aplicare a controalelor, prin intermediul căruia se verifică dacă fiecare control propus la nivelul instituției este util și dacă va fi utilizat sau nu în cadrul SMSI, inclusiv justificarea corespunzătoare a fiecărei verificări.

Mai jos prezentăm propunerea unei liste a documentelor, politicilor și procedurilor pe care o facem conducerii AEP ce trebuie adoptate la nivelul instituției în contextul protejării securității informațiilor, ce au fost analizate și vor trebui create în conformitate cu clauzele pe care le-am identificat în Anexa A la standardul ISO 27001:2018, pe care le considerăm utile a fi create și adoptate în cadrul SMSI la nivelul AEP:

- **„Declarație de politica privind securitatea informaţiilor”;**
- **„Domeniul de aplicare al SMSI”;**
- **„PO-SMSI-Organizarea securității informației”;**
- **„PO-SMSI-Informația disponibilă în mod public”;**
- **„PO-SMSI-Manipularea mediilor de stocare”;**
- **„PO-SMSI-Conștientizare și instruire”;**
- **„PO-SMSI-Managementul resurselor informaționale”;**
- **„PO-SMSI-Clasificarea și etichetarea informației SMSI”;**
- **„PO-SMSI-Controlul accesului”;**
- **„PO-SMSI-Securitatea fizică”;**
- **„PO-SMSI-Inventarul activelor”;**
- **„PO-SMSI-Securitatea echipamentelor”;**
- **„PO-SMSI-Procesarea corectă a datelor în cadrul aplicațiilor”;**
- **„PO-SMSI-Proceduri operaționale și responsabilități”;**
- **„PO-SMSI-Protecția împotriva codurilor mobile și dăunătoare”;**
- **„PO-SMSI-Copie de siguranță”;**

- „**PO-SMSI-Securitatea fișierelor de sistem”;**
- „**PO-SMSI-Monitorizare”;**
- „**PO-SMSI-Managementul securității rețelei”;**
- „**PO-SMSI-Planificarea și acceptanța sistemului”;**
- „**PO-SMSI-Managementul serviciilor furnizate de terți”;**
- „**PO-SMSI-Managementul incidentelor SMSI”;**
- „**PO-SMSI-Managementul continuității activităților”;**
- „**PO-SMSI-Conformitatea cu cerințele legale”;**
- „**PO-SMSI-Achiziția, dezvoltarea și mentenanța sistemelor”;**
- „**PO-SMSI- Procedura de audit intern”;**
- „**Declarația de aplicabilitate (SOA)”;**
- „**Registrul riscurilor și tratarea acestora”;**
- „**Politica de securitate a furnizorilor”;**
- „**Program de audit intern”;**
- „**Politica de clasificare a informațiilor”.**[30]

Se poate spune că un număr mare de politici și proceduri nu reprezintă decât o îngreunare a activității pentru instituție, acest lucru putând fi adevărat doar dacă acestea au fost scrise numai în vederea trecerii auditului de certificare ISO 27001:2018. Concluzionăm că setul de documente ce vor conține politici, proceduri și documente propuse spre adoptare în cadrul SMSI la nivelul Autorității Electorale Permanente vot trebui scrise cu intenția reducerii riscurilor de securitate informațională și astfel își vor demonstra valoarea odată cu trecerea timpului, prin reducerea numărului de incidente de securitate la nivelul instituției.

4.2.8. Monitorizarea performanței prin indicatori la nivelul Autorității Electorale Permanente

În contextul implementării SMSI la nivelul AEP, vor fi definite o serie de dispoziții și obiective de securitate a informațiilor ce vor conține și orientări sau concepte pentru punerea lor în practică de către toate departamentele, iar respectarea acestor dispoziții va fi monitorizată în permanență.

În analiza proceselor de management, performanța la nivel de echipă sau a fiecărui angajat în parte va reprezenta unul dintre obiectivele majore ce trebuie urmărit la nivelul managementului instituției, în condițiile în care acest indicator se va raporta permanent la calitatea serviciilor pe care prin efectul legii AEP trebuie să le asigure către cetățeni.

Pentru a măsura nivelul realizării obiectivelor specifice cu privire la securitatea informațiilor și a măsura eficacitatea strategiilor implementate prin intermediul SMSI, va fi necesară definirea unui sistem integrat de indicatori de performanță, pe care instituția va trebui să-i folosească pentru a autoevalua rezultatele.

Indicatorii de performanță sunt instrumente eficiente prin care se poate măsura performanța activităților și acțiunilor întreprinse în domeniul securității, precum și succesul acestora în îndeplinirea obiectivelor generale și specifice ale instituției stabilite în cadrul SMSI. Indicatorii oferă informații despre performanța întregului SMSI și a fiecărei activități în parte și servesc drept catalizatori pentru ca managementul să se implice atunci când aceștia nu sunt atinși și să ia măsuri în consecință. Această implicare poate însemna evaluarea situației la un anumit moment în comparație cu situația dorită și intervenția corectivă a managementului pentru remediere și atingerea indicatorilor.

În cadrul activităților desfășurate pentru implementarea SMSI vor trebui regândiți, stabiliți și adoptați noi indicatori de performanță ce vor trebui să urmărească conceptul de obiective de tip **SMART (**specifice, măsurabile, accesibile, relevante/realizabile, la termen). Drept urmare indicatorii de performanță trebuie să fie specifici, măsurabili, accesibili și realizabili, atât de-a lungul axei temporale, cât și prin implementarea lor în toate departamentele

instituției, aceștia trebuind să fie structurați în mod sistematic și să se bazeze pe fundamente statistice și matematice adecvate și solide.

Pentru a aduce plus valoare creării unui mecanism menit să susțină performanța proceselor de monitorizare și evaluare în cadrul AEP, în cadrul implementării SMSI va trebui acordată o atenție deosebită pregătirii profesionale continue a personalului cu atribuții în domeniul monitorizării și evaluării indicatorilor de performanță.

4.2.9. Managementul incidentelor de securitate la nivelul Autorității Electorale Permanente

Deși nu este menționată în mod explicit în secțiunea normativă a standardului, managementul incidentelor de securitate a informațiilor este o componentă esențială a unui SMSI funcțional, ce va trebui să fie implementată în cadrul sistemului de management ce se va implementa la nivelul AEP.

Incidentele relevante pentru securitate sunt în general neconformități care pot avea un impact decisiv asupra procesului de îmbunătățire continuă și asupra maturității SMSI, în cazul în care cauzele acestora sunt investigate. După identificarea greșelilor și extragerea concluziilor relevante din ele, se vor regândi activitățile și strategiile și se vor elimina sau înlocui măsurile ce se vor constata a fi ineficiente, se vor actualiza conceptele de securitate existente sau se vor implementa noi soluții și astfel se vor obține cele mai mari beneficii de pe urma unui sistem de management care va funcționa în condiții predictibile.

Pentru o implementare corectă și predictibilă a managementului incidentelor, la nivelul AEP se va întocmi în cadrul SMSI o politică de management a incidentelor. Acest document va stabili care sunt activitățile prin care se vor implementa măsurile de securitate, de către echipa tehnică a AEP, ce va avea cunoștințe și aptitudini în acest domeniu. Pentru ca politica să aducă valoare adăugată instituției în demersul de implementare a SMSI, trebuie să se fundamenteze pe rezultatele analizei riscurilor de securitate, ce trebuie făcută în prealabil.

Procesul de management al informaţiilor în timpul gestionării incidentelor trebuie să înceapă cu colectarea informaţiilor, care poate fi diferită de la caz la caz deoarece obținerea datelor despre incident se poate face prin primirea rapoartelor de incident din partea angajaților sau beneficiarilor, sau prin recepționarea de alerte de la sistemul informatic de monitorizare a incidentelor.

RMSI are obligativitatea de a raporta către conducerea AEP toate incidentele referitoare la informații, furnizând periodic rapoarte privind toate incidentele de securitate. Conducerea împreună cu angajații DIPE și RMSI decid dacă incidentalele de securitate întâmplate, trebuie raportate mai departe către organele de cercetare ale statului și/sau către CERT/CSIRT.

Pentru a minimiza probabilitatea apariției unui incident de securitate la nivelul AEP, echipa desemnată să asigure implementarea SMSI trebuie să analizeze cu atenție datele despre incidente sau vulnerabilități, care sunt transmise de CERT/CSIRT partenere ale instituției, de prestatorii de servicii de securitate informatică, de autoritățile statului cu competență în securitatea informațională etc.

4.2.10.Comunicarea în contextul implementării SMSI la nivelul Autorității Electorale Permanente

În vederea implementării unui SMSI, la nivelul AEP va fi necesară cooperarea Departamentului Informatizarea Proceselor Electorale, ce va implementa și administra sistemul, cu celelalte departamente ale instituției pentru ridicarea permanentă a nivelului de securitate a informațiilor. Cooperarea interinstituțională de acest fel se realizează prin comunicare, care este elementul cheie în ceea ce privește atingerea target-ului de securitate, ce va avea ca efect păstrarea renumelui AEP de instituție constituțională de prestigiu a statului român.

Sarcina principală a componentei „comunicare” în cadrul misiunii de implementare a SMSI și certificarea acestuia în conformitate cu standardul de referință este determinarea și

descrierea cerințelor și nevoilor de comunicare internă și externă a AEP cu privire la acest subiect. La nivelul AEP, comunicarea în general se află în atribuțiile Departamentului Cooperare Internațională, acestea fiind cel mai potrivit departament pentru a prelua ca atribuții componenta de comunicare din cadrul SMSI.

Comunicarea externă în acest context se referă la comunicarea cu colaboratorii din afara instituției, ce de obicei sunt furnizorii, auditorii externi, instituțiile ce au rol de CERT/CSIRT sau cu alte instituții ale statului cu care AEP are relații de colaborare în ceea ce privește asigurarea securității informaționale.

Atunci când se vor disemina informații despre incidentele de securitate ce au avut loc în cadrul instituției, cel care face comunicarea va trebui să fie foarte atent în scopul filtrării informațiilor sensibile sau clasificate ce se pot strecura în materialul ce trebuie comunicat și să aibă în vedere adoptarea tuturor măsurilor necesare de confidențialitate a informațiilor ce se vor comunica, mai ales cele ce se vor transmite prin canale externe.

4.2.11. Competență și conștientizare în rândul personalului Autorității Electorale Permanente

Întreg colectivul de angajați ai instituției are obligația de a lua la cunoștință politica de securitate a informațiilor, să o analizeze cu atenție, să își asume responsabilitățile în ceea ce privește SMSI, precum și urmările încălcării acesteia sau alte neconformități. Conștientizarea fenomenului securității informațiilor trebuie să fie proporțională cu nivelul cu care managementul are capacitatea de a disemina informațiile relevante referitoare la sistemul SMSI.

Un mod clasic prin care se poate realiza conștientizarea colectivului este modificarea fișelor de post ale angajaților din domeniul SMSI. Fișele de post ale angajaților implicaţi în implementarea sistemului vor trebui să fie modificate în sensul introducerii de atribuții care sunt obligatorii implementării SMSI și se vor specifica competențele necesare pentru angajații ce vor avea responsabilități cu privire la asigurarea securității informațiilor.

Formarea profesională continuă a funcționarilor publici din cadrul AEP va juca un rol foarte important pentru implementarea cu succes a sistemului de management. Succesul va implica o bună cunoaștere a domeniului securității informațiilor și a activităților conexe acestora de către toți angajații ce au atribuții directe sau indirecte în securitatea informaționala a instituției. Formarea profesională trebuie să aibă loc în toate etapele de implementare a SMSI şi să atingă cât mai multe din țintele de cunoaștere a prevederilor standardului, a politicilor și procedurilor interne aferente sistemului.

Este necesar să fie puse în practică campanii de conștientizare a securității informațiilor care vor trebui să fie împărțite în trei faze, ce vor cuprinde următoarele activități: evaluarea cerințelor de cunoștințe și informații, planificarea campaniei și punerea acesteia în aplicare. Conștientizarea securității informației trebuie să fie mai mult decât un proiect punctual, căci în campaniile ce se vor derula la nivelul instituției vor trebui incluse mecanisme care să asigure durabilitatea acesteia. De asemenea, vor trebui analizate în prealabil la nivelul conducerii împreună cu RMSI metodele de evaluare a eficienței campaniei, ce se vor pune în aplicare după finalizarea acesteia.

4.2.12. Audit intern în vederea implementării SMSI la nivelul Autorității Electorale Permanente

Obiectivele principale ale auditurilor interne ale SMSI la nivelul AEP vor include monitorizarea măsurii în care SMSI implementat va îndeplini pe de o parte, scopul, obiectivele și cerințele instituției și pe de altă parte cerințele standardului ISO/IEC 27001:2018, activitate ce poartă numele de „controlul conformității”. Totodată echipa de audit va monitoriza implementarea eficacității măsurilor de securitate a informațiilor ce au fost luate de echipa de implementare a sistemului, activitate ce este denumită „controlul implementării și eficacității”.

După implementarea SMSI la nivelul AEP și crearea întregii documentații aferente, se vor planifica misiuni de audit public intern, ce vor avea ca obiective controlul aspectelor privind frecvența, procedura, rolurile și responsabilitățile, cerințele de planificare, trasabilitatea și raportarea măsurilor luate în cadrul sistemului de management. Echipa de management, împreună cu cea tehnică vor trebui să se definească metode rapide de tratare a acțiunilor corective și preventive recomandate de echipa de audit și să se stabilească cine le va urmări pentru a implementa măsurile ce au fost lăsate de auditori.

Misiunile de audit sunt menite să asigure că toate procesele instituționale acoperite de SMSI, stabilite în conformitate cu domeniul de aplicare sunt auditate periodic și că întotdeauna auditul va lăsa în urmă dovezi scrise ale celor constatate.

Auditurile interne ale SMSI vor reprezenta un instrument vital în procesul de îmbunătățire continuă a sistemului de management ce se va implementa la nivelul AEP. Ele vor fi utilizate pentru asigurarea conformității sistemului de management cu cerințele proprii ale instituției și cu cele ale standardului ISO 27001:2018 pentru stabilirea componentelor sistemului care impun îmbunătățiri. Programul de audit va asigura acoperirea controlului asupra tuturor aspectelor de securitate a informațiilor din domeniul de aplicare, într-un mod eficient pentru îmbunătățirea sistemului de management în vederea certificării acestuia în conformitate cu standardul ISO 27001:2018.

După remedierea măsurilor lăsate de auditurile interne se poate demara procedura de certificare, ce implică un audit de certificare care este întotdeauna un audit extern efectuat de entități autorizate de entitățile naționale și internaționale de standardizare, ce au angajați auditori calificați și certificați de o autoritățile de certificare ISO 27001:2018.

Rezultatele pregătirii misiunii de audit extern în vederea certificării vor fi concretizate într-un set de documente ce vor fi trimise unui auditor acreditat ISO 27001:2018 pentru revizuire și un set de evidențe și dovezi care vor demonstra cât de eficient și complet a fost implementat SMSI-ul la nivelul Autorității Electorale Permanente.

4.2.13. Îmbunătățirea continuă a SMSI la nivelul Autorității Electorale Permanente

Trebuie reținut faptul că, indiferent de câte analize ale managementului sau misiuni de audit ale SMSI se vor efectua la nivelul AEP este puțin probabil ca acesta să fie conceput într-o formă finală perfectă de la începutul implementării acestuia. Chiar dacă instituția va beneficia de ajutorul și experiența unei companii de consultanță ce va analiza contextul și va participa la implementarea efectivă, implementarea SMSI nu va fi simplă deoarece mediul instituțional este diferit, activitățile și provocările instituției sunt diferite și nu a fost încă identificată o soluție panaceu, care să funcționeze perfect pentru toate instituțiile unde se implementează astfel de sisteme de management.

Mai mult, circumstanțele geopolitice, în ceea ce privește starea de securitate sunt în continuă schimbare, astfel încât nu poate exista niciodată o „soluție perfectă” permanentă, când este vorba despre securitatea informațională.

Din acest motiv, la nivelul AEP va trebui asigurat un continuu proces de analiză a modelelor de urmat în acest domeniu, pentru adaptarea la propriile nevoi și îmbunătățirea continuă a politicilor, procedurilor și documentelor SMSI. Este deosebit de important ca instituția să profite de neconformitățile identificate în cadrul tuturor controalelor sau misiunilor de audit, pentru a îmbunătăți în permanență SMSI și pentru a actualiza în mod constant acest sistem, procesul fiind cunoscut sub numele de proces de îmbunătățire continuă.

Rezultatele acestor analize de gestiune a securități informaționale vor duce la îmbunătățirea politicilor și procedurilor de securitate a informațiilor în instituție, ce vor avea ca scop îmbunătățirea continuă a SMSI.

CAPITOLUL 5
CONCLUZII FINALE, DEZVOLTĂRI VIITOARE, CONTRIBUȚII PERSONALE ȘI MODALITĂȚI DE VALORIFICARE A REZULTATELOR CERCETĂRII

5.1. CONCLUZII FINALE PRIVIND CERCETĂRILE EFECTUALE ÎN CADRUL TEZEI DE DOCTORAT

Cercetarea efectuată în cadrul prezentei teze de doctorat, intitulată „**Cercetări și contribuții privind implementarea sistemelor de calitate-risc în vederea asigurării securității informaționale în instituțiile publice**”, a avut ca punct de plecare necesitatea stringentă percepută în spațiul public privind securitatea informațiilor în instituțiile publice. Această necesitate, ce a fost declanșată de reconfigurarea profundă a rolului, efectelor și în același timp a vulnerabilităților pe care le presupun procesele de management informațional, trebuie să devină o prioritate a oricărei instituții publice.

Ipoteza lucrării o constituie potențialul de eficientizare a răspunsului organizațiilor de stat în fața amenințărilor ce privesc securitatea informațiilor, în contextul implementării de sisteme de tip calitate-risc și certificarea acestora în conformitate cu standardele internaționale în acest domeniu. Această ipoteză este explorată și demonstrată prin intermediul modelului practic prezentat detaliat în cadrul capitolului 4 al tezei de doctorat, „**Cercetări și contribuții practice privind implementarea la nivelul Autorității Electorale Permanente a unui sistem de management al securității informațiilor și certificarea acestuia conform SR/EN ISO 27001:2018**”.

Obiectivele teoretice ale tezei de doctorat:

- **Analiza teoretică și comparativ-critică a stadiului actual al cercetărilor cu privire la securitatea informațională.**
- **Stabilirea rolului și importanței securității informațiilor în instituțiile publice.**
- **Cercetarea metodelor, modalităților și sistemelor prin care se poate asigura securitatea informațiilor la nivelul instituțiilor publice.**
- **Analiza teoretică sistemelor de management a securității informaționale și certificarea acestora conform standardului internațional SR EN ISO/IEC 27001:2018.**
- **Identificarea particularităților aplicabilității SMSI în contextul implementării în instituții de stat.**

Obiectivele practice ale tezei de doctorat:

- **Proiectarea unui model de implementare practică a SMSI și certificarea acestuia conform standardului internațional SR EN ISO/IEC 27001:2018 la nivelul Autorității Electorale Permanente din România.**
- **Propunerea unui set de măsuri ce pot face parte din Politica de securitate ce se va adopta în cadrul SMSI al AEP.**
- **Stabilirea procedurilor, documentelor și politicilor ce vor trebui adoptate de AEP în cadrul SMSI.**
- **Identificarea riscurilor de securitate a informațiilor de la nivelul AEP în vederea tratării acestora.**
- **Propunerea planului de acțiune pentru implementarea SMSI la nivelul AEP ce va conține fazele acestuia, termenele de implementare, responsabilii și livrabilele.**

Concluzia generală a tezei este că în aceste vremuri caracterizate de tensiuni politice majore, războaie clasice sau hibride, pe lângă creșterea exponențială a numărului de incidente de securitate din domeniul informațiilor, a crescut în mod proporțional și complexitatea atacurilor asupra acestora, dar, mai ales gradul de sofisticare a mijloacelor și tehnicilor de atac, ceea ce a impus apariția și dezvoltarea de metode, instrumente și procedee de apărare activă împotriva acestor atacuri.

5.2.DEZVOLTĂRI VIITOARE PROPUSE ÎN CADRUL DOMENIULUI CERCETAT

Rezultatele studiilor efectuate în cadrul tezei de doctorat au condus încă din faza de cercetare către concluzia că pentru asigurarea unui climat de securitate informațională în instituțiile publice este potrivită măsura implementării unor Sisteme de Management a Securității Informațiilor, în conformitate cu rigorile standardului ISO 27001:2018.

Astfel se justifică necesitatea continuării studiului de față cu privire la domeniul securității informațiilor, care să vizeze gestionarea riscurilor de securitate prin implementarea unor standarde internaționale care vizează domeniul securității informaționale, dintre care amintim: toate celelalte standarde din seria ISO 27000; standardul COBIT, certificarea ITIL etc.

Pentru îndeplinirea scopului de menținere a securității informațiilor în entitățile de stat, am identificat nevoia de studiu aprofundat în ceea ce privește analiza modului prin care politicile de securitate a informațiilor se pot transforma în politici publice, care să stea la baza îndeplinirii obiectivelor generale și specifice ale acestora.

Continuarea cercetării în direcțiile prezentate anterior poate avea ca rezultat identificarea unor noi metode practice prin care instituțiile publice vor adopta noi politici de securitate a informațiilor cât mai cuprinzătoare în vederea garantării unui climat de securitate a informațiilor pe care le gestionează.

Concluziile ce vor reieși în urma cercetărilor științifice vor ajuta instituțiile publice în procesul de analiză inițială, consultanță și implementare a politicilor de securitate a informațiilor standardizate, ale căror rezultate au fost testate în prealabil de către entități de certificate recunoscute la nivel internațional.

Prin implementarea acestor noi politici instituțiile vor fi obligate să revizuiască sau să schimbe în totalitate documentația și procedurile de securitate, prin intermediul cărora se va putea asigura prevenirea apariției unor potențiale breșe de securitate a informațiilor.

5.3. CONTRIBUȚII PERSONALE ALE AUTORULUI ÎN DOMENIUL CERCETAT

În concordanță cu limitele de ordin normativ identificate în cadrul cercetării bibliografice efectuate în cadrul tezei de doctorat, precum şi cu dinamica ridicată a domeniului cercetat, punctez ca și contribuții personale următoarele:

- **aprofundarea studiilor** cu privire la particularități și metode de implementare a SMSI și certificare a acestuia conform SR EN ISO/IEC 27001:2018 în cadrul instituțiilor publice, printre care amintim obligativitatea acestor entități de a respecta „OSGG nr.600/2018 privind aprobarea Codului de control al managementului intern al entităților publice”, fapt ce impune adaptarea procesului de implementare și a tuturor documentelor sistemului de management la regulile stabilite de Ordin;

- **planificarea activităților de implementare a SMSI** și de certificare a acestuia în conformitate cu standardul ISO 27001:2018, în cadrul instituțiilor publice, stabilirea responsabililor fiecărei activități și măsurarea valorii adăugate a fiecărei activități în ceea ce privește securitatea informațională;
- **analiza legislației incidente securității informaționale din România** ce era în vigoare la data cercetării și implicațiile acesteia în ceea ce privește implementarea SMSI în cadrul instituțiilor publice din România;
- **contribuția practică a autorului este propunerea unui model de implementare practică a la nivelul Autorității Electorale Permanente**, ce reprezintă o noutate în contextul securității informațiilor în cadrul acestei instituții publice; această viitoare implementare a SMSI va contribui la ridicarea nivelului de securitate a informațiilor, prin care se va crea o imagine pozitivă a instituției, ridicând-o la cele mai înalte standarde între entitățile de management electoral de la nivel internațional.
- **Certificarea SMSI conform standardului ISO 27001:2018** va aduce împreună cu ea mai multe avantaje pentru menținerea unul climat de securitate a informațiilor în AEP, deoarece este un standard recunoscut de securitate a informațiilor la nivel mondial. Implementarea măsurilor de securitate impuse de acest standard pot ajuta instituția să micșoreze numărul sau să scadă intensitatea riscurilor de securitate și să implementeze politici de securitate informațională, în scopul construirii unei bune reputații în concepția publică.

În concluzie, menționăm că implementarea SMSI și certificarea acestuia conform normelor standardului ISO 27001:2018 în cadrul AEP va asigura o imagine pozitivă a acesteia în mentalul colectiv, având la bază un nivel ridicat al securității ce este verificat permanent de către entități de audit extern pentru asigurarea securității informațiilor.

5.4. MODALITĂȚI DE VALORIFICARE A REZULTATELOR CERCETĂRII

Rezultatele obținute în urma cercetărilor efectuate în cadrul tezei de doctorat au fost valorificate prin intermediul analizelor și studiilor de caz create, care au ca scop convingerea managementului de top al Autorității Electorale Permanente în sensul implementării SMSI și certificarea acestuia conform „SR EN ISO/IEC 27001:2018”.

Prin aceste rezultate vom convinge beneficiarii de servicii că instituția și-a creat o imagine credibilă și un mediu digital modern și european, prin care se străduiește să asigure un cadru general de securitate a informațiilor la un nivel ridicat. Astfel, a fost agreată de principiu la nivelul conducerii instituției utilizarea Capitolului 4 al tezei de doctorat drept consultanță inițială în vederea implementării SMSI la nivelul AEP.

Un alt mod de valorificare a rezultatelor cercetării științifice din cadrul tezei au fost publicările de lucrări științifice în reviste sau buletine de specialitate și lucrările publicate la congrese sau conferințe naționale și internaționale, în calitate de autor sau coautor

BIBLIOGRAFIE SELECTIVĂ

[1] Legea nr. 182/2002 privind protecția informațiilor clasificate, disponibil la https://lege5.ro /App /Document /gm4dsnbx /legea nr 1822002 privind protecția informatiilor clasificate?pid=12542165, site consultat la data 03.05.2021;
[2] Șerb, Aurel, Baron, Constantin, Isăilă, Narcisa, Securitate informatică în societatea informațională, Editura Pro Universitaria, București (2010), p. 31
[3] Giurcan, Gigi, Terorismul cibernetic, teză de doctorat (2010), p. 94;
[4] Klimburg, Alexander (ed.), National Cyber Security-Framework Manual, NATO Cooperative Cyber Defence Center of Excellence, Tallin, Estonia (2012), disponibil la https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/, site consultat la data 12.05.2021;
[5] Klimburg, Alexander (ed.), National Cyber Security-Framework Manual, NATO Cooperative Cyber Defence Center of Excellence, Tallin, Estonia (2012), disponibil la https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/, site consultat la data 15.05.2021;
[6] Morgenthau, Hans, Politics Among Nations: The Struggle for Power and Peace, Kalyani Publishers, [2018], p. 290-292;
[7] Howard, John D., Longstaff, Thomas A., A common language for computer security incidents, Office of Scientific and Technical Information, United States Department of Energy (1998);
[8] Definiție hacker în limba română, disponibil la https://dexonline.ro/definitie/hacker, site consultat la data 10.06.2021;
[9] Definiție hacker în limba engleză, disponibil la https://www.lexico.com/en/ definition/hacker, site consultat la data 10.06.2021;
[10] Stan, Emil, Străinu, Emil, Terorismul cibernetic, Editura Academiei de Înalte Studii Militare (2002);
[11] Stan, Emil, Străinu, Emil, Terorismul cibernetic, Editura Academiei de Înalte Studii Militare (2002), p. 169;
[12] Idem
[13] Sullivan, Peter, Care este rolul unui Computer Emergency Response Team (CERT), disponibil la https://www.techtarget.com/whatis/definition /CERT Computer Emergency Readiness Team, site consultat la data de 30.06.2021;
[14] Coteanu, Ion., Seche Luiza, Dicționar Explicativ al Limbii Romane, Editura Univers Enciclopedic, Bucureşti, (1996)
[15] Roșca Constantin, Dicționar de Ergonomie, Editura CERTI, Craiova, (1997)
[16] Asociația Romana de Standardizare - Organismul National de Standardizare (ASRO), Managementul riscului. Cod de practică şi îndrumare pentru implementarea standardului SR ISO 31000, disponibil la http://standardizare.wordpress.com/2013/07/ 02/sr-bs-311002013-managementul-riscului-cod-de-practica-si-indrumare-pentru-implementarea-standardului-sr-iso-31000/, site consultat la data de 01.07.2021;
[17] The National Institute of Standards and Technology (NIST) - U.S. Department of Commerce, NIST SP 800-37R2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, disponibil la, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, site consultat la data de 01.07.2021;
[18] Mitnick, Kevin D., Simon, William L., The art of intrusion. The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers, Wiley Publishing Inc., Indianapolis, Indiana

(2005), disponibil la https://repo.zenk-security.com/Magazine%20E-book/ Kevin Mitnick-The Art of Intrusion.pdf, site consultat la data 02.07.2021;
[19] Papastergiou, Spyridon, Mouratidis, Haralambos, Kalogeraki, Eleni Maria, Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures, Evolving Systems, No.21 (2021), p. 91-108, disponibil la https://link.springer.com/content/pdf/10.1007/s12530-020-09335-4.pdf, site consultat la data de 01.08.2021;
[20] Ravndal, Jacob Aasland, Johnsen, Siw Tynes, Kjeksrud, Stian, Broen, Torgeir, Resilience methodology – multinational experiment 7, Norwegian Defence Research Establishment (FFI) (2014), disponibil la https://publications.ffi.no/nb/item/asset/dspace: 2430/14-00973.pdf, site consultat la data de 01.08.2021;
[21] Rosenzweig Paul, Bucci, Steven P., Inserra, David, A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace, The Heritage Foundation, No. 2785 (2013), disponibil https://www.heritage.org/defense/report/congressional guide seven steps us security prosperity and freedom cyberspace, site consultat la data de 03.08.2021;
[22] International Organization for Standardization, disponibil la https://www.iso.org/ about-us.html, site consultat la data 07.07.2021;
[23] ISO/IEC 27001:2018 Information Security Management, disponibil la, https://www. iso.org/isoiec-27001-information-security.html, site consultat la data 18.07.2021;
[24] Familia de standarde internaționale ISO 27000, tehnologia informației – tehnici de securitate – sisteme de management al securității informației, privire de ansamblu și vocabular, disponibil la https://standards.iso.org/ittf/PubliclyAvailableStandards/c07390 6 ISO IEC 27000 2018 E.zip, site consultat la data 18.07.2021;
[25] Măsuri de control și obiective de securitate ale standardului 27001 https://www.it governance.co.uk/blog/iso 27001 the 14 control sets of annex a explained, site consultat la data 24.07.2021;
[26] Strategia bazată pe modelul Deming (PDCA), Studiu privind beneficiile și efectele implementării sistemelor de management al calității în instituții publice din state europene, disponibil la https://www.mdlpa.ro/uploads/articole/attachments/61a87b75ef8 ca072647906.pdf, site consultat la data 24.07.2021;
[27] Despre Autoritatea Electorală Permanentă, disponibil la https://www.roaep.ro/ prezentare/despre-noi/, site consultat la data 08.08.2021;
[28] Regulamentul de Organizare și Funcționare al AEP, aprobat prin Hotărârea nr. 4/2020 a Birourilor Permanente ale Camerei Deputaților și Senatului, disponibil la https: //www.roaep.ro/prezentare/wp-content/uploads/2020/12/regulamentul de organizare si functionare a autoritatii electorale permanente 2020.pdf, site consultat la data 22.08.2021;
[29] Henning, David, Tackling ISO 27001: A project to build an ISMS, SANS Institute (2009), disponibil la https://sansorg.egnyte.com/dl/JjBP0dMfnB, site consultat la data 22.08.2021;
[30] Asociația de Standardizare din Romania, SR EN ISO/IEC 27001:2018 Tehnologia informației, Tehnici de securitate, Sisteme de management al securității informației, Cerințe. Privire de ansamblu și vocabular, (2018);