UNIVERSITATEA DE STAT DIN MOLDOVA

ȘCOALA DOCTORALĂ ȘTIINȚE ALE NATURII

Cu titlu de manuscris
C.Z.U. 004.056:336.71(478)(043)

BRICEAG VALENTIN

ANALIZA ȘI CREȘTEREA NIVELULUI DE MATURITATE A SISTEMULUI DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI PENTRU ENTITĂȚI DIN REPUBLICA MOLDOVA

(Pe exemplul băncilor comerciale)

232.02 Tehnologii, produse și sisteme informaționale

Rezumatul tezei de doctor în Informatică

Chișinău, 2024

Teza a fost elaborată în cadrul Universității de Stat din Moldova, Școala Doctorală Științe ale Naturii, Departamentul de Informatică al Facultății de Matematică și Informatică.

Conducător științific:

BRAGARU Tudor	doctor în economie, profesor universitar, Universitatea de Stat din Moldova

Componența Comisiei de Doctorat:

CĂPĂȚÂNĂ Gheorghe	Doctor în științe tehnice, profesor universitar, Universitatea de Stat din Moldova – *președinte*
BRAGARU Tudor	Doctor în economie, profesor universitar, Universitatea de Stat din Moldova – *conducător de doctorat*
BOLUN Ion	Doctor habilitat în informatică, profesor universitar, Universitatea Tehnică a Moldovei – *referent*
COJOCARU Igor	Doctor în informatică, conferențiar universitar, Institutul de Dezvoltare a Societății Informaționale – *referent*
OHRIMENCO Serghei	Doctor habilitat în economie, profesor universitar, Academia de Studii Economice a Moldovei – *referent*

Susținerea va avea loc la **18.09.2024,** ora **15:00** în cadrul Ședinței Comisiei de susținere publică a tezei de doctorat din cadrul Școlii Doctorale Științe ale Naturii, USM. Sediul – Universitatea de Stat din Moldova (http://www.usm.md), **str. M. Kogălniceanu 65 A, blocul 3, sala 332**, MD-2009, Chișinău, Moldova.

Teza de doctor și rezumatul pot fi consultate la Biblioteca Națională a Republicii Moldova (str.31 August, 78a, Chișinău, MD 2012) și Biblioteca Centrală a Universității de Stat din Moldova (str. Alexei Mateevici 60, Chișinău, MD 2009), pe pagina web a ANACEC (http://www.cnaa.md) și pe pagina web a USM (http://www.usm.md).

Rezumatul a fost expediat la „____”_____2024

Președintele Comisiei de Doctorat
Doctor în științe tehnice, profesor universitar _____ (semnătura) CĂPĂȚÂNĂ Gheorghe

Autor: _____ (semnătura) BRICEAG Valentin

© Briceag Valentin, 2024

CUPRINS

REPERELE CONCEPTUALE ALE CERCETĂRII 4

CONȚINUTUL TEZEI 7

CONCLUZII FINALE ȘI RECOMANDĂRI 26

BIBLIOGRAFIE 29

LISTA PUBLICAȚIILOR LA TEMA TEZEI 31

ADNOTARE 32

ANNOTATION 33

АННОТАЦИЯ 34

REPERELE CONCEPTUALE ALE CERCETĂRII

Actualitatea și importanța temei abordate. Actualmente majoritatea absolută a persoanelor fizice și juridice, a organizațiilor private, publice, guvernamentale etc. sunt prezente în spațiul digital/virtual global, fără careva frontiere bine definite și clar delimitate. Prezența masivă a oamenilor și organizațiilor în spațiul virtual constituie o sursă majoră a riscurilor de securitate pentru datele personale și informațiile sensibile manipulate în spațiul cibernetic, dar care sunt valoroase pentru o persoană fizică, o organizație, o regiune sau un stat. Confundarea conceptelor de Securitate a Informației (SecInf), Securitatea Cibernetică (SC), informatică etc. [1], iluzia precum că datele, informațiile nu sunt atât de valoroase încât merită a cheltui bani cu asigurarea lor, alte iluzii precum că SecInf rezidă exclusiv în securitatea IT/IS și este exclusiv grija departamentului IT și că cumpărarea mai multor instrumente poate consolida SC etc. – duc la tratarea eronată a SecInf/SC.

Or, succesul unei organizații moderne, indiferent de sfera sa de activitate, de dimensiune, forma de proprietate etc., depinde de **înțelegerea rolului pe care informațiile îl joacă în viața sa și de gestionarea eficientă a acestor informații. Inclusiv de asigurarea securității informației ca proces desfășurat într-un mediu aflat în continuă schimbare,** care se maturizează *(crește, se îmbunătățește)* de-a lungul timpului în funcție de cerințe, cultură, scop urmărit, investiții, personal implicat etc.

Asigurarea securității informației în spațiul cibernetic devine o preocupare majoră a tuturor actorilor implicați la diferite niveluri, pornind de la persoane fizice *(protecția datelor personale),* organizații particulare și publice *(universități, școli, spitale, primării, bănci etc. – protecția datelor sensibile)* și terminând cu nivelul organelor guvernamentale de reglementare și supraveghere *(de exemplu Ministerul Educației, Ministerul Sănătății, Ministerul Finanțelor, Banca Națională, Inspectoratul Fiscal de Stat, Serviciul Tehnologia Informației și Securitate Cibernetică etc.),* unde se concentrează responsabilitatea elaborării și aplicării politicilor de securitate coerente în domeniul respectiv la nivel de stat sau la nivel global pe anumite industrii.

Încadrarea temei în preocupările internaționale, în context inter-/ și transdisciplinar. Tema cercetată se încadrează perfect și corelează puternic cu strategiile și bunele practici generate de organizațiile globale specializate. Printre cele mai importante asemenea organizații sunt dezvoltatorii standardelor sistemelor de management *(și audit, ca componentă indispensabilă a acestora)* precum și organizațiile ce oferă recomandări, educație și certificări profesionale în domeniul securității informațiilor precum Asociația mondială de Audit și Control a Sistemelor Informaționale (ISACA, www.isaca.org), Institutul Național de Standardizare și Tehnologie din S.U.A. (NIST, http://nist.gov), Comitetul pentru securitatea datelor din industria cardurilor de

plată (PCI SSC, https://www.pcisecuritystandards.org), Organizația Internațională pentru Standardizare (ISO, https://www.iso.org/standards.html/), Institutul SANS (SysAdmin, Audit, Network, Security, http://sans.org), Centrul de internet securitate/CIS (https://cissecurity.org), Organizația mondială de certificare profesională (ISC)² (Information Security Certifications), care menține actual corpul de cunoștințe CBK *(Common Body of Knowledge)* pe care se bazează certificările profesionale, recunoscute drept standard global de excelență și altele.

Scop urmărit. Realizarea unui **model multiprofil de maturitate (M^{3}SI) simplu, transparent, ușor de administrat și utilizat** pentru realizarea de **profiluri de SecInf tipice unor industrii (PSITI) și profiluri individuale de SecInf (PISI),** particularizate conform nevoilor concrete ale unor entități, care ar susține nevoile tuturor actorilor implicați de la toate nivelurile, pornind de la managerii de vârf, profesioniștii și experții în securitatea informației etc., până la utilizatorii finali, conectați la rețea de la stații terminale, adesea aflate la distanță și negestionate de entitate.

Pentru atingerea scopului au fost realizate un set de **obiective majore** precum: *studiul diverselor cadre de abordare și de reglementare a SecInf, crearea unei baze generice de date M^{3}SI privind cunoștințele despre cadre, zone, cerințe, amenințări, riscuri și controale de SecInf; elaborarea unui profilul de securitate a informației tipic sectorului bancar PSITI și a unui profil individual de securitate a informației PISI pentru o Bancă Comercială (BC) ipotetică, dar cu aplicabilitatea directă confirmată de Banca Națională a Moldovei BNM); elaborarea aplicației instrumentale de administrare a modelului multiprofil M^{3}SI, a profilurilor tipice PSITI și a profilurilor individuale PISI.*

Cercetarea este focusată pe problemele organizaționale, de management în asigurarea securității informației prin prisma unui Sistem de Management a Securității Informației (SMSI), bazat pe abordarea riscurilor de securitate a informației, constituit dintr-un set de măsuri tehnico-organizatorice *(e.g. acte normative, proceduri interne, resurse umane, procese și servicii IT/IS etc.)* și orientat spre atingerea obiectivelor de asigurare a SecInf în cadrul entității. **SMSI trebuie privit ca parte indispensabilă a sistemului de control intern.**

Metodologia utilizată. Dezvoltarea modelului de maturitate M^{3}SI, care ar permite determinarea stării actuale a SecInf/SC, a SMSI și direcțiile prioritare de dezvoltare se bazează, în temei, pe **sintezarea metodologiilor și modelelor de securitate deschise**, ținând cont de cerințele principalului standard sistemic ISO/IEC 27001:2022 [2], urmărind simplificarea și automatizarea proceselor rutinare.

Rezultatele tezei includ adoptarea unui cadru generic unic – Model multiprofil de maturitate a SecInf/SC M^{3}SI, cu o bază de date unică privind cunoștințele despre cadrele de abordare și controalele de SecInf, din care sunt generate profiluri tipice și particulare de SecInf, potrivite necesităților concrete de analiză, măsurare și îmbunătățire continuă a SC.

Importanța, valoarea aplicativă a rezultatelor obținute constă în funcționarea mai sigură a organizațiilor. Profilurile tipice PSITI și cele particulare rezultante PISI, simple și transparente, permit diferitelor entități implementarea, gestionarea eficientă și îmbunătățirea continuă a SecInf, ceea ce, la rândul său, conduce la atingerea mai sigură a obiectivelor de afaceri.

Aplicația instrumentală informatică de suport M^{3}SI simplifică și ușurează esențial gestionarea SecInf , automatizând operațiile rutinare de administrare a bazei de date cu cunoștințele despre amenințări *(care exploatează vulnerabilitățile și duc la pierderi de active),* riscuri, cerințe și controale specifice, de generare a profilurilor particulare, de evaluare a nivelului de maturitate și urmărire a progresului. Aplicația M^{3}SI este de tip **web cu acces controlat**. Toate acestea luate împreună permit diferitelor entități *organizarea, abordarea și gestionarea eficientă a securității informației,* prevenirea și combaterea mai eficientă a riscurilor și amenințărilor în adresa securității informației, compararea maturități în timp și/sau între entități tipice.

Aprobarea rezultatelor cercetării. Rezultatele științifice obținute de autor în cadrul tezei au fost prezentate în cinci rapoarte la trei conferințe științifice internaționale diferite și au fost publicate în trei reviste diferite, una din România și două reviste de categoria B, incluse în Registrul Național al RM privind revistele de profil. Pentru detalii a se vedea lista publicațiilor la tema tezei.

Volumul și structura tezei. Teza este scrisă în limba română cu titlu de manuscris, tehnoredactată și imprimată la calculator. Lucrarea este structurată în *introducere, 3 capitole, concluzii generale și recomandări, bibliografie* și *anexe.*

Capitolul *„1. Analiza stării actuale a securității informației în sectorul bancar al Republicii Moldova”* face o trecere în revistă a stării SC, identifică unele probleme și provocări majore legate de SC, cadrul legal și de reglementare a SecInf în băncile comerciale ale RM, justifică actualitatea și problematica cercetării. **Capitolul** *„2. Aspecte teoretice, metodologice și practici de abordare a securității informației prin prisma SMSI”* prezintă succint aspectele teoretice, metodologice și practice de abordare a SecInf, precum și abordări moderne a SecInf bazate pe standarde de bune practici, pe riscuri și pe modele de maturitate, principalele direcții și recomandări de organizare și îmbunătățire continuă a SMSI. **Capitolul** *„3. Model multiprofil de maturitate a securității informației M^{3}SI”* prezintă esența inovativă a cercetării prin abordarea modernă a SecInf în baza standardelor deschise, modelelor de maturitate multinivel, multidimensionale, cu suport informatic, cu generarea modelelor tipice unor industrii PSITI și a modelelor PISI particularizate, individualizate în acord cu politicile corporative concrete, standardele directoare a familiei ISO/IEC27k, valorile țintă ale criteriilor de evaluare a maturității SecInf.

CONȚINUTUL TEZEI

Capitolul „*1*. *Analiza stării actuale a securității informației în sectorul bancar al Republicii Moldova (RM)”* justifică actualitatea și identifică unele probleme majore comune legate de SecInf/SC în băncile comerciale ale RM, elucidează noua paradigmă de abordare a SecInf prin prisma SMSI. Acestea sunt legate, în principal, de accesul de la distanță la mijloacele aflate în contul clientului în scopul obținerii de informații privind starea contului, efectuarea de plăți, alimentarea contului și alte tranzacții electronice prin Sisteme/Servicii Automatizate de Deservire la Distanță *(SADD)* puse la dispoziția clientului de bancă fie prin internet-banking, fie prin mobile-banking. SADD sunt utilizate pentru efectuarea de plăți preponderent în mod electronic cu carduri bancare, eventual cu bani virtuali *(e-/web-many)*, sisteme de e-banking, Internet/online banking, mobile-banking și/sau automate bancare/ATM și/sau sisteme automate de auto-deservire *(POS terminale/Point of Sale)* și/sau terminale *„Self-service”*. **Una din principalele sarcini a tezei rezumă în identificarea criteriilor unice comune de creștere a nivelului de maturitate a SecInf**, pornind de la cadrul legal unic al activității sectorului bancar din RM, a principalelor aplicații, instrumente și soluții informatice precum și a provocărilor moderne de SC.

Cadrul legal și de reglementare al sectorului bancar din Republica Moldova elucidează succint conceptul de SecInf și setul de Legi importante, regulamente ale BNM și regulamente interne ale BC, ce prescriu crearea și îmbunătățirea continuă a SMSI ca mijloc de gestionare și asigurare eficientă a SecInf în domeniul bancar.

Pentru buna funcționare mecanismele de SecInf trebuie să fie capabile să facă față unei game largi de riscuri, atacuri, amenințări, accidente, care trebuie tratate în mod previzibil, simultan și/sau post factum, cu asumarea conștientă a riscurilor, în limita unor costuri raționale, suportabile.

SecInf este definită ca **conservarea celor trei proprietăți fundamentale ale informației**, în orice formă a sa electronică, pe suport hârtie etc., referite în literatura de specialitate ca **triada CIA**. Caracteristicile CIA sunt definite în ISO/IEC 27000:2018 [1]: ***Confidențialitate*** *(clauza 3.10),* ***Integritate*** *(clauza 3.36),* ***Disponibilitate*** *(clauza 3.7).*

Definițiile de SecInf și SC sunt aproximativ aceleași în majoritatea surselor, e.g. sunt identice în ISO/IEC 27000:2018, ISO/IEC 27032:2012. Iar pentru a corespunde modificărilor ISO/IEC 27001:2022, care și-au extins titlu *„Securitatea informațiilor”* spre *„Securitatea informațiilor,* ***securitatea cibernetică și protecția vieții private”*** în versiunea ISO/IEC 27032:2023 *(cl.3.6)*, SC este definită ca *„****protecția oamenilor, societății, organizațiilor și națiunilor împotriva riscurilor cibernetice”.*** Totodată, SecInf/SC se referă și la alte atribute secundare, asigurate în baza celor fundamentale, precum **posesia informației** *(cine este stăpânul, posesorul,*

responsabilul), **utilitatea informației** *(sau semnificația, cu atât mai mare, cu cât informația este mai valoroasă, mai accesibilă),* **autenticitatea informației** *(clauza 3.6), (informațiile neautentice constituie dezinformații),* **contabilizarea** *(în engleză accountability, de exemplu pentru justificarea achitărilor reciproce)*, **non-repudierea** *(sau imposibilitatea dezicerii de unele acțiuni efectuate, e.g. plasarea unei comenzi, clauza 3.48)* și **fiabilitatea** *(clauza 3.55)* a standardului referit mai sus.

De regulă, **SecInf/SC este asigurată în cadrul unor SMSI proprietare**, care variază în funcție de industrie, domeniul și obiectul de activitate al organizației, strategiile și politicile interne în acord cu reglementările în vigoare și cadrul legal aferent. Iar realizarea SMSI presupune seturi de controale *(preventive, detective, corective)* și proceduri operaționale, ce asigură caracteristicile primare și secundare ale informației, protecția tuturor activelor și resurselor informaționale din cadrul entității, inclusiv personal, tehnologii informaționale și comunicaționale, servicii de suport etc. pentru a ține sub control riscurile și incidentele de SC la un nivel acceptabil prestabilit.

Sectorul bancar în Republica Moldova funcționează pe două niveluri: la primul nivel este Banca Națională a Moldovei și la al doilea sunt 11 bănci comerciale (https://bnm.md/ro/content/bancile-licentiate-din-republica-moldova/). Specificul tezei este axat pe SADD, serviciile TIC, plăți cu carduri, e-banking etc., reglementate la nivel național de un set de legi și regulamente. O listă completă a regulamentelor specifice activității BNM și BC a se vedea la adresa https://www.bnm.md/ro/content/lista-regulamentelor. Versiunile oficiale, îndeosebi a legilor în vigoare, sunt disponibile la https://www.legis.md/.

La nivel global activitățile BC sunt reglementate de standardele-pereche ISO/IEC 27001:2022 [2] și ISO/IEC 27002:2022 [3], ISO/IEC 27032:2023, GDPR [4], PCI DSS versiunea 4.x din noiembrie 2023 [5] și altele *(detalii a se vedea în teză)*.

Scopul SMSI pentru o BC este de a oferi o viziune clară referitor la sistemele de protecție și prevenire a atacurilor asupra informației și activelor informaționale sub orice formă. Principalele cerințe de securitate a informației, de stabilire a SMSI, de implementare și funcționare a SMSI, de monitorizare și revizuire a SMSI, de menținere și îmbunătățire a SMSI, de documentare a SMSI sunt expuse în *Regulamentul cu privire la sistemele de control intern în bănci*, secțiunea 3, clauzele 33-37 și în secțiunea 4, cerințe privind auditul intern al SMSI (https://www.legis.md/cautare/getResults?doc_id=49565&lang=ro).

Principalele elemente arhitecturale, sarcini ale SMSI și logica funcționării a se vedea *(Fig. 1)*. Acesta reflectă abordarea procesuală PDCA a SMSI în ciclul de analiză a performanței și îmbunătățirea continuă conform misiunii, strategiei generale de afaceri și a politicilor de securitate.

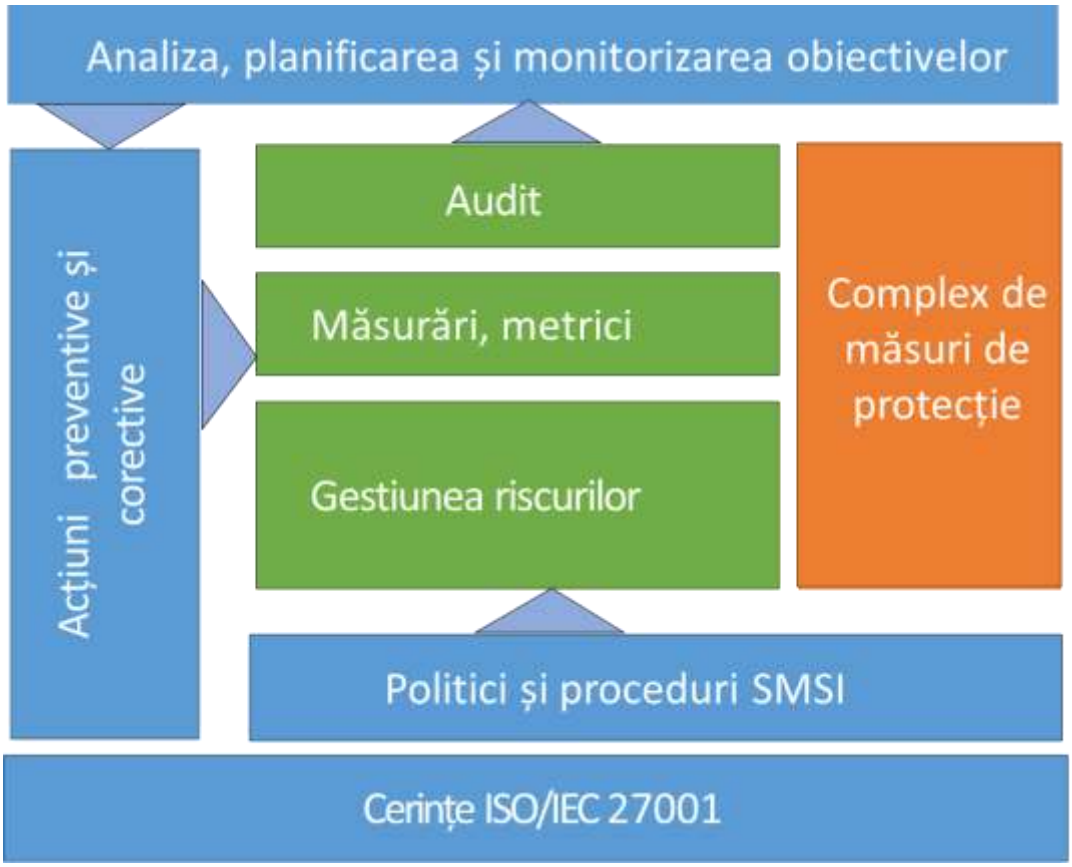


Figura 1. Principalele componente și logica funcționării SMSI

Obiectivele SMSI rezidă în a asigura că băncile dispun de o strategie adecvată aferentă TIC, aliniată la strategia generală de afaceri; că procesele de guvernanță internă sunt stabilite adecvat în raport cu sistemele IT/IS; că cadrul intern de gestionare a riscurilor IT/IS și de control intern protejează în mod adecvat sistemele IT/IS; că sistemul de plăți online este conform cu standardul internațional de securitate a datelor din industria cardurilor de plată PCI DSS; că sunt respectate drepturile privind protecția datelor cu caracter personal conform Legii RM nr. 133 din 2011 [6] și GDPR [4] din 2016 cu aplicare din 2018.

Cerințele de bază față de SecInf, SC, SMSI sunt în permanentă îmbunătățire cu scopul asigurării concordanței cu prevederile legislației, inclusiv cu Directivele UE, cu Regulamentul BNM cu privire la sistemele de control intern în băncile din RM etc. într-un mediu/spațiu cibernetic aflat în continuă schimbare.

Un SMSI veritabil trebuie să posede un set de caracteristici obligatorii [2], e.g.: *să fie bine documentat/stabilit în scris; să asigure îndeplinirea cerințelor clienților; să asigure atingerea obiectivelor organizației în condiții de siguranță; să fie aplicabil în toate activitățile organizației* și altele. Detalii privind cerințele, inclusiv de planificare, suport, operare, audit intern sistematic de performanță, controalele/măsurile de securitate, metricile a se vedea, de exemplu [2-4], [7-8].

SMSI acoperă trei zone largi de resurse pentru asigurarea SecInf, prezentate în *(Fig. 2).*



Figura 2. Trei zone largi de resurse gestionate în cadrul SMSI

Domeniile de management ale SMSI sunt realizate prin **procese, politici, proceduri, structuri organizatorice, software și hardware** pentru a proteja activele informaționale.

Tipul controalelor/măsurilor de securitate sunt conforme cu ISO/IEC 27002:2022 [3]: **Preventive**, cu scopul de a preveni apariția unor incidente de securitate a informațiilor; **Detective,** care acționează atunci când are loc un incident de SecInf/ SC; **Corective,** care acționează după ce are loc un incident de SecInf/ SC.

Conform cerințelor ISO/IEC 27001 [2], **SMSI este un sistem documentat,** bazat pe dovezi, înscrisuri etc. cu structurarea documentației SMSI în forma „piramidală" pe niveluri, care sugerează volumul, conținuturile, personalul implicat *(Fig. 3)*.

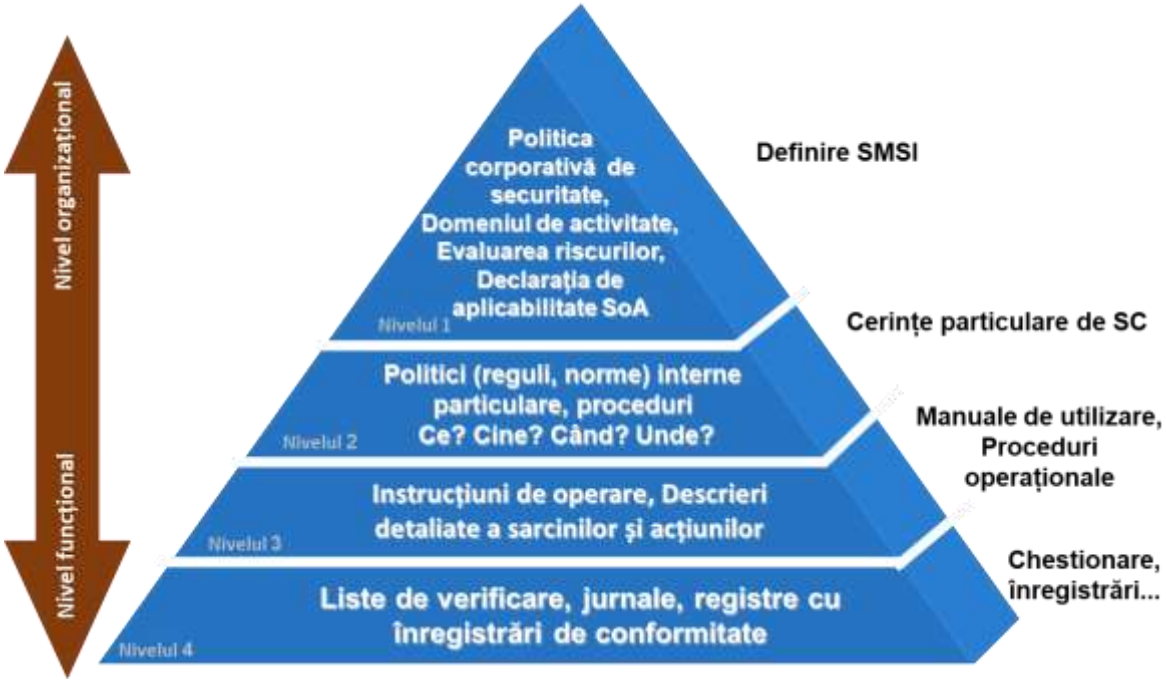


Figura 3. Documentele SMSI

Conformitatea cu standardul internațional de securitate a datelor din industria cardurilor de plată PCI DSS [5] este o cerință obligatorie pentru toate organizațiile care stochează, procesează tranzacțiile cu carduri bancare și este benevolă pentru cele care doar utilizează sisteme de plăți electronice. În RM avem ambele tipuri de bănci. Conform Legii 133 [6] a RM și la nivelul UE GDPR [4], asemenea date trebuie protejate, stocate, procesate, prelucrate dezvăluite de către diferite organizații și entități doar în anumite condiții legale, și doar dacă există garanții speciale prescrise.

Importanța, provocările și problemele majore de SecInf în activitatea bancară sunt confirmate de **vitalitatea informației** în societățile moderne, **evaluat la nivelul celui de al patrulea element vital după apă, aer și foc**. Conform NIST, ISO, IEC, ITU și altor organisme internaționale preocupate de domeniul SecInf și aprobarea bunelor practici, informația a devenit un bun fundamental al organizației, statului, societății, care trebuie protejat corespunzător. Iar TIC a devenit elementul esențial în crearea, procesarea, stocarea, transmiterea, protecția și distrugerea informației. Pe de altă parte, evoluția rapidă a TIC, a e-afacerilor, e-educației, e-guvernării, e-distracțiilor, Smart Home, IoT, IoB etc. duce la creșterea concomitentă a riscurilor informaționale și a modului în care instituțiile statului, organizațiile private, persoanele individuale și societatea în întregime ar trebui să răspundă provocărilor și oportunităților create de revoluția tehnologică. În teză sunt aduse date convingătoare privind **pierderile în urma atacurilor cibernetice** asupra SecInf *(Fig. 4, [8])*, o listă cuprinzătoare a statisticilor și tendințelor poate fi consultată la [8].

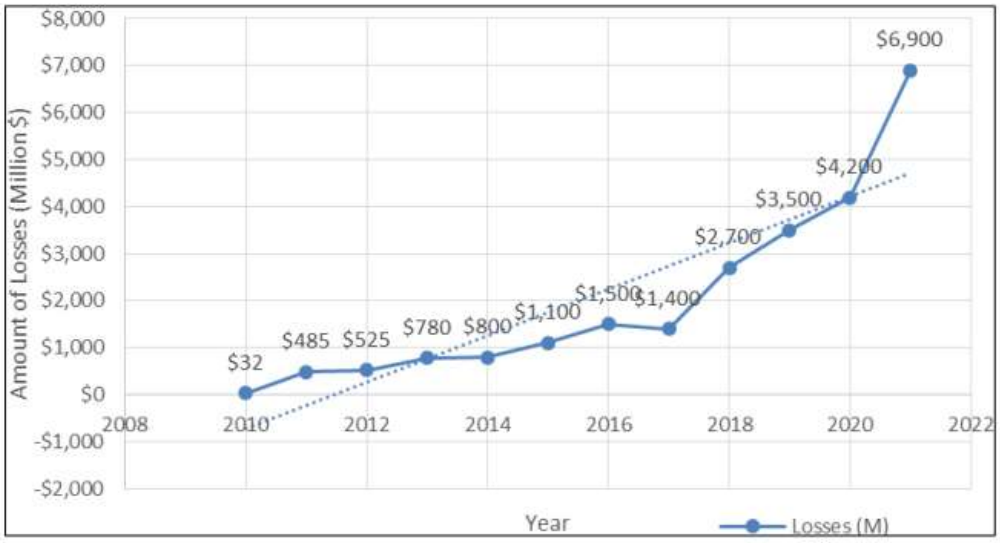


Figura 4. Valoarea pierderilor din atacurile cibernetice în anii 2010-2021, S.U.A.

Conform statisticilor, criminalitatea informatică rămâne a fi o amenințare perpetuă pentru interesele naționale și economice ale țărilor și corporațiilor. Iar securitatea informației a devenit esențială, atât pentru persoane fizice și juridice, cât și pentru societate și stat în întregime, ca

componentă semnificativă a securității naționale și regionale. Costurile crimelor cibernetice în cinci ani, din 2018 pană în 2022 au crescut de peste 13 ori, de la 0,86 la 8, 44 trilioane USD. Estimarea creșterii pentru următorii 5 ani, din 2022 pană în 2027 este de peste trei ori, de la 8,44 la 23,82 trilioane USD *(Fig. 5, [9]).* Ca urmare, gestionarea adecvată a securității informației și a siguranței tranzacțiilor electronice are o importanță crucială și devine un element esențial al bunelor practici informaționale bazate pe TIC.

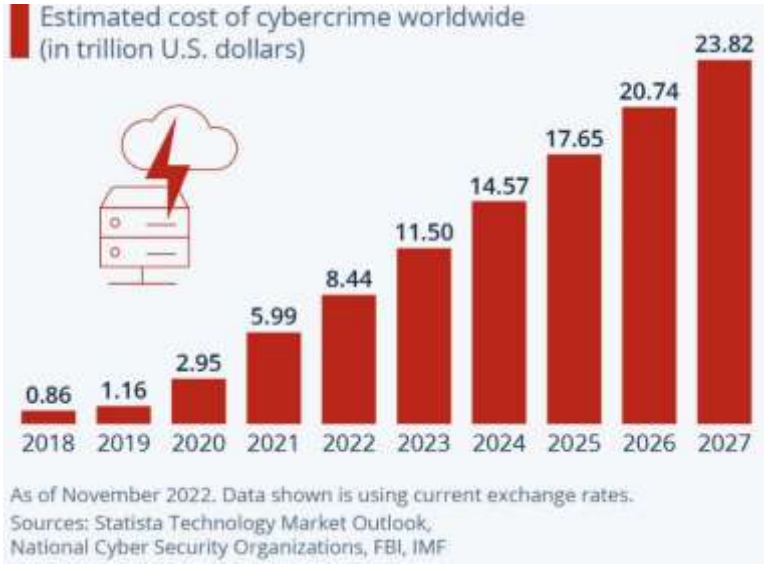


Figura 5. Creșterea costurilor crimelor cibernetice

Amenințările, riscurile, atacurile și incidentele de SecInf se materializează prin **exploatarea vulnerabilităților** care pot proveni în cea mai mare parte din trei surse principale:

- **Omul,** prin acțiuni sale voite sau nu, e.g. pierderea sau furtul sau distrugerea unui laptop cu informații sensibile, atacuri efectuate de hackeri asupra unui site, sistem etc.;
- **Infrastructura critică**, tehnologiile și sistemele de suport ale afacerilor (rețele informatice și comunicaționale, serverele, dispozitivele, inclusiv periferice, IoT, IoB, inclusiv software-ul incorporat în toate acestea), incapabile de a menține respectivele funcții din cauza penelor, exploatării vulnerabilităților etc.;
- **Natura**, e.g. calamități naturale, incendii, inundații.

Un set minim de resurse informaționale ce trebuie protejate pentru a diminua nivelul de fraudă și amenințărilor asupra SecInf se referă, îndeosebi, la mediul IT/IS:

- **Personal** (angajați, clienți, furnizori);
- **Active tangibile** (documente, date, cunoștințe, expertize, înregistrări);
- **Active fizice IT/IS** (echipamente, computere, routere, discuri etc.);
- **Software** (de sistem, aplicativ, web, personale/comerciale, SGBD etc.);
- **Servicii IT/IS** (interne, externe, Internet Service Provider etc.);

- **Locații** (sedii, inclusiv virtuale, site-uri web etc.).

Lupta cu complexitatea SecInf în entități este susținută de metode, instrumente și tehnici destinate, asistate de calculator care, cu timpul au devenit mult mai numeroase și mai accesibile din punct de vedere financiar.

Sunt de menționat **aplicațiile instrumentale de securitate a informațiilor**, pornind de la programe antivirus *(e.g. Top 10 cele mai bune teste antivirus gratuite [10])* și terminând cu instrumente de pre-audit a SC *(e.g. Top CIS/SANS Controls v.8 [11], CSAT [12], CMMC [13], Evaluarea gratuită a securității cibernetice [14], Cadrul de securitate cibernetică NIST [15]).* Utilizarea acestora și altor instrumente profesionale specializate ajută entitățile la eliminarea scurgerilor de informații, realizarea de pre-audit al SC *(depistarea punctelor vulnerabile, planificarea și realizarea îmbunătățirilor continue etc.)* și permit a face față sarcinii din ce în ce mai complexe de asigurare a securității informațiilor. **Asemenea programe instrumentale încep să fie implementate și în companiile cu un număr relativ mic de angajați.**

Un instrument util în alegerea produselor software poate fi **Pătratul magic interactiv de la Gartner** [16]. Caracteristicile interactive ale Pătratului magic permit generarea unor vederi personalizate prin ajustarea ponderilor aplicate fiecărui criteriu de evaluare, specifice utilizatorului, salvarea și partajarea aceste vederi pentru analize interne și luarea deciziilor.

În concluziile capitolului 1 este elucidată dominanta dezvoltării lumii contemporane în cadrul societății moderne, exprimată prin e-transformarea, schimbarea continuă a valorilor, structurilor, fenomenelor, proceselor, modului de a lucra, învăța, a se distra etc.; prin utilizarea masivă TIC, Internet și Web în toate domeniile activității umane, dezvoltarea economiei digitale și competitivitatea sporită a e-afacerilor; creșterea semnificației informației, estimată la nivelul celui de-al patrulea element vital după apă, aer și foc, informația devenind unul dintre cei mai importanți factori ai progresului social; hiper-conectivitatea rețelelor corporative, IoT, IoB, și rețele Wi-Fi la Internetul global. Toate acestea duc la sporirea atacurilor cibernetice și confirmă că SecInf/SC a devenit o problemă critică pentru succesul afacerii și necesită abordarea sa transversală, în adâncime, aliniată la strategiile și obiectivele afacerii.

În capitolul 2 sunt examinate unele aspecte teoretice, metodologice și bune practici de abordare a SecInf în cadrul SMSI cu scopul de **a justifica alegerea modului de abordare a SC prin modele multiprofil de maturitate**. Sarcina de bază constă în acordarea cerințelor ISO, NIST, ISACA, CMMI etc. privind SecInf cu cerințele, necesitățile organizației și contextele concrete ale sistemelor de management al calității, continuității activității, incidentelor (evenimentelor) de securitate. Această sarcină este confirmată de noua ediție a standardelor-pereche ISO/IEC 27001:2022 [2] și ISO/IEC 27002:2022 [3], care și-au extins cel mai de sus titlu de la *„Securitatea*

informațiilor” la „*Securitatea informațiilor*, **securitatea cibernetică și protecția vieții private***”*, subliniind integrarea ISO/IEC 27001:2022 cu ISO/IEC 27032:2023 [17].

În cadrul tezei este elocvent demonstrat că standardele de bune practici din domeniul securității informației constituie fundamentul, temelia pentru conceperea și dezvoltarea unui model multiprofil de măsurare a maturității securității informației. Unele dintre aceste cadre sunt menționate în *(Fig. 6).*

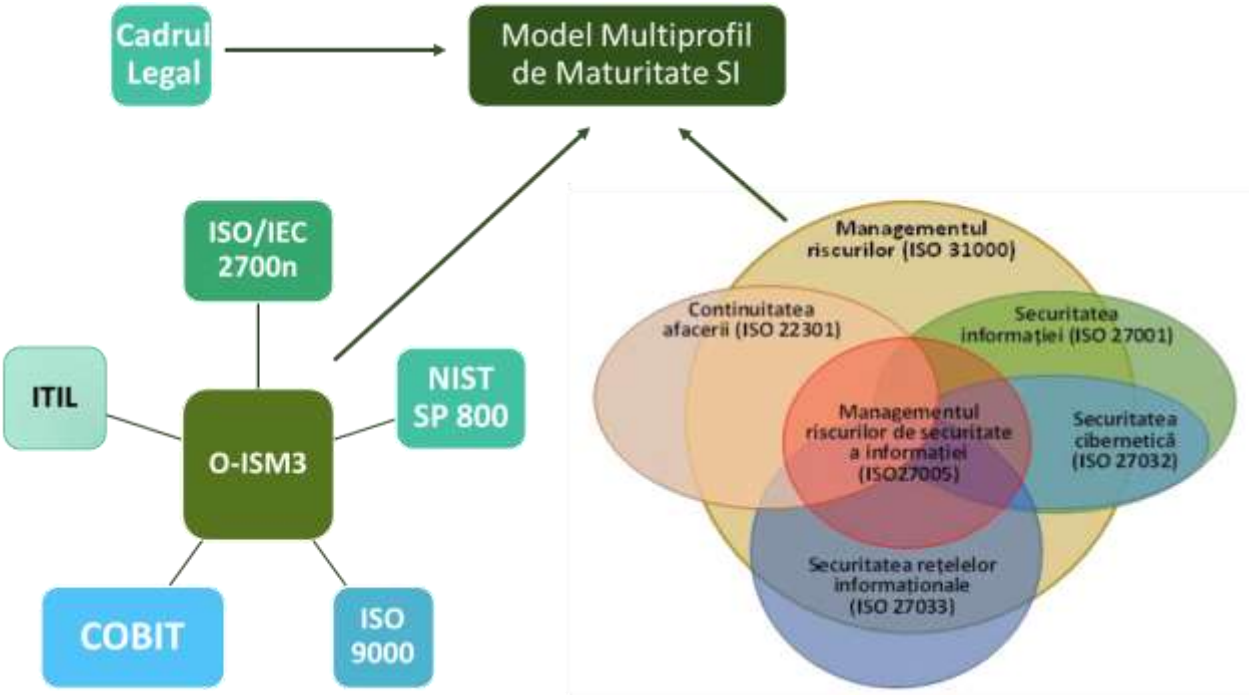


Figura 6. Corelarea unor standarde de bune practici pentru realizarea M^{3}SI

În baza corelării standardelor de bune practici a fost dezvoltat modelul generic de maturitate, din care sunt generate profiluri de securitate a informației tipice unor industrii PSITI, adaptate inițial pentru sectorul bancar. Acest profil servește ca bază pentru profilurile individuale PISI, concepute pentru evaluarea SecInf a băncilor din RM. Este de menționat că **modelele sunt suficient de versatile** pentru a fi implementate și în alte sfere de activitate, cum ar fi sectorul educațional, structuri guvernamentale, servicii medicale etc. Principalul aport al modelelor este că organizațiile din diverse sectoare în baza evaluării calitative a nivelurilor de maturitate pot trece la evaluarea cantitativă a securității informației, care să le conducă spre un nivel de protecție optimizat și aliniat la cele mai recunoscute standarde internaționale, reglementări naționale și locale.

În toate cadrele/standardele de bune practici ca cerințe-cheie ale SecInf sunt formulate **principiile de bază**, precum: **abordarea procesuală PDCA, îmbunătățirea continuă, orientarea spre client, angajamentul și susținerea conducerii de vârf, implicarea personalului, luarea deciziilor bazată de dovezi, managementul relațiilor cu părțile**

interesate. Totodată, în realizarea SecInf sunt utilizate o serie de alte principii și paradigme, printre care **abordarea bazată pe risc [18], arhitectura zero trust (ZTA) [19], privilegii minimale, securitate prin design, apărarea în profunzime, paradoxul lui Mayfield** și altele.

Paradoxul lui Mayfield [20] este reprezentat grafic prin două curbe asimptotice în spațiul bidimensional, **curba riscurilor** și **curba investițiilor** cu costul sistemului pe axa verticală și cota persoanelor ce poate accesa sistemul pe axa orizontală, cu un optim în punctul de întretăiere a curbelor *(Fig. 7)*. Paradoxul subliniază că **acces perfect** *(fără restricții de securitate)* **și securitate perfectă** *(fără restricții de acces)* **sunt cazuri extremale** cu costuri ce tind la infinit, între care trebuie găsit un optim. Ca ilustrare a Paradoxului Mayfield poate fi adusă regula/principiul Pareto pentru echilibrarea cost-securitate a măsurilor de SC.

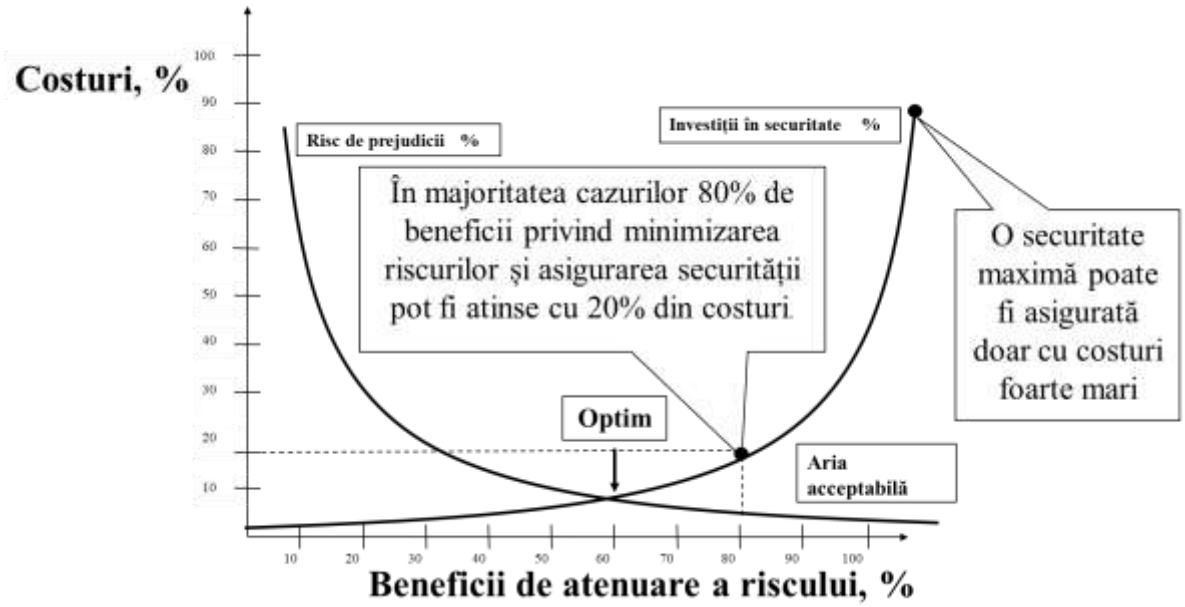


Figura 7. O ilustrare a paradoxului Mayfield pe diagrama de echilibrare

Or, la un moment dat, securitatea suplimentară devine nerealist de costisitoare, la fel cum și adăugarea de utilizatori suplimentari devine nerealist de scumpă, iar diferența dintre aceste două costuri este relativ mică. Semnificația acestui paradox constă în **corelarea riscurilor cu bugetul de securitate în mod realist**, confirmat și de principiul SMSI privind tratarea doar a informațiilor valoroase pentru o entitate în atingerea obiectivelor urmărite:

- Deplasarea spre dreapta față de optim semnifică o investiție în viitor;
- Deplasarea spre stânga față de optim semnifică o rămânere în urmă.

La nivel global, cele mai răspândite și recunoscute cadre/bune practici de abordare a SecInf/SC sunt:

- ISO/IEC 27001:2022 și familia ISO27k, o normă internațională formatoare cu circa 80 de standarde operaționale dintre cele 100 planificate, care definesc cerințele pentru

conceperea și administrarea unui SMSI, aspectele de securitate logică, fizică și organizațională, precum și recomandările de bune practici;

- COBIT 2019 *(Control OBjectiv for IT, [21])* de la ISACA *(Information Systems Audit and Control Association);*
- Cadrul elaborat de National Institute of Standards and Technology *(NIST S.U.A., [22])* în seria de publicații speciale NIST SP 800.x;
- Modelul Open Information Security Management Maturity Model *(O-ISM3, 2017, [18], [19]),* dezvoltat de către consorțiul independent The Open Group, care este compatibil cu/și ține cont de cerințele ISO27k, COBIT, ITIL și altele.

Toate acestea subliniază **abordarea holistică a SecInf/SC bazată pe risc**, **pe modele de maturitate adaptabile/**personalizabile a unor procese prescrise, **pe cultura organizațională** de securitate etc. Adaptabilitatea modelor se referă la dimensiunea și complexitatea organizației, sectorul de activitate, alocarea resurselor, reactivitate la schimbările tehnologice din mediul de afaceri, alinierea cu tehnologiile emergente și modele de lucru etc. Importanța nivelurilor de maturitate constă în faptul că ele **oferă un cadru pentru evaluarea situației curente pentru stabilirea obiectivelor de îmbunătățire și pentru măsurarea progresului.** Ca urmare, organizațiile alocă resurse în mod eficient, concentrându-se pe domeniile cu cele mai mari riscuri sau pe cele care necesită îmbunătățiri urgente. Un model personalizabil permite prioritizarea inițiativelor de securitate bazate pe evaluarea riscurilor specifice organizației, asigurându-se că bugetul și eforturile sunt direcționate acolo unde pot avea cel mai mare impact. Focusarea pe îmbunătățire continuă încurajează entitățile să urmărească constant îmbunătățirea practicilor și proceselor de securitate a informației, promovând un ciclu de îmbunătățire continuă. Or, **securitatea informației nu este un obiectiv static, ci un proces dinamic** care necesită adaptare continuă la noile amenințări, tehnologii și schimbări ale mediului de afaceri.

Formarea continuă și conștientizarea personalului este vitală pentru a asigura că toți membrii organizației înțeleg riscurile de securitate și contribuie la protecția informațiilor. De regulă, formarea și conștientizarea este diferită pentru diferite categorii de personal.

O semnificație deosebită în acest capitol revine abordării securității informației bazată pe riscuri. Procesul de **gestiune a riscurilor este un proces ciclic, continuu și sistematic** *(Fig. 8, realizată de autor în traducere din [23]),* cu responsabilități stabilite de identificare, evaluare/măsurare, monitorizare și adoptare de măsuri de control cu două puncte decizionale, fie prin asumarea expunerii la risc, fie prin tratamentul suplimentar pentru a diminua valoarea riscului rezidual până la nivelul acceptabil.

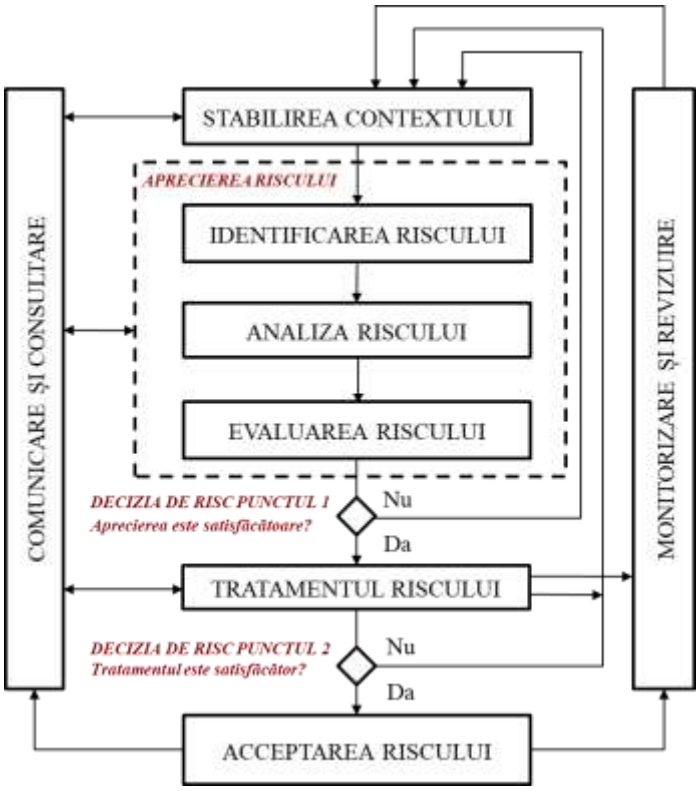


Figura 8. Procesul de analiză și gestionare a riscurilor de SecInf

Fluxul general de analiză și tratare conform ISO 27005:2022 *[23]* include stabilirea contextului *(Clauza 7*), aprecierea riscului *(Clauza 8),* tratarea riscului *(Clauza 9),* acceptarea riscului *(Clauza 10),* comunicarea și consultarea riscului *(Clauza 11),* monitorizarea și revizuirea riscului *(Clauza 12).* Totodată, activitățile necesare pentru analiză riscurilor cibernetice prezentate în *(Fig. 8)* sunt descrise în detalii și în alte standarde, precum ISO 27001:2022 [2], ISO 31000:2018, NIST SP-1800 și altele.

Analiza, evaluarea și tratarea riscurilor cibernetice se concentrează pe metode de analiză calitativ-cantitative în baza standardelor ISO/IEC 27005 [23] și ISO 31000:2018, având ca țintă lupta cu complexitatea și diminuarea influenței factorului uman prin automatizarea analizei riscurilor în măsura posibilă. Riscurile de securitate sunt analizate în funcție de probabilitatea apariției riscului și de gravitatea, impactul asupra obiectivelor în cazul în care apare riscul. Pentru trecerea de la valori calitative la valori cantitative ale probabilității, impactului, valorii și nivelului de risc sunt utilizate valori semi-cantitative, descrise în *Tablele A.1-A.5* ISO/IEC 2705:2022 [23] și *Tablele 1-2* [24] .

Etapa finală a procesului de evaluare a riscurilor este **raportul de evaluare**, care să sprijine managementul în luarea deciziilor adecvate privind bugetul, politicile, procedurile de SC.

După încheierea evaluării și aprecierii riscului, valoarea riscului este comparată cu criteriile convenite de acceptare a riscului și este realizata tratarea riscului, rezumând un risc rezidual

(Fig. 9). Decizia de tratare se ia în conformitate cu matricea de analiză a riscului *(Fig. 10, elaborată în baza Tabelului A.3 [23])*. Proprietarul riscului trebuie să aprobe tratarea riscurilor selectate și trebuie să accepte riscul rezidual conform criteriilor prestabilite.

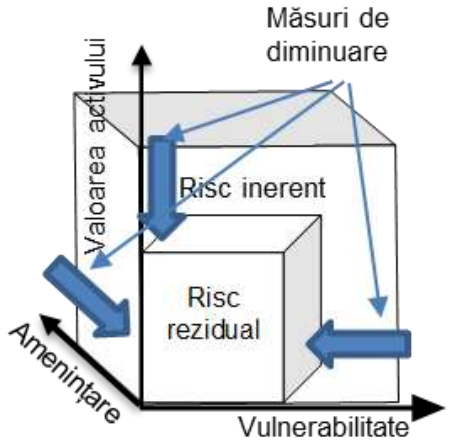


Figura 9. Risc rezidual vs risc inerent

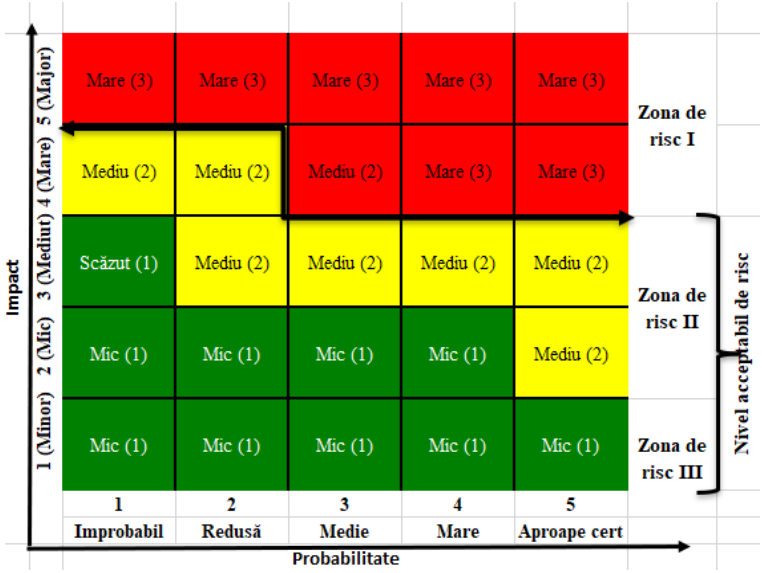


Figura 10. Matricea 5x5 de apreciere a riscurilor pe 3 niveluri

În digrama din Figura 10 zona din partea de dreapta-sus (colorată cu roșu) sunt riscuri cu probabilitate mare și impact mare, pentru care trebuie aplicate controale de diminuare a valorii riscului, iar în stânga-jos *(colorată cu verde)* – cu probabilitate mică și impact mic, care pot fi ignorate *(nu afectează grav afacerea*). Zona de mijloc *(colorată cu galben)* sunt riscuri cu probabilitate medie și impact mediu, care pot fi tratate conform criteriilor politicii de securitate.

Capitolul „3. Model multiprofil de maturitate a securității informației M^{3}SI” prezintă partea inovativă, originală a tezei de abordare a SecInf în baza standardelor deschise, modelelor de maturitate multinivel, multidimensionale, cu suport informatic, cu generarea modelelor tipice unor industrii PSITI și a modelelor PISI particularizate, individualizate în acord cu politicile corporative concrete, standardele directoare ale familiei ISO/IEC27k, valorile țintă ale criteriilor de evaluare a maturității SecInf.

Maturitatea este **o măsură a capacității unei organizații de îmbunătățire continuă** a unor domenii de management *(O-ISM3, 2017 [18], Muneer, 2023 [19]).* Iar modelele de maturitate reprezintă **colecții de bune practici pentru măsurarea progresării entității** de la niveluri inferioare spre niveluri mai înalte de aptitudine sau de „maturitate”. În esență, modelele de maturitate reprezintă seturi de bune practici globale aprobate, care permit organizațiilor să construiască și să facă referință la capabilitățile-cheie, care abordează cele mai comune provocări ale afacerii lor. Deși marea majoritate a modelelor de maturitate existente, e.g. O-ISM3 [18, 19], COBIT [21], ITIL, ISO 9001:2015 etc. în general sunt compatibile cu cerințele ISO/IEC

27001:2022, nu există o înțelegere clară a relaționării domeniilor și proceselor de bază folosite de către acestea. Spre deosebire de aceste diferite cadre de bune practici/standarde internaționale și modelele de maturitate izolate, **modelul multiprofil al maturității securității informației M^{3}SI elaborat în cadrul tezei oferă o imagine universală unică și integră asupra SecInf**, aplicabilă pentru orice entitate, la orice nivel, pornind de la cadrul global/național de reglementare și bune practici, continuând cu cerințele specifice pentru diverse industrii PSITI și terminând cu nivelul de aplicare local/profiluri individuale PISI, specifice cerințelor și contextelor particulare concrete al unei organizații și/sau a unei subdiviziuni a acesteia și/sau a unei misiuni etc.

Ideea inovativă realizată în cadrul tezei prin M^{3}SI se referă și la **relaționarea model general-model tipic industriei-model personalizat** cu diferite cadre de abordare a SecInf. O entitate poate porni de la clonarea unui cadru existent ca PSITI, după care urmează adaptarea acestuia conform legislației în vigoare. Astfel, M^{3}SI are la bază cele mai bune practici de securitate a informației/cadre normative de reglementare cunoscute la moment și deja amintite mai sus, *e.g. OISM3:2017, NIST SP 800-53 ediția 5, NIST 800-207 Zero Trust Architecture, ISO/IEC 27001:2022, ISO/IEC 27002:2022, PCI-DSS versiunea 4.x, COBIT:2019 etc.*

Într-o oarecare măsură M^{3}SI a anticipat modificarea ISO/IEC 27001 și ISO/IEC 27002, ediția III din 2022, în care au fost schimbate numele standardelor: *din „ISO/IEC 27001:2013 Tehnologia Informației – Tehnici de securitate – Sisteme de management a Securității Informației" în „ISO/IEC 27001:2022* ***Securitatea informațiilor, securitatea cibernetică și protecția vieții private*** *– Sisteme de management al Securității informațiilor.* Această modificare subliniază **abordarea unică a celor trei tipuri de securitate**, menționate în titlul standardului și maparea mai facilă a diferitelor controale de securitate cu diferite cerințe și standarde, apropierea conceptelor de securitate etc.

M^{3}SI este oferă o flexibilitate înaltă, astfel încât permite adăugarea, eliminarea, modificarea de noi cunoștințe structurate privind amenințările și riscurile existente, controalele și metricile preconizate pentru evaluarea nivelului de maturitate a SecInf. M^{3}SI este însoțit de o aplicație instrumentală software, care permite generarea profilurilor de securitate a informației tipice unor industrii/PSITI, e.g. educație, bănci, medicină și particularizate în profiluri de securitate individuală a informației/PISI la nivel de entitate concretă, e.g. Universitatea de Stat din Moldova, Bancă comercială „Alfa Bank", sau la nivel de subdiviziuni sau zone/sfere separate, e.g. zona departamentului de plăți electronice al băncii comerciale sau zona de securitate a sistemelor informatice cu cerințe specifice contextului intern/extern. O viziune ierarhică simplificată a M^{3}SI a se vedea *(Fig. 11).*

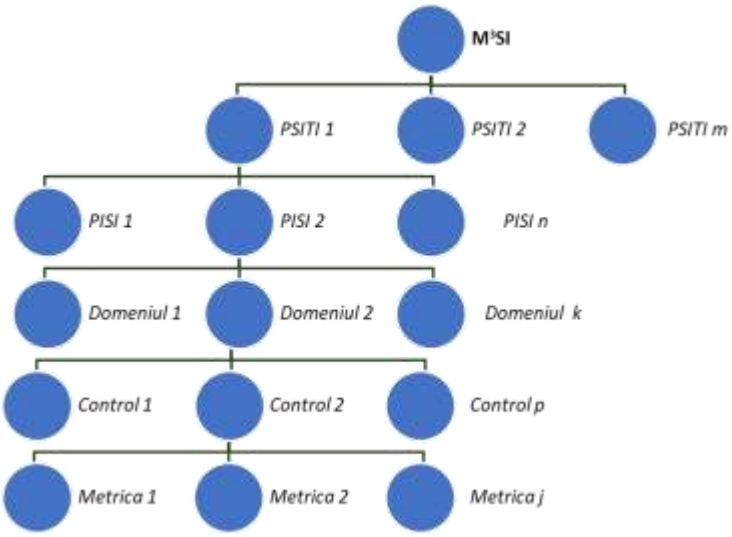


Figura 11. O viziune ierarhică simplificată a modelor de maturitate în M³SI

La cel mai de sus nivel, M³SI include un oarecare număr prestabilit de domenii de SC, stabilit conform cadrelor generale de abordare corelate prin cartografiere. Modelul multiprofil acoperă mai multe ramuri industriale cu modele tipice PSITI, care, la rândul acoperă entități tipice cu modele similare PISI *(Fig. 12).*

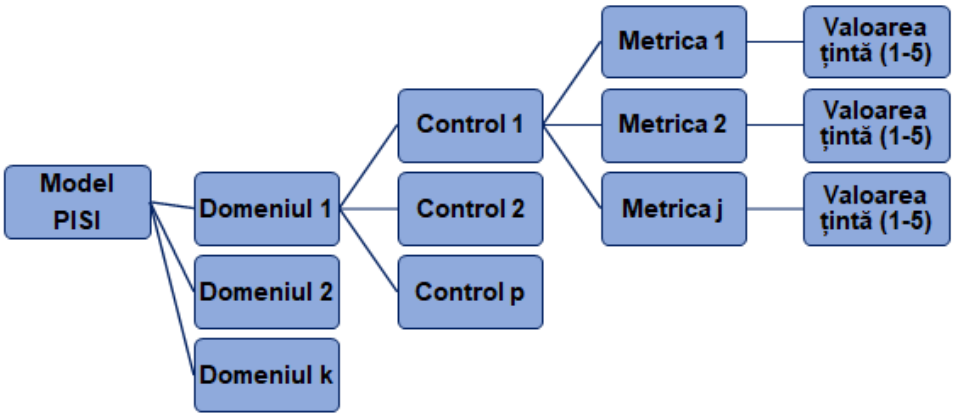


Figura 12. O viziune a profilurilor PISI

De regulă, particularitățile modelelor tipice pentru diverse industrii PSITI sunt formulate în standarde și reglementări specifice, *e.g. PCI DSS, GDPR,* acte global aplicabile, *e.g. HIPAA* și reglementări locale ale organelor de supraveghere. Profilul de maturitate PSITI ar putea specifica aceste cerințe pentru satisfacerea necesităților managementului.

Modelul PSITI nu este menit să ofere răspunsul definitiv la întrebarea cât de bun este un SMSI individual, ci servește ca suport de structurare a unui SMSI individual sau a unui profil particular de SC sau pentru compararea maturității diferitelor entități tipice.

Deoarece măsurile și controalele securității sunt derivate din situațiile statice și/sau dinamice concrete de funcționare ale organizației și misiunii evaluării, PISI ar trebuie particularizate/interpretate de la caz la caz în baza unui PSITI sau a unui PISI similar. Orice entitate

concretă își va crea propriul profil PISI conform contextului său specific, care va ține cont de aria SMSI/SoA și de țintele stabilite. Fragmente de PSITI și PISI a se vedea (*Fig. 13, Fig. 14).*

ID	Nume Control	Descriere	Risk	Niveluri de Maturitate	Actiuni
1	+ Cadrul de organizare a securității informației				
2	+ Managementul resurselor informaționale				
3	+ Securitatea Resurse Umane				
4	- Securitatea fizică și a mediului de lucru				
4.1	Zone de securitate	să prevină accesul fizic neautorizat, distrugerile și pătrunderile în interiorul băncii, precum și accesul la resursele informaționale.		1. Controalele sunt doar partial definite si/sau executate intr-un mod inconsecvent 2. Controalele sunt in vigoare si executate doar intr-un mod structurat si consecvent, dar informal 3. Controalele sunt documentate si executate intr-un mod structurat, formal si dovedit 4. Eficacitatea controalelor este evaluata si verificata periodic pentru calitate 5. A fost creat un sistem ecologic care sa asigure un control continuu si eficient si sa rezolve riscurile	Editeaza Sterge
4.2	Securitatea echipamentelor	să prevină pierderea, distrugerea, furtul sau compromiterea echipamentelor TI și întreruperea proceselor de activitate ale băncii.		1. Controalele sunt doar partial definite si/sau executate intr-un mod inconsecvent 2. Controalele sunt in vigoare si executate doar intr-un mod structurat si consecvent, dar informal 3. Controalele sunt documentate si executate intr-un mod structurat, formal si dovedit 4. Eficacitatea controalelor este evaluata si verificata periodic pentru calitate 5. A fost creat un sistem ecologic care sa asigure un control continuu si eficient si sa rezolve riscurile	Editeaza Sterge
5	+ Managementul comunicațiilor și operațiunilor				
6	+ Controlul accesului la resursele informaționale				
7	+ Achiziționarea, dezvoltarea și mentenanță sistemelor de aplicații				
8	+ Managementul incidentelor de securitate a informației				
9	+ Managementul continuitatii activitatii				
10	+ Conformitatea				
11	+ Auditul intern al securității informației				

Figura 13. Un fragment de PSITI pentru activitatea bancară din Republica Moldova

ID	Nume Control	Descriere	Nivel curent	Evidente
1	- Cadrul de organizare a securității informației		3.25	
1.1	Politica de securitate a informației	să asigure orientarea generală de management și sprijinul pentru securitatea informației în conformitate cu cerințele de afacere, legislația și actele normative aplicabile.	3	lista
1.2	Organizarea SMSI	să asigure cadrul intern adecvat pentru managementul securității informației.	4	lista
1.3	Relația cu terțele părți	să asigure securitatea informației în relația cu terțele părți care prestează sau beneficiază de servicii ce implică informația băncii	3	lista
1.4	Externalizarea serviciilor TI	să asigure securitatea și continuitatea serviciilor TI externalizate către furnizori externi de servicii.	3	lista
2	- Managementul resurselor informaționale		2.67	
2.1	Responsabilitatea pentru resurse	să asigure stabilirea și asumarea responsabilității pentru protecția corespunzătoare a resurselor informaționale ale băncii.	3	lista
2.2	Clasificarea informației	să asigure faptul că informația beneficiază de un nivel de protecție adecvat, proporțional importanței ei, reglementărilor aplicabile și amenințărilor aferente	2	lista
2.3	Managementul riscurilor	să asigure faptul că banca isi gestioneaza riscurile intr-o maniera eficace si eficienta	3	lista
3	- Securitatea Resurse Umane		3.00	
3.1	Înainte de angajare	să asigure faptul că noii angajați, terțele părți, precum și reprezentanții acestora sunt corespunzător verificați înainte de acordarea accesului la sisteme, iar responsabilitățile pentru securitatea informației sunt adecvat stabilite, comunicate și asumate.	4	lista
3.2	Instruirea	să asigure faptul că cerințele de securitate sunt cunoscute în măsură suficientă de către angajații băncii, terțele părți, precum și reprezentanții acestora.	3	lista
3.3	Pe perioada angajării	să asigure faptul că cerințele de securitate sunt respectate necondiționat de către angajații băncii, terțele părți, precum și de reprezentanții acestora, iar responsabilitățile și răspunderea juridică ale acestora sunt stabilite și conștientizate corespunzător.	3	lista
3.4	Încetarea contractului sau schimbul locului de muncă	să asigure faptul că angajații, terțele părți, precum și reprezentanții acestora încetează relația cu banca într-o manieră controlată din punct de vedere al riscurilor de securitate.	2	lista
4	- Securitatea fizică și a mediului de lucru		3.50	
4.1	Zone de securitate	să prevină accesul fizic neautorizat, distrugerile și pătrunderile în interiorul băncii, precum și accesul la resursele informaționale.	4	lista
4.2	Securitatea echipamentelor	să prevină pierderea, distrugerea, furtul sau compromiterea echipamentelor TI și întreruperea proceselor de activitate ale băncii.	3	lista

Figura 14. Un fragment de PISI pentru o bancă ipotetică

În afară de *Domenii/Arii* și *Controale* PISI mai conține: *Nivelul de maturitate așteptat; Nivelul de maturitate identificat; Lista de probe și argumente de rigoare atașate*, care documentează nivelul de maturitate identificat. În ultimă instanță, rezultatul evaluării conform

PISI permite identificarea etapelor/pașilor de îmbunătățire continuă a securității informației. Totodată, este posibilă și acumularea istoricului privind domeniile și îmbunătățirile incrementale, care pot apărea în entitatea analizată de la o lună la alta, de la un trimestru la altul sau de la un an la altul, în funcție de frecvența impusă de cerințele afacerii.

Aplicația M^{3}SI este concepută pentru a face față provocărilor și complexității SecInf și diferă calitativ de alte instrumente răspândite prin:

a) **Sintezarea și sistematizarea** cunoștințelor despre diverse cadre de SecInf și instrumente/chestionare de evaluare, inclusiv definirea celor cinci niveluri de maturitate într-o singură bază de date cumulativă adaptabilă și extensibilă;
b) **Aplicabilitatea universală a aplicației**, pornind de la controalele ISO/IEC 27001:2022, care pot fi extinse/restrânse, e.g. la Top 20 CIS Controls [11], orientate preponderent spre Internet; CMMC, orientate preponderent spre securitatea cibernetică; PCI DSS, orientate la tranzacțiile cu carduri bancare și altele;
c) **Acumularea istoricului** evaluării nivelurilor de maturitate ale entității conform unor PISI și misiuni particularizate, urmărirea progresului, dinamicii etc.;
d) **Asigurarea comparabilității evaluărilor** din contul formalizării criteriilor de evaluare și a metricelor de SecInf.

Pentru a utiliza aplicația ce integrează modelul generic M^{3}SI, PSITI și PISI, utilizatorul trebuie:

1. **Să definească aria de aplicabilitate** a SMSI sau a misiunii de evaluare, pornind de la modelul tipic industriei, prin eliminarea/adăugarea/modificarea unor controale specifice în M^{3}SI și PSITI, dictate de necesitățile și constrângerile organizației.

2. **Să genereze profilul individualizat** de maturitate al securității informației PISI *(Eventual prin identificarea unui PISI similar/apropiat și adaptarea lui sau prin construirea inițială a PISI prin combinarea domeniilor de control și controalelor aferente în conformitate cu riscurile și amenințările caracteristice pentru industria și entitatea dată).*

3. **Să completeze răspunsurile șa lista de întrebări** și/sau să selecteze metricile criteriilor respective *(din meniurile derulante de pe paginile fiecărui control, inclus în PISI).* În baza răspunsurilor la fiecare întrebare *(alegerii unor opțiuni din listele derulante sau a introducerii rezultatelor măsurărilor criteriilor de evaluare)* aplicația determină în mod automat scorurile nivelului de maturitate conform metricilor furnizate pe controale și domenii, după care afișează „Raportul” rezultant al evaluării ca **diagrame de tip radar și/sau diagrame detaliate sub forma unor bare color** pe domeniile de control conform scării/culorilor matricei de analiză a riscurilor [23].

4. **Să realizeze recomandările de îmbunătățire** bazate pe evaluarea realizată/raportul rezultant. Scorurile obținute sunt utilizate fie pentru a măsura progresul organizației, fie pentru a formula obiective/sarcini de îmbunătățite, fie pentru a diminua riscurile conform nevoilor și constrângerilor clienților și ale organizației, fie pentru a asigura trecerea evolutivă în trepte de la un efort ad-hoc individual *(nivelul inițial al maturității)* la o abordare organizațională consistentă și optimizabilă de îmbunătățire continuă a SC *(cel mai înalt nivel de maturitate)*.

Pașii scenariului de utilizare M^{3}SI includ actualizarea PISI *(eventual și a bazei de cunoștințe)* conform misiunii, realizarea evaluării, documentarea și afișarea rezultatelor evaluării. Interfața web-aplicației M^{3}SI este intuitivă, ușor de utilizat și după lansarea inițială afișează două zone de operare, Zona 1 și Zona 2, care este structurată în trei subzone 2.1-2.3 *(Fig. 15)*.



Figura 15. Viziune de ansamblu a interfeței M^{3}SI

Prima zonă *(din stânga)* conține o listă a meniurilor funcționale. Acestea pot fi utilizate prin selectarea și activarea tradițională a lor prin ***Click*** când cursorul este plasat pe obiectul selectat sau prin tastarea ***Enter***. Obiectul selectat este evidențiat prin text de culoare albastră. **Zona 2,** spațiul de lucru, este locul principal pe ecran în care se afișează toate exemplarele obiectului selectat și posibilitățile de manipulare cu acestea. Această zonă are trei subzone: lista obiectelor cu unele caracteristici de identificare *(zona 2.1),* posibilitățile de manipulare/**Acțiuni** precum clonarea, ștergerea, editarea cu obiectul selectat, la fel sunt evidențiate prin culoare *(zona 2.3, Fig. 15)*: **Editare** nume și tip obiect – de culoare verde și **Ștergere** – de culoare roșie, în partea dreaptă a ecranului. Tot în această zonă pot fi editate înregistrările, atributele cadrelor de bune practici, pot fi introduse datele de evaluare etc. prin activarea butonului de culoare albastră cu numărul de înregistrări al obiectului selectat *(zona 2.2, Fig. 15).*

Baza de date (BD) a modelului M^{3}SI întrunește cunoștințele despre cele mai bune practici, modele, standarde, instrumente de SecInf care se aplică la nivel global, național și local. Conținutul principal al BD îl constituie cunoștințele despre ariile și controalele de SecInf/SC, preluate și

adaptate din cele mai răspândite cadre de abordare a SecInf, precum OISM3:2018, NIST SP:2018, familia ISO 27k, inclusiv ISO/IEC 27001:2022, ISO/IEC 27004, ISO/IEC 27032:2023, ISO/IEC 27033 (2012-2016), PCI DSS versiunea 4.x, COBIT:2019, ISO/IEC 20000-1:2018, ITIL versiunea 4:2019 și **adaptate de** autor pentru necesitățile aplicației. **Aportul important al autorului** în realizarea conținutului bazei de cunoștințe constă nu doar în sintetizarea lor ci și în **definirea criteriilor de evaluare pe cele cinci niveluri de maturitate**.

Exemple de afișare a rapoartelor sub forma grafică a se vedea *(Fig. 16).*



Figura 16. Exemple de afișare grafică sumară a evaluării BC „Alfa”

Cele două suprafețe colorate pe diagrama radar semnifică scorul – ținta curentă (albastru) și scorul real curent – culoare violetă pe ariile de control. Raportul în formă grafică este util în toate cazurile misiunilor de audit al SecInf *(intern de performanță, pre-audit de certificare)* sau de analiză vizuală a decalajelor și de planificare a îmbunătățirilor sub forma unei viziuni integratoare, pe o pagină.

Pe fiecare dintre arii/domenii de control sunt afișate diagrame grafice de tip bare. Acestea sunt utile pentru analize punctuale, e.g. pentru justificarea unor proiecte în baza analizei decalajelor. În Figura 17 sunt afișate două asemenea domenii, fiecare cu câte cinci controale, barele de culoare albastră reflectând valorile țintelor iar de culoare roșie valorile reale ale controalelor. După cum se poate observa din *(Fig. 17)* entitatea are mari rezerve de îmbunătățire pe controlul *ID.03. Super utilizatori* al domeniului *Managementul accesului* și rezerve moderate pe domeniul *Guvernanță,* controalele *GU.01 Strategie; GU.02 Politici; GU.03 Plan/Foaie de parcurs* și *GU.04 Arhitectura informațiilor întreprinderii*.

Pentru alte detalii privind rapoartele de evaluare și afișările grafice a se explora aplicația. De regulă, fiecare PISI are propriile sale metrici, orientate spre atingerea obiectivelor

specifice. Iar determinarea maturității se bazează pe revizuirea documentației SMSI, intervievarea personalului, efectuarea unor măsurători, a unor analize a discrepanței pentru fiecare dintre domeniile de securitate incluse în PISI și valorile măsurate.

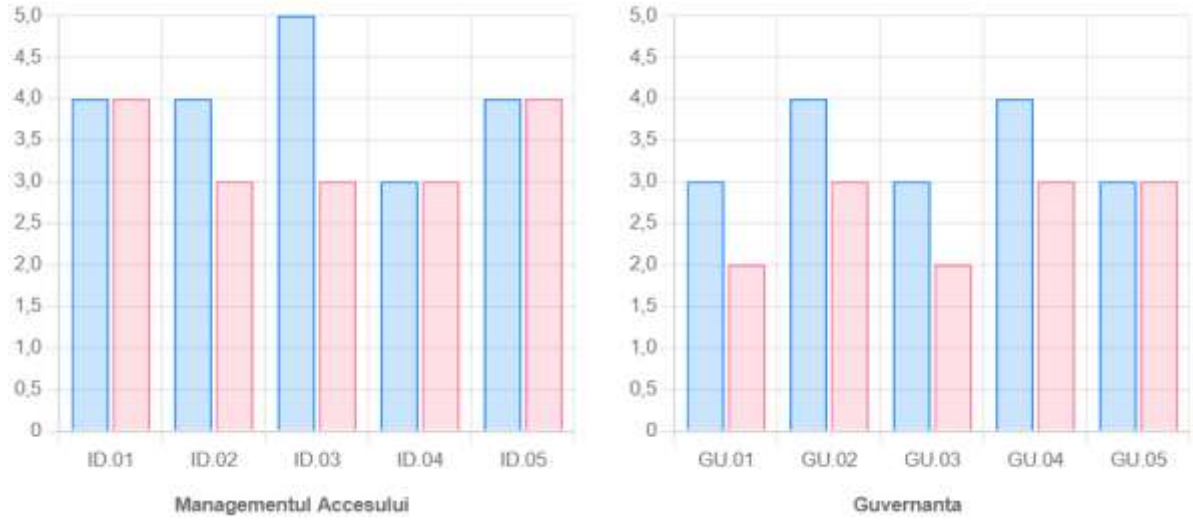


Figura 17. Exemplu de afișare detaliată pe domenii separate

Evaluarea nivelurilor pentru fiecare dintre domeniile PISI se realizează conform criteriilor elaborate/metricilor modelului. De exemplu, scorul de măsurare a îndeplinirii criteriului poate fi „*Conform”, „Conform parțial”, „Neconform”*. În cazul când criteriul specificat are mai multe metrici și acestea au fost apreciate cu valori diferite, scorul sumar este apreciat, de regulă la nivelul metricii cu valoarea cea mai scăzută, fie cu o valoare medie.

În final, platforma M^{3}SI posedă o serie **de avantaje și caracteristici inovative**:

1. Este o **platformă integrată de concepere, dezvoltare, evaluare și îmbunătățire continuă a SecInf**; o **metodă practică și un instrument** de determinare a riscurilor de SecInf.

2. **Aplicația de suport generează și afișează rezultatul evaluării sub formă de diagrame vizuale**, care înlesnesc analiza decalajelor. În baza acestora Consiliul de conducere, auditorii și organele de supraveghere obțin informații obiective, consistente, calitative asupra stării SecInf și justifică deciziile sale.

3. **Ofițerii de SecInf și echipele de profesioniști** de securitate TI/SI/Cibernetică etc. **elimină o mare parte a rutinei** privind planificarea sarcinilor de viitor.

4. Platforma M^{3}SIpermite **acumularea istoricului, evoluției domeniilor de SecInf și a îmbunătățirilor incrementale**, care pot apărea în entitatea analizată de la o lună la alta, de la un trimestru la altul sau de la un an la altul, în funcție de frecvența impusă de cerințele afacerii.

5. Platforma M^{3}SI, accesibilă la adresa https://www.m3-si.eu/, **permite analiza comparativă a maturității entităților tipice**, precum bănci, universități, spitale etc.

CONCLUZII FINALE ȘI RECOMANDĂRI

În cadrul tezei **au fost analizate starea SecInf/SC în diferite entități, pierderile și provocările în adresa SC,** în special din sectorul bancar, au fost identificate unele probleme, care pot fi depășite prin schimbarea paradigmei abordării SecInf, orientată sper management.

La fel **au fost analizate diverse cadre global recunoscute de abordare a SecInf** cu scopul de a **sinteza și justifica un model de maturitate integrator**, care să permită utilizarea tuturor celor mai bune practici. Baza de cunoștințe a modelului M^3SI întrunește ele mai recomandate abordări bazate pe standardele de bune practici global acceptate, precum COBIT de la ISACA, ISO 27k de la ISO, seria NIST SP 800.x, PCI DSS și abordarea bazată pe riscuri.

În realitate, multor entități le este greu să obțină o viziune unică, obiectivă, comprehensibilă a tuturor riscurilor și capacităților de securitate cibernetică, aceasta necesitând mult timp, competențe și expertize speciale, de care entitățile nu totdeauna dispun. **Complexitatea este un factor foarte important în realizarea unei viziuni unice și obiective a riscurilor și capacităților de SecInf**. Inclusiv și pentru că riscurile sunt în creștere continuă, cauzată de integrarea noilor aplicații TIC practic în toate sferele activității umane, de apariția noilor vulnerabilități, noilor amenințări, atacuri. Inclusiv și pentru că gestiunea riscurilor **SecInf este un proces continuu**, care ar trebui să permită organizației să-și atingă obiectivele de afaceri stabilite **într-un mediu în continuă schimbare**.

Deși este un proces destul de complex și cu multă rutină, managementul riscurilor duce la creșterea nivelului de maturitate a SecInf și a organizației în întregime. În acest sens **cele mai bune practici cu cele mai relevante recomandări sunt cele din standardul ISO/IEC 27005**. Acestea țin de evaluarea riscurilor bazată pe analiza calitativă a probabilității prin calificative de genul: *5 – Aproape sigur; 4 – Foarte probabil; 3 – Probabil; 2–Puțin probabil; 1 – Improbabil* și a impactului de tipul *5 – Catastrofal, 4 – Critic, 3 – Serios, 2–Semnificativ, 1 – Minor,* în linii mari similare celor cinci niveluri de maturitate. De la care se trece la calculul valorii riscului ca produs dintre probabilitate și impact, la sortarea riscurilor în ordinea descrescătoare a valorii lor și tratării conform strategiilor adoptate.

Securitatea cibernetică implementată corect în condițiile telelucrului în masă și a accesului de la distanță a informațiilor sensibile presupune o noua abordare orientată nu doar pe soluții tehnice-tehnologice, pe TIC și pe sisteme informaționale tradiționale, dar și pe securitatea dispozitivelor mobile, de domiciliu cât și pe securitatea IoT, IoB, cloud etc., inclusiv pe schimbarea abordării sistemelor de management, care ar permite controlul și monitorizarea eficientă a riscurilor cibernetice.

O altă problemă semnificativă este și **modul în care informațiile privind securitatea cibernetică sunt colectate, gestionate, raportate/difuzate și utilizate** de către rolurile respective din entități, monitorizarea și suportul în timp real al cărora care este destul de dificil. **Evaluarea și urmărirea securității informatice prin colectarea și înregistrarea „manuală”** a informațiilor pe foi de calcul sau alte instrumente pentru a urmări numeroasele amenințări, inițiative/proiecte, programe și procese de securitate, alinierea SecInf la numeroasele cadre legale, cadre de abordare și diferite reglementări **nu mai sunt eficiente**. Devine extrem de dificilă nu doar colectarea de date și evaluarea, ci și actualizarea și păstrarea consistenței numeroaselor documente pentru obținerea unei imagini coerente asupra tuturor aspectelor securității informației, compararea și analiza evoluției în timp și/sau între entități.

Pentru soluționarea problemelor enumerate și nu doar, în cadrul tezei a fost creat un prototip de planificare-evaluare a SecInf în baza unui model multiprofil de maturitate M^3SI, cu profiluri tipice PSITI și profiluri individuale PISI, cu criterii și proceduri prestabilite de evaluare, ceea ce permite diferiților evaluatori să ajungă aproximativ la aceleași rezultate. Modelul este susținut de o aplicație informatică originală care reduce volumul muncii de rutină.

Toate acestea fac gestionarea și asigurarea SecInf în cadrul entităților sau unor conglomerate de entități din același domeniu de activitate mai transparentă, mai simplă și mai ușor de înțeles și de aplicat.

Într-adevăr, pe de o parte, contextele interne și externe pot diferi esențial pentru diferite entități și, ca urmare, nu poate exista un singur model de evaluare a maturității. Fiecare model PISI urmărește propriile obiective și rezolvarea propriilor probleme conform misiunii. Pe de altă parte, este dificil să se aplice modele de maturitate personalizate fără a înțelege modelul de bază/enunțul general al problemei, profilurile tipice industriei și modurile de abordare. Concepute pentru a optimiza performanța securității unei entități într-un mediu global în continuă schimbare, **modelul multiprofil M^3SI, profilurile tipice unor industrii PSITI, profilurile particulare PISI de evaluare a SecInf și aplicația aferentă, oferă îndrumare și suport organizației pentru îmbunătățirea proceselor de SecInf,** inclusiv capacitatea de gestionare, dezvoltare, achiziționare și întreținere a controalelor, instrumentelor, produselor și serviciilor de SecInf. Toate acestea ajută organizația la evaluarea nivelului de maturitate, la stabilirea priorităților de îmbunătățire și punerea în aplicare a acestor îmbunătățiri în contexte și procese specifice unei entități.

În esența sa, **M^3SI reprezintă o bază de date generică, cumulativă, adaptabilă și extensibilă** privind cunoștințele despre cadrele de abordare, zonele, controalele, criteriile și țintele de SecInf, din care sunt generate profiluri tipice unor industrii PSITI (e.g. educație, sănătate,

bănci), care, la rândul lor servesc ca bază pentru construirea/generarea de profiluri particulare PISI, bazându-se inclusiv și pe acumularea experienței entităților similare, cu profiluri similare.

Cu M^{3}SI și aplicația de suport maturitatea poate fi evaluată sistematic, mai larg sau mai îngust, mai concret pentru a identifica, sesiza decalajele, „punctele de plecare" și a aplica modelul la o gamă mai largă de sarcini și situații, sau mai larg **pentru a planifica schimbările într-un mod mai coordonat și mai rezonabil**, **inclusiv pentru a compara nivelurile de maturitate la diferite momente de timp și/sau nivelurile de maturitate ale diferitelor entități** cu activități similare etc.

În realitate, **cele cinci niveluri de maturitate semnifică etape prin care trece un SMSI lansat**. PISI face referință la capacitățile-cheie ale SMSI, controale, teste/chestionare, șabloane tipice, bune practici de evaluare și măsurare a nivelului de maturitate stabilite în diverse cadre de abordare și standarde global recunoscute, precum ISO, NIST, ISACA etc. Iar criteriile, la fel sunt stabilite în baza bunelor practici, sunt destinate **pentru aprecierea** (măsurarea-evaluarea) și **îmbunătățirea continuă a SecInf,** care să răspundă atât propriilor nevoi și politici particulare de securitate a informației specifice organizației, cât și celor globale. Aplicația aferentă M^{3}SI oferă suport inteligent de generare a profilurilor de evaluare consistentă pentru maturizarea SecInf prin îmbunătățirea continuă precum și diferite moduri de afișare a rapoartelor, potrivite mai bine cu scopul măsurării maturității, precum urmărirea dinamicii în timp sau auditul intern de performanță sau pre-audit de certificare etc.

Abordarea **„model multiprofil – profil tipic industriei – profil particular specific entității"** și aplicația respectivă M3-SI (https://www.m3-si.eu/) de suport automatizat este utilă atât pentru rolurile specifice de securitate, care trebuie să fie la curent cu starea actuală, să întrețină documentele necesare, să asigure raportarea/informarea, cât și pentru toți cei care au nevoie de acces la informațiile de securitate, precum auditori, inspectori și manageri.

În perspectivă **M^{3}SI ar putea colabora cu alte instrumente similare**, gen CIS CSAT, C2M2 etc., inclusiv la nivelul de import/export de date și afișarea rapoartelor integrate obținute din datele comune.

Implementarea rezultatelor. Modelul elaborat M^{3}SI și web aplicația de suport au fost implementate în BNM, confirmată printr-un *Act de implementare,* cu ilustrarea practică pentru o bancă ipotetică „Alfa" *(Ilustrarea în baza unei bănci reale ar fi încălcat SecInf pentru acea entitate).* Dar modelul M^{3}SI și aplicația aferentă pot fi aplicate în mod direct pentru orice bancă din RM, cu adaptarea necesară a profilurilor PISI; inclusiv și pentru orice alte industrii și entități cu mici adaptări doar a conținutului bazei de date și/sau a profilurilor PSITI și PISI.

BIBLIOGRAFIE

Toate sursele web, inclusiv din textul tezei, au fost verificare la data de 28.02.2024.

[1] *ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary*

[2] *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*

[3] *ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls*

[4] *Regulamentul General privind Protecția Datelor (GDPR) nr. 2016/679, aprobat de Parlamentul European și Consiliul UE din 27 aprilie 2016, aplicabil din 25 mai 2018.* Available: https://gdpr-info.eu/

[5] *The Complete Guide to PCI-DSS 4.0.* Available: https://colortokens.com/blog/pci-dss-4-0/

[6] *Lege Nr. LP133/2011 din 08.07.2011 privind protecția datelor cu caracter personal, adoptată de Parlamentul RM, cu modificări LP52 din 12.03.20, MO84/14.03.20 art.88; în vigoare din 14.03.2020*

[7] *ISO/IEC 27004:2016. Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation*

[8] 239 Cybersecurity Statistics (2023). Available: https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/

[9] FLECK, A. *Cybercrime expected to skyrocket in coming years. Dec 2, 2022.* Available: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[10] *Cele mai bune teste antivirus gratuite 2024.* Disponibil: https://top10programeantivirus.com/cel-mai-bun-antivirus-gratuit/

[11] *CIS Controls Version 8. (CIS/SANS TOP 20 Security Controls).* Available: https://www.cisecurity.org/controls/v8/?utm_source=website&utm_medium=email&utm_campaign=v8_release/

[12] *CIS Controls Self-Assessment Tool (CIS CSAT).* Available: https://csat.cisecurity.org/

[13] *Cybersecurity Maturity Model Certification v.1.02. (CMMC 1.2, 2020).* Available: https://www.acq.osd.mil/cmmc/draft.html/

[14] *Free assessment of your cyber security defenses.* Available: https://www.itgovernance.co.uk/free-assessment-of-your-cyber-security-defences

[15] *The NIST Cybersecurity Framework (CSF) 2.0 (2024).* Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf/

[16] *Gartner Magic Quadrant.* Available: https://www.gartner.com/en/research/methodologies/magic-quadrants-research

[17] *ISO/IEC 27032:2023. Cybersecurity – Guidelines for Internet security*

[18] The Open Group. *Open Information Security Management Maturity Model (O-ISM3, 2017),* Version 2.0. Available: https://www.opengroup.org/forum/security/infosecmanagement/

[19] MUNEER, A. et al *A Balanced Information Security Maturity Model Based on ISO/IEC 27001:2013 and O-ISM3. International Journal of Innovative Science and Research Technology, Volume 8, Issue 6, June, 2023, p,2444-2450. ISSN No:-2456-2165*

[20] MAYFIELD, R., CVITANIC, J. *Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security*. Information Systems Control Journal, 2, 2001, ISACA. p. 32-35

[21] *COBIT® 2019 Framework: Governance and Management Objectives*. ISACA, 2019. -300 p. Available: https://www.iso27001security.com/html/iso27000.html/

[22] NIST National Institute of Standards and Technologies. *Special Publication 800 series, Computer security.* Available: https://csrc.nist.gov/publications/sp800

[23] *ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks*

[24] **BRICEAG, V.**, BRAGARU, T. *Evaluarea riscului securității cibernetice.* Revista Economica, 2(122), SEP ASEM, 2021, pp. 138-147. ISSN 1810-9136

[25] *Amenințări generice la adresa securității cibernetice.* ENISA (2020). Disponibil: https://dnsc.ro/vezi/document/amenintari-generice-securitate-cibernetica/

[26] *CVE (Common Vulnerabilities and Exposures, 2021).* Available: https://cve.mitre.org/

[27] *Cybersecurity Maturity Model Certification Guide (CMMC, 2022).* Available: https://www.varonis.com/blog/cmmc-compliance/

[28] *Cybersecurity Capability Maturity Model (C2M2, version 2.1, 2022).* Available: https://c2m2.doe.gov/C2M2%20Version%202.1%20June%202022.pdf

LISTA PUBLICAȚIILOR LA TEMA TEZEI

1. BRAGARU, T., **BRICEAG, V.**, MALCOCI, V., GALAICU V. (2019). *Securitatea informației vis-a-vis de securitatea informațională.* Revista Studia *Universitatis* Moldaviae, 2(122), seria „Științe exacte și economice", CEP USM, 2019, pp. 38-47. ISSN 1857-2073; ISSN online 2345-1033
2. BRAGARU, T., **BRICEAG, V.** *Evaluarea securității informației organizației în baza unui model de maturitate*. IN: Materialele conferinței științifico-practice internaționale „Teoria și practica administrării publice", Chișinău, AAP, 22 mai 2020, pp.248-252. ISBN 978-9975-3240-9-0
3. **BRICEAG, V.**, BRAGARU, T. *Evaluarea riscului securității cibernetice.* Revista Economica, 2(122), SEP ASEM, 2021, pp. 138-147. ISSN 1810-9136
4. **BRICEAG, V.** Inteligent support for assessing the level of maturity of information security. International Conference „Mathematics & Information Technologies: Research and Education" (MITRE - 2021). Abstracts. Chișinău: CEP USM, 2021. -p.94. ISBN 978-9975-158-19-0. Available: https://ibn.idsi.md/vizualizare_articol/134317
5. **BRICEAG, V.**, BRAGARU, T. Sustainable Curricular assurance of the information security management course. International Conference „Mathematics & Information Technologies: Research and Education" (MITRE - 2021). Abstracts. Chișinău: CEP USM, 2021. -p.118. ISBN 978-9975-158-19-0.
6. BRAGARU, T., **BRICEAG, V**. Sustainable cybersecurity training for modern society. Sustainable cybersecurity training for modern society. Proceeding of International Teleconference of young researchers "Creating the Society of Consciousness" (TELE-2022), 11th Edition, 18-19 March 2022. ARA Journal of Sciences, Nr. 5, 2022, pp.30-41. ISSN: 0896-1018. Available: https://www.americanromanianacademy.org/_files/ugd/754172_0c407fa356a04c2a8a000f6a3f92bae8.pdf
7. BRAGARU, T., **BRICEAG, V.** Sustainable cybersecurity training for modern society. The thesis of International teleconference of young researchers "Creating the Society of Consciousness" (TELE-2022), 11th Edition of 18-19 March 2022. Society. Consciousness. Computer. Volume 8 (2022). Editorial Office "Vasile Alecsandri University of Bacău", Romania, Bacău, 2022, p.32. ISSN 2359-7321. Available: https://ibn.idsi.md/vizualizare_articol/179237
8. **BRICEAG, V.** *Model Multiprofil de Maturitate a Securității Informației (M^3SI).* Revista Română de Informatică și Automatică (RRIA), ISSN 1220-1758, vol. 32, nr. 1, pp. 99-112. ICI București, 2022. Disponibilă la: https://rria.ici.ro/en/vol-32-no-1-2022. ISSN 1220-1758

ADNOTARE

BRICEAG Valentin: „Analiza și creșterea nivelului de maturitate a sistemului de management al securității informației pentru entități din Republica Moldova (pe exemplul băncilor comerciale)”.

Teză de doctor în informatică, Chișinău, 2024.

Structura tezei: teza este scrisă în limba română și constă din introducere, trei capitole, concluzii generale și recomandări, bibliografie 93 de titluri și 4 anexe. Teza conține 141 de pagini cu text de bază, 54 figuri și 10 tabele. Rezultatele obținute sunt publicate în 8 lucrări științifice cu volum total de circa 7 coli de autor.

Cuvinte-cheie: Securitatea Informației (SecInf), Securitatea cibernetică (SC), Sistem de Management al Securității Informației (SMSI), Model Multiprofil de Maturitate a Securității Informației (M^3SI), Baza generică de date M^3SI, Profil de securitate a informației tipic unei industrii (PSITI), Profil individual de securitate a informației (PISI) pentru o entitate concretă.

Scop: elaborarea unui model multiprofil de maturitate a securității informației cu suport informatic pentru evaluarea și creșterea nivelului de maturitate.

Obiective: Crearea unei baze generice de date M^3SI privind cunoștințele despre cadrele de abordare, cerințe, amenințări, riscuri și controale de securitate a informației; Elaborarea aplicației instrumentale de suport a modelului multiprofil M^3SI, a profilurilor tipice unor industrii PSITI și a profilurilor PISI pentru entități concrete; Generarea, aprobarea și validarea unui profil tipic PSITI pentru activitatea bancară, stabilirea valorilor țintă ale criteriilor de măsurare și evaluarea conform PISI.

Noutatea și originalitatea științifică: modelul generic M^3SI, profilul tipic PSITI și profilurile particulare PISI cu controale, criterii și metrici specifice, instrumentul software de suport pentru M^3SI și procesul de evaluare sunt originale și potrivite pentru diferite entități și contexte diferite de utilizare.

Rezultatul obținut care contribuie la soluționarea unei probleme științifice importante îl constituie baza de cunoștințe despre cadrele de abordare și controalele de securitate a informației și generarea modelelor multiprofil conforme unor cerințe tipice comune și specifice individuale, pentru cazuri particulare, concrete.

Semnificația teoretică este determinată de sintezarea bazei de cunoștințe, a modelelor, profilurilor, controalelor de securitate a informației, a criteriilor de evaluare și măsurare a maturității conform cerințelor tipice și particulare.

Valoarea aplicativă constă în aportul substanțial al modelelor, profilurilor generate și a aplicației de suport pentru măsurarea și evaluarea nivelului de maturitate a securității informației, aplicabile pentru un cerc larg de organizații și utilizatori evaluatori, auditori ai securității informației.

Implementarea rezultatelor: modelele M^3SI, PSITI, PISI și aplicația de suport au fost implementate în BNM pentru activitățile de supraveghere și evaluare a SecInf a BC din Moldova.

ANNOTATION

BRICEAG Valentin: "Analysis and Enhancement of the Information Security Management System Maturity Level for the Republic of Moldova Entities (Case Study - Commercial Banks)".

PhD thesis in computer science, Chisinau, 2024.

Thesis structure: the thesis is written in Romanian and consists of an introduction, three chapters, general conclusions and recommendations, a bibliography of 93 titles and 4 appendices. The thesis contains 141 pages of basic text, 54 figures and 10 tables. The obtained results were published in 8 papers with a volume of over 7 sheets of author.

Keywords: Information Security (IS), Cyber Security (CS), Information Security Management System (ISMS), Multiprofile Information Security Maturity Model (M^3SI), Generic Database M^3SI, Information Security Profile Typical of an Industry (PSITI), Individual Information Security Profile (PISI) for a specific entity.

Research purpose: the development of a multi-profile information security maturity model with TI support for evaluating and increasing the maturity level of information security.

Research objectives: Create a generic M^3SI database of knowledge about IS approach frameworks, requirements, threats, risks and controls; Development of the instrumental support application of the M^3SI multi-profile model, of the typical for an industry profile PSITI and of the individual PISI profile for concrete entity; Generating, approving and validating a typical PSITI profile for banking activity, establishing the target values of the measurement criteria and evaluation according to PISI.

Scientific novelty and originality: The generic M^3SI model, the typical PSITI profile and the particular PISI profiles with specific controls, criteria and metrics, the software tool supporting the model M^3SI and the evaluation process are original and suitable for different entities and different contexts of use.

The obtained result, which contributes to solving of an important scientific problem, is the database with the knowledges about the information security approach frameworks and controls and the generation of multi-profile models conforming to typical common and specific individual requirements, for particular, concrete cases.

The theoretical significance it is determined by the synthesis of the knowledges base, information security models, profiles, controls and their evaluation and measurement of the criteria for evaluating and measuring their maturity according to typical and particular requirements.

The applicative value: it consists in the substantial contribution of the generated models, profiles and the supporting application in the measurement and evaluation of the maturity level of IS, applicable to a wide area of organizations and user's evaluator, auditors of IS.

Implementation of the results: the M^3SI, PSITI, PISI models and the auxiliary application were implemented in the NBM for supervisory activities and assessment of information security of banks in Moldova.

АННОТАЦИЯ

Бричаг Валентин: «Анализ и повышение уровня зрелости системы управления информационной безопасностью для предприятий Республики Молдова (на примере коммерческих банков)».

Докторская диссертация по информатике, Кишинёв, 2024.

Структура диссертации: диссертация написана на румынском языке и состоит из введения, трех глав, общих выводов и рекомендаций, библиографии из 93 названий и 4-ёх приложений. Диссертация содержит 141 страниц основного текста 54 рисунков и 10 таблиц. Полученные результаты опубликованы в 8-и научных работах с общим объёмом около 7 авторских листов.

Ключевые слова: информационная безопасность (ИБ), кибербезопасность (КБ), система управления информационной безопасностью (СУИБ), многопрофильная модель зрелости информационной безопасности (M^3SI), универсальная база данных M^3SI, типичный для отрасли профиль информационной безопасности (PSITI), Индивидуальный профиль информационной безопасности (PISI) для конкретной организации.

Цель: разработка многопрофильной модели зрелости ИБ с ИТ-поддержкой для оценки и повышения уровня зрелости.

Подцели: создание базы данных M^3SI, содержащее обобщённые знания о подходах к ИБ, о требованиях, угрозах, рисках и средствах контроля ИБ; разработка инструментального приложения для поддержки многопрофильной модели M^3SI, типовых отраслевых профилей PSITI и индивидуальных профилей PISI для конкретных объектов; разработка, утверждение и валидация типового профиля PSITI для банковской деятельности, установление целевых значений критериев и оценка согласно PISI.

Научная новизна и оригинальность: генерирующая модель M^3SI, типичный для отрасли профиль PSITI и индивидуальные профили PISI для конкретных объектов со специфическим контролями ИБ, критериями и показателями, программный инструмент, для поддержки модели M^3SI и процесса оценки – являются оригинальными и подходят для различных объектов и различных конкретных контекстов использования.

Полученный результат, способствующий решению важной научной задачи, является обобщённая база знаний по основным общепризнанным подходам и управлению ИБ и построение на их основе многоуровневых моделей, соответствующих типовым отраслевым и конкретным индивидуальным требованиям, для конкретных частных случаев.

Теоретическая значимость: определяется синтезом базы знаний, критериев оценки зрелости и их измерения в соответствии с типовыми и специфическими/частными требованиями.

Прикладная ценность: заключается в существенном вкладе моделей, профилей и вспомогательного приложения для измерения и оценки уровня зрелости ИБ, применимого к широкому кругу организаций и пользователей оценщиков и аудиторов ИБ.

Внедрение результатов: модели M^3SI, PSITI, PISI и вспомогательное приложение были внедрены в НБМ для надзорной деятельности и оценки ИБ банков Молдовы.

BRICEAG Valentin

ANALIZA ȘI CREȘTEREA NIVELULUI DE MATURITATE A SISTEMULUI DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI PENTRU ENTITĂȚI DIN REPUBLICA MOLDOVA

(pe exemplu băncilor comerciale)

232.02 Tehnologii, produse și sisteme informaționale

Rezumatul tezei de doctor în Informatică

Aprobat spre tipar: 02.05.2024
Hârtie ofset. Tipar ofset.
Coli de tipar: 2.0

Formatul hârtiei 60×84 1/16
Tiraj 25 ex.
Comanda nr. 60/24

Centrul Editorial-Poligrafic al USM
Str. Al. Mateevici, 60, Chișinău, MD-2009
Email: cep1usm@mail.ru, usmcep@mail.ru