UNIVERSITATEA DE STAT DIN MOLDOVA
ȘCOALA DOCTORALĂ ȘTIINȚE FIZICE, MATEMATICE, ALE INFORMAȚIEI ȘI INGINEREȘTI

Cu titlu de manuscris
C.Z.U.: 004.056(043.2)

BUZDUGAN AURELIAN

SISTEME DE SUPORT DECIZIONAL PENTRU IDENTIFICAREA ȘI DIMINUAREA RISCURILOR CIBERNETICE IN INFRASTRUCTURI CRITICE

121.03 Programarea calculatoarelor

Rezumat

Autor: Buzdugan, Aurelian
Conducător științific: Căpățână, Gheorghe
doctor în științe tehnice, profesor universitar

Membrii Comisiei de îndrumare: Beldiga Maria, conf. univ., dr. în informatică
Cerbu Olga, conf. univ., dr. în șt. fizico-matematice
Ciobu Victor, conf. univ., dr. în șt.fizice

CHIȘINĂU, 2022

Teza a fost elaborată în cadrul Școlii doctorale științe fizice, matematice, ale informației și inginerești, Universitatea de Stat din Moldova.

Comisia de doctorat:

1. **ARNAUT Vsevolod**, doctor în științe fizico-matematice, conferențiar universitar, Universitatea de Stat din Moldova, Președinte al Comisiei de susținere publică;
2. **CĂPĂȚÂNĂ Gheorghe**, doctor în științe tehnice, profesor universitar, Universitatea de Stat din Moldova, conducător științific;
3. **FILIP Florin Gheorghe**, doctor inginer, profesor universitar, academician, Academia Română, membru/referent;
4. **COSTAȘ Ilie**, doctor habilitat în informatică, profesor universitar, Academia de Studii Economice a Moldovei, membru/referent;
5. **BELDIGA Maria**, doctor în informatică, conferențiar universitar, Universitatea de Stat din Moldova, membru/referent;
6. **NOVAC Ludmila**, doctor în științe fizico-matematice, conferențiar universitar, Universitatea de Stat din Moldova, secretar științific.

Susținerea va avea loc la **30 noiembrie 2022, orele 15:00.**

Teza de doctor și rezumatul pot fi consultate la biblioteca Universității de Stat din Moldova şi pe pagina web a Agenției Naționale de Asigurare a Calității în Educație și Cercetare (www.cnaa.md).

Rezumatul a fost expediat la 26 octombrie 2022.

Autor: Buzdugan Aurelian

Secretar științific: Novac Ludmila

Cuprins

REPERELE CONCEPTUALE ALE CERCETĂRII 4

CONȚINUTUL TEZEI 7

CONCLUZII GENERALE ȘI RECOMANDĂRI 20

BIBLIOGRAFIE 23

ADNOTARE 24

REPERELE CONCEPTUALE ALE CERCETĂRII

Actualitatea temei

Evoluția impresionantă a tehnologiilor informaționale (TI) și comunicațiilor a transformat lumea în una interdependentă cu avantaje enorme, dar și cu dezavantaje prin dependența crescândă de sistemele din TI, inclusiv din infrastructurile critice (IC). Securitatea cibernetică a IC este o prioritate la nivel național [1], european [2, 3] și global [4, 5]. Atacurile cibernetice pot afecta sistemele cu tehnologii operaționale (TO) în toate domeniile IC de la medical [6], nuclear și radiologic. Ca exemple elocvente, Ministerul Afacerilor Externe Austriac sau fabrica Thyssen-Krupp, considerate IC, au fost victime ale atacurilor cibernetice [7]. De aceea, sunt deosebit de actuale mecanismele eficiente, inclusiv inteligente, de identificare și gestionare a riscurilor cibernetice în IC.

Scopul tezei de doctorat este dezvoltarea unui concept de sistem suport decizional (SSD) inteligent pentru minimizarea și gestionarea riscurilor cibernetice în IC cu obiectivele de cercetare:

1. Cercetarea aspectelor generale ale SSD și ale managementului riscurilor cibernetice în IC.
2. Identificarea elementelor și factorilor specifici SSD.
3. Evaluarea impactului dimensiunii umane în acest domeniu.
4. Dezvoltarea unui model, sistem formal metric inteligent, a unei aplicații de evaluare a maturității securității cibernetice în cadrul IC și SSD pentru identificarea priorităților cheie.

Metodologia cercetării

În teză au fost aplicate analiza sistematică și analiza selectivă a literaturii. Metodologia predefinită de analiză permite identificarea, analiza și interpretarea studiilor existente și disponibile privind utilizarea SSD la analiza riscurilor cibernetice. Modelul de studiu reduce probabilitatea unei părtiniri și creează o imagine de ansamblu cuprinzătoare asupra subiectului dorit. Analiza a fost atât calitativă, cât și cantitativă, bazată pe scopul evaluării. Având în vedere natura și domeniul cercetării, majoritatea rezultatelor au fost prezentate textual în urma analizei calitative. De asemenea, a fost utilizată metoda logică pentru a rezuma cercetările în utilizarea SSD în scopul propus, iar metoda comparativă - pentru a dezvolta conceptul de SSD și modelul de evaluare a securității cibernetice pentru IC în orice domeniu și pentru aplicări universale.

Noutatea și originalitatea științifică

Rezultatele originale, cuprinzătoare și multilaterale includ un concept de SSD, un model de evaluare a maturității securității cibernetice, o bază de cunoștințe și un sistem formal metric inteligent cu aplicație prototip. Prototipul permite aplicarea modelului de evaluare a securității cibernetice.

Problema științifică rezolvată

A fost dezvoltată o soluție inovativă pentru asigurarea securității cibernetice IC asistată de un SSD original, destinat identificării, clasificării și managementului riscurilor cibernetice în IC. În premieră au fost dezvoltate un sistem formal metric inteligent și un prototip software pentru implementarea procesului de evaluare și compararea nivelului de maturitate cu bunele practici sau cu alte IC. Modelul de la baza sistemului formal metric inteligent conține cinci niveluri de maturitate bazate pe criterii de dimensiune tehnologică și umană. Modelul este universal pentru domeniul IC și contribuie la sporirea nivelului de maturitate a securității cibernetice și minimizarea riscurilor. SSD și modelul propus pot fi utilizate separat sau complementar și adaptate pentru orice tip de IC, în funcție de context și cerințe. Rezultatele sunt o contribuție la realizarea obiectivelor Direcției strategice 2(g) a priorității strategice V „Competitivitate Economică și Tehnologii Inovative" a Programului Național de Cercetare și Inovare pentru anii 2020-2023 al Republicii Moldova.

Semnificația teoretică

A fost dezvoltat un concept de SSD pentru evaluarea maturității securității cibernetice și un model aplicabil pentru autoevaluări și evaluări externe a securității cibernetice IC. Au fost dezvoltate un sistem formal metric inteligent și un prototip software ce implementează procesele de evaluare.

Valoarea aplicativă a rezultatelor

Modelul de evaluare a securității cibernetice IC propus include identificarea nivelului de maturitate în baza a patru criterii: administrative și management, educație și evaluare, mediul de lucru și gestionarea riscurilor cibernetice. Adițional au fost dezvoltate un sistem formal metric inteligent și un prototip software în *Python* pentru integrările viitoare în metodologiile generale de management ale riscului. Modelul permite luarea timpurie de către decidenți de măsuri corelate cu procesele operaționale din IC și poate fi utilizat inclusiv pentru acreditare sau licențiere.

Rezultatele obținute reprezintă o contribuție aplicativă în sprijinul acțiunii „Evaluarea și raportarea privind starea și nivelul de securitate a obiectivelor de infrastructură critică din perspectiva securității informaționale" din Obiectivul nr. 5 „Sporirea capacităților de protecție a infrastructurilor critice naționale", Pilonul III „Consolidarea capacităților operaționale", Capitolul IV al Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și Planului de acțiuni pentru implementarea acesteia. Valoarea practică a modelului a fost validată de Autoritatea Slovenă de Securitate Nucleară, Institutul Național de Metrologie din Moldova și Centrul Național de Suport al Securității Nucleare de la UTM (reflectat în curriculumul de „Securitate nucleară și radiologică").

Rezultatele științifice înaintate spre susținere

- Cercetările în domeniul managementului riscurilor cibernetice în IC au condus la definirea arhitecturii și principiului de funcționare a SSD, conceptelor teoretice de implementare și adaptare a sistemelor informaționale în IC: factorul uman, publicul țintă, reziliența, modelarea și simularea, complexitatea și interdependența, factorii mediului de lucru.
- Evaluarea și analiza impactului elementelor factorului uman asupra SSD propus în domeniul IC a contribuit la identificarea tendințelor și a celor mai bune practici de proiectare, dezvoltare și utilizare a sistemelor TI. Îmbunătățirea eficienței SSD se realizează prin:
  - utilizarea unui SSD ca modul pentru a facilita interoperabilitatea și integrarea acestuia în cadrele existente de gestiune a riscurilor;
  - utilizarea standardelor pentru dezvoltarea interfeței cu utilizatorul și codificare, pentru a reduce costurile și a îmbunătăți gradul de utilizare a platformei;
  - evaluarea cu tehnologii moderne a stării fizice a operatorilor de luare a deciziilor critice.
- Modelului de evaluare a maturității securității cibernetice IC.
- Sistemul formal metric inteligent „Securitatea cibernetică în infrastructuri critice", baza de cunoștințe și prototipul aplicației dezvoltate în premieră.
- Evaluarea securității cibernetice în domeniile IC ale Republicii Moldova a contribuit la validarea modelului de evaluare a maturității securității cibernetice, a confirmat aplicabilitatea retroactivă într-un anumit domeniu al IC sau entitate individuală și la elaborarea unor recomandări de îmbunătățire a maturității securității cibernetice naționale.

Aprobarea rezultatelor tezei și publicații științifice

Rezultatele științifice au fost prezentate și discutate la 24 de conferințe naționale, inclusiv cu participare internațională, și internaționale care au avut loc în: Republica Moldova (10), Austria (5), România (5), Ucraina (1), China (1), Japonia (1) și Macedonia de Nord (1).

Sistemul formal metric inteligent „Securitatea cibernetică în infrastructurile critice" a fost înregistrat la AGEPI cu Dreptul de autor iar la Saloanele Internaționale ale Inovării Cadet INOVA'21 (Sibiu, 2021) și „Traian Vuia" (Timișoara, 2022) a fost apreciat cu medalii de bronz.

Au fost elaborate și publicate 22 articole - autor principal, 6 articole - coautor; 8 articole - mono-autor; 3 rezumate - mono-autor; 3 articole în reviste științifice de specialitate, inclusiv 1 în Republica Moldova (B+); 2 articole indexate Web of Science; 7 - indexate Scopus; 7 - publicate la editura Springer; 2 articole acceptate pentru publicare în Springer; 25 de articole și rezumate.

CONȚINUTUL TEZEI

Teza este compusă din introducere, trei capitole, concluzii și recomandări finale, bibliografie și 7 anexe. Conținutul de bază include 131 de pagini, 17 figuri și 4 tabele.

În **Introducere** este prezentată actualitatea și importanța acestei teme. De asemenea este descris scopul tezei de doctorat și au fost identificate obiectivele cercetării, metodologiile de cercetare, rezultatele științifice noi obținute în urma cercetării și valoarea lor practică.

Capitolul I prezintă situația curentă a cunoștințelor și cercetărilor în domeniu privind amenințările cibernetice asupra IC, cât și elementele de bază în gestionarea riscurilor și oportunitatea de a utiliza SSD în IC. Analiza a contribuit la o mai bună înțelegere a temei precum și la identificarea ariilor ulterioare de cercetare. Inițial cercetarea abordează definirea scopurilor și problemelor care au fost analizate pe parcursul cercetării. Prima parte are drept scop definirea riscurilor de securitate cibernetice, componentele acestora și impactul lor asupra IC. Ulterior, teoria existentă a fost utilizată în vederea aprofundării cunoștințelor în acest domeniu. Astfel, anumite modele de atenuare și identificare a riscurilor au fost dezvoltate sau identificate și aplicate pe baza datelor obținute anterior.

Riscurile de securitate cibernetică în IC reprezintă o tema actuală din cauza incidentelor recente, precum și a rolului critic al componentelor TI în IC. O prezentare a funcțiilor computerelor în IC este oferită în Figura 1. Amenințările cibernetice globale devin din ce în ce mai acute datorită dezvoltării continue a metodelor și tehnicilor de atac, dar și a capacității de a cauza daune fizice prin intermediul sistemelor informaționale. Atacurile actorilor de stat creează riscuri și mai mari, deoarece aceștia pot avea un nivel înalt și sofisticat de expertiză și cunoștințe, precum și acces și resurse suficiente pentru a-și atinge obiectivele. Mai mult, dezvoltarea rapidă a sistemelor de inteligență artificială și a *internet-of-things*, contribuie nu doar la securitatea IC, ci și deschid un nou peisaj de amenințări mult mai complex și mai inteligent, ce nu este complet considerat în prezent în sistemele de securitate sau siguranță în exploatare. Aceste sisteme deseori extind ariile de atac, prin urmare gestionarea riscurilor devine și mai complexă.

Discuțiile privind protecția IC sunt acum axate pe dimensiunea cibernetică, datorită faptului că toate infrastructurile includ componente TI, în principal pentru funcțiile operaționale. Protecția IC este un subiect care depășește cu mult domeniul tehnic, fiind o provocare majoră legată de strategii și politici. Astfel, această temă necesită o abordare interdisciplinară, având în vedere impactul și nivelul de integrare a TI în IC. De asemenea, interconectarea IC la nivel național sau internațional poate duce involuntar la o creștere a suprafeței de atac, ceea ce stimulează diversificarea metodelor de atac utilizate. Potrivit Verizon, în 2021 rata incidentelor *ransomware*

care pot duce la sabotajul operațiunilor într-o organizație, a fost de 10%, ce denotă o creștere dublă față de 2020. De asemenea, rata incidentelor care a afectat IC este de aproximativ 10% din numărul total de incidente [8]. Dacă se compară timpul de răspuns, peste 90% din incidente au avut loc în câteva minute, dintre care 70% au fost depistate după câteva luni. Astfel, timpul necesar pentru a lansa un atac este scurt în comparație cu eforturile de a securiza și monitoriza aceste componente digitale din cadrul IC [9]. În plus, cel mai recent raport al grupului de experți guvernamentali al ONU privind promovarea comportamentului responsabil al statului în spațiul cibernetic în contextul securității internaționale, a identificat ca prioritate riscurile cibernetice față de IC și a propus norme privind stoparea oricăror atacuri împotriva IC din alte țări, asigurarea unei protecții adecvate a propriilor IC, precum și cooperarea cu alte state pentru a face schimb de cunoștințe, expertiză și bunele practici din acest domeniu [4].

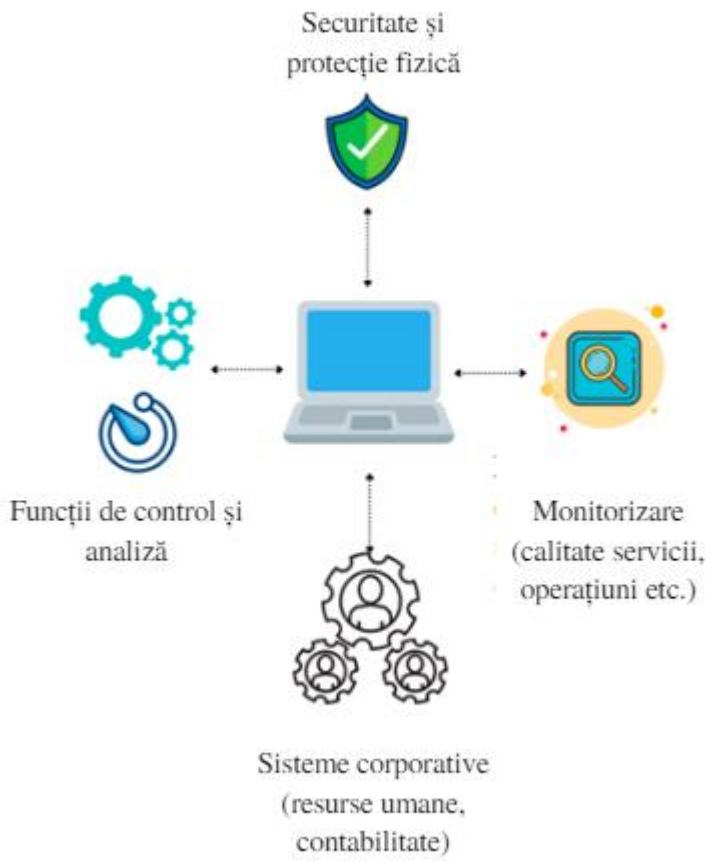

Fig. 1. Rolul computerelor în IC

Necesitatea eficientizării gestionării riscurilor cibernetice în vederea prevenirii atacurilor asupra IC rezultă de asemenea din activitatea autorului ca lector invitat (2015-2017) al Departamentului de Securitate și Siguranța Nucleară al Agenției Internaționale pentru Energie Atomică. În această perioadă, au fost predate o serie de module din securitatea cibernetică care au

făcut parte din training-ul oferit în Kazahstan, Slovenia și Moldova. Scopul principal al cursurilor din acea perioadă, a fost ridicarea conștientizării rolului securității cibernetice în sistemele IC utilizate de operatorii nucleari și radiologici.

Un alt interes personal îl reprezintă utilizarea tehnologiilor emergente, cum ar fi inteligența artificială sau *machine learning*, ce oferă posibilități organizațiilor și indivizilor în detectarea anomaliilor care pot corespunde incidentelor de securitate. Securitatea cibernetică devine adesea o cursă contra cronometru pentru a asigura oportunitatea și eficacitatea acestor controale de securitate. Sinergismul dintre inteligența artificială și securitatea cibernetică poate oferi noi capabilități și resurse în asigurarea securității unui sistem sau dispozitiv. În același timp, aceeași sinergie poate crea riscuri într-un sistem la un nivel mult mai înalt. Cu toate acestea, multe dintre riscurile de securitate cibernetică care există în prezent în IC ar putea fi minimizate prin implementarea unor bune practici de securitate care pot fi preluate și adaptate din domeniul TI tradiționale.

Gestionarea riscurilor cibernetice depinde în mare măsură de procesarea unui volum mare de date despre riscuri și de un proces complex de analiză, prioritizare și luare a deciziilor. Interconectarea, interdependența și digitizarea IC cresc considerabil volumul de date necesare de evaluat pentru managementul riscului. Cunoașterea securității cibernetice este necesară pentru a putea reflecta riscurile unui sistem TI în IC, dar și cunoașterea contextului IC și a sistemelor operaționale. Prelucrarea datelor în procesul de luare a deciziilor depășește limitele umane și ar trebui utilizate sisteme informatice pentru a sprijini acest proces.

În aceasta teză sunt explorați factorii specifici ai gestionării riscurilor cibernetice în acest domeniu, precum și provocările pe care le creează operatorilor și decidenților. Una dintre întrebările cheie evaluate este dacă procesul existent de gestionare a riscurilor abordează în mod adecvat riscurile cibernetice. Au fost identificate domeniile în care sunt recomandate cercetări ulterioare, precum și a fost propus un concept de SSD care va îmbunătăți gestionarea riscurilor cibernetice în IC. Pentru a evalua eficiența și aplicabilitatea acestui concept de SSD, a fost dezvoltat în premieră un sistem formal metric inteligent și un prototip în *Python* care implementează procesul de evaluare a modelului propus, cât și incorporează elemente din constatările și rezultatele obținute în cadrul acestei cercetări.

Dimensiunea umană are un rol critic în dezvoltarea și utilizarea sistemelor de sprijinire a deciziilor. În această lucrare au fost evaluate implicațiile dimensiunii umane într-un SSD pentru gestionarea riscurilor cibernetice în IC. A fost analizat impactul pe care factorul uman îl are asupra SSD și au fost propuse soluții pentru depășirea limitărilor cauzate de dimensiunea umană. De

asemenea, s-a discutat despre modul în care soluțiile și recomandările propuse pot crește eficiența SSD utilizată în domenii cu cerințe stringente de securitate, precum IC.

Luând în considerare numărul de metodologii de gestionare a riscurilor în IC, se poate considera că gestionarea ar trebui să fie holistică și să includă scenarii și funcții care să acopere și riscurile cibernetice. Această constatare a definit potențialele cercetări ulterioare în definirea unui SSD pentru a identifica, prioritiza și eventual propune controale care ar gestiona eficient riscurile cibernetice în IC.

Ca soluție la problema abordată s-a propus efectuarea procesului de gestionare a riscurilor prin intermediul unui SSD. Elementele identificate ca necesare și critice pentru acest sistem sunt: cunoștințele despre sistemul IC și componentele sale digitale, metodologiile și instrumentele de atac cibernetic, reziliența, interconectarea, interdependența cu alte sisteme și modul de prezentare a rezultatelor. Deoarece aceste elemente ar putea implica cantități mari de date specializate, SSD ar fi soluția optimă prin integrarea diverselor metodologii și sisteme informaționale pentru identificarea riscurilor și selectarea sau recomandarea celor mai bune soluții. Un astfel de sistem ce utilizează și tehnologii moderne este o soluție adecvată din punct de vedere a eficienței și a costurilor și ar contribui la rezolvarea problemei identificate.

În urma analizei au fost identificate câteva domenii care nu au o acoperire extinsă din care au fost selectate subiectele viitoare de cercetare. Înțelegerea riscurilor cibernetice și a tuturor implicațiilor asupra unui IC, în combinație cu SSD, ar permite decidenților să ia decizii efective și operative față de riscurile identificate. Un SSD care se concentrează în mod explicit pe riscurile cibernetice ar completa și susține cercetările existente și este necesar pentru susținerea obiectivelor pe termen lung în gestionarea riscurilor emergente. În timp ce evenimentele fizice și daunele din IC au reprezentat ani de zile riscurile majore, se constată că momentan gestionarea riscurilor din acest domeniu nu acoperă în mod exhaustiv noua natură a riscurilor pe care o aduce spațiul cibernetic. Un SSD concentrat în mod explicit pe riscurile cibernetice și dezvoltat într-un mod în care este văzut ca o componentă, ar crește probabilitatea ca acesta să fie integrat de responsabilii de management al riscului și utilizat în scenarii de caz real. Astfel, s-ar îmbunătăți procesele de management al riscului în domenii IC, precum medicină, nuclear sau radiologic [10].

Aceste rezultate constituie perspective valoroase asupra posibilității de a utiliza SSD pentru gestionarea riscurilor cibernetice în IC. Rezultatele analizelor efectuate validează și confirmă actualitatea problemei de cercetare selectate și a oferit informații valoroase pentru înțelegerea stării curente în acest domeniu. Cunoștințele acumulate au permis confirmarea obiectivele de cercetare și necesitatea de a explora factorii necesari pentru conceptul de SSD.

Capitolul II descrie procesul de validare a potențialului SSD în gestionarea riscurilor cibernetice în domeniul IC și conceptul de SSD propus. Pentru a asigura calitatea analizei au fost analizate cele mai recente evoluții și rezultate din acest domeniu, selectând studii de specialitate din jurnale sau lucrări ale conferințelor. Pe baza acestor rezultate, a fost conceput un SSD pentru gestionarea riscurilor cibernetice în IC. Capitolul începe cu descrierea metodelor de cercetare utilizate și, în principal, a analizei sistematice a literaturii. Metoda implică identificarea lucrărilor existente la acest subiect, astfel previne dublarea și suprapunerea cercetărilor și ajută la identificarea potențialelor direcții de cercetare și domenii care nu au fost suficient analizate, cât și pentru dezvoltarea de noi concepte și modele pentru a rezolva problema identificată.

În urma analizei s-a constatat că nu există nici-un SSD care să ia în considerare toate tipurile de riscuri de securitate cibernetică și doar un subset dintre acestea. De asemenea, se constată că metodele existente ce combină identificarea, prioritizarea și atenuarea riscurilor sunt insuficient explorate. Această direcție a fost selectată la baza conceptului de SSD propus, care ar ameliora procesul de evaluare și gestionare a riscurilor. De asemenea, procesul de gestionare a riscurilor devine din ce în ce mai complex și, adesea, necesită adaptat cerințelor și contextului fiecărui tip de IC. În urma analizei se observă, că riscurile cibernetice sunt incluse în general în procesul de gestionare al riscurilor, dar aceste riscuri ar fi mai bine identificate și gestionate atunci când avem cunoștințe de specialitate. Foarte puține metodologii evaluează exclusiv impactul pe care TI și securitatea cibernetică îl au asupra IC, ca modul sau proces separat. Pentru o gestionare eficientă a riscurilor cibernetice în IC este necesar să fie îmbunătățite acuratețea și capacitatea de luare a deciziilor.

O altă necesitate identificată este construirea și dezvoltarea unui SSD modular care să fie ușor de integrat în alte SSD sau în entități responsabil de gestionare a riscurilor. Se observă un număr mic de lucrări în acest domeniu pe problema data, ce denotă faptul că dezvoltarea unui SSD comun pentru toate tipurile de riscuri poate consuma prea mult timp și resurse. Astfel, un SSD dezvoltat ca modul cu diverse interfețe pentru conectare și partajare a datelor ar permite o integrare și adaptare facilă pentru diverse domenii și sisteme. De asemenea se remarcă un accent pe importanța interfeței unui SSD care poate fi corelată cu eficiența în utilizare de către operatori sau factorii de decizie, precum și cu nivelul de cunoștințe în TI necesar.

Ulterior, a fost prezentat conceptul de SSD pentru gestionarea riscurilor cibernetice în domeniul IC, precum și factorii ce sunt direct corelați cu eficiența, performanța și rata de implementare a unui SSD. Au fost identificate și descrise următoarele elementele cheie necesare de luat în considerare la elaborarea unui SSD pentru domeniul IC: factorul uman, utilizatorul final,

reziliența, modelarea și simularea, complexitatea și interdependența (Figura 2). Acestea reprezintă unul din rezultatele originale ale tezei.

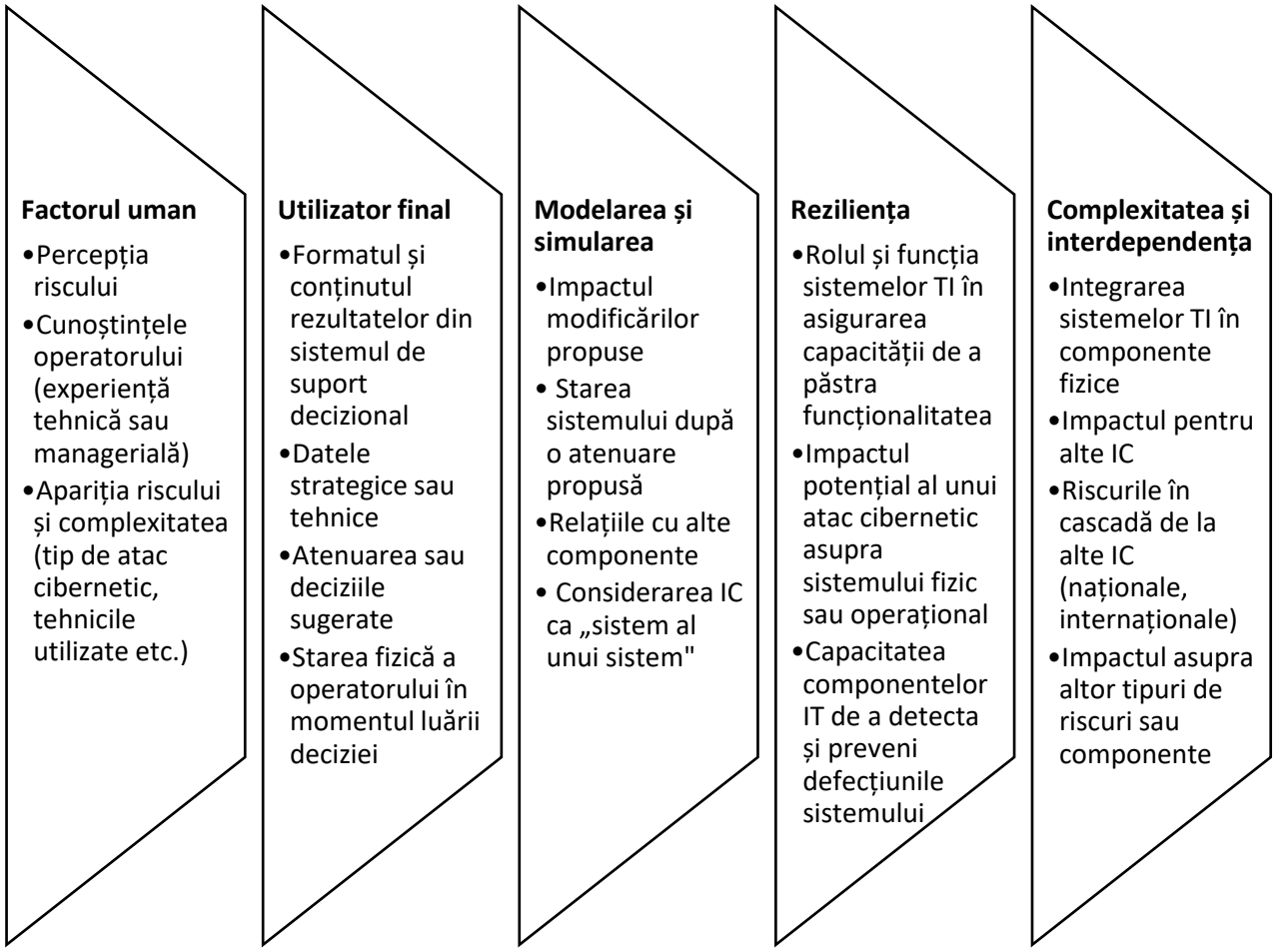

Fig. 2. Elemente necesare în cadrul unui SSD în IC

Sistemul limbaj este unul dintre primele elemente care trebuie luate în considerare când se identifică tipurile de date necesare și sursele potențiale. Ținând cont de faptul că SSD urmează să fie adaptat pentru IC, au fost selectate sursele de date utile și necesare. În timp ce anumite abordări ce țin de riscurile cibernetice pot fi adaptate din domeniul TI, domeniul IC conține sisteme specifice, cum ar fi sistemele industriale de control, care trebuie luate în considerare. Elementele propuse pentru sistemul limbaj ar trebui fi utilizate din faza de proiectare. Fiecare tip de informație poate fi clasificat în funcție de unul sau mai multe tipuri de date propuse. O astfel de abordare este utilă atunci când se dezvoltă module și sisteme pentru recomandarea sau identificarea deciziilor. În cazul în care datele de intrare nu sunt structurate, întrucât sunt abordate sisteme complexe pentru domenii specifice, categoriile ar putea fi utilizate pentru a reduce costurile și resursele necesare pentru prelucrarea ulterioară a acestor date. Intrările propuse pentru sistemul lingvistic sunt prezentate în Figura 3. De asemenea a fost evaluată arhitectura generala a unui SSD și au fost

propuse adaptări pentru sistemele de prezentare și limbaj, ținând cont de domeniul specific a IC. Au fost identificate și propuse elemente pentru cele două sisteme, precum și recomandări privind modul de evaluare și includere a elementelor factorului uman în fază de proiectare a SSD.

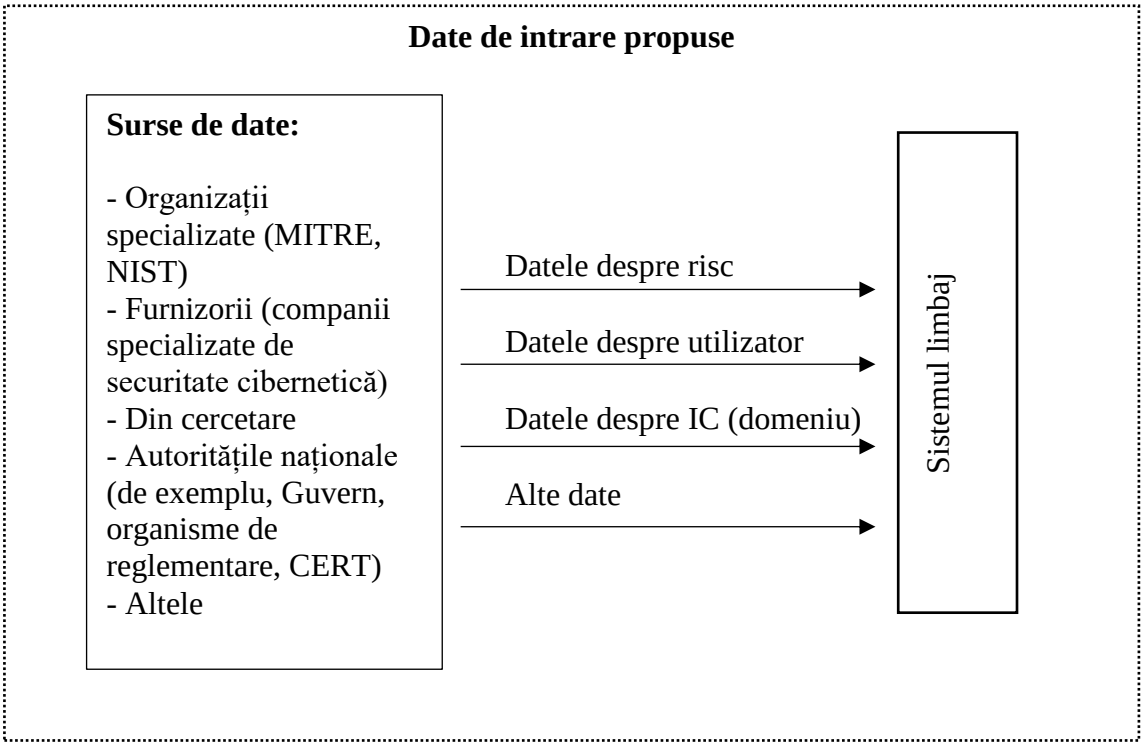

Fig. 3. Tipuri de date propuse pentru sistemul limbaj din cadrul SSD

Sistemul de prezentare, sau interfața cu utilizatorul, are unul dintre cele mai importante roluri în asigurarea eficienței și a integrării sistemului de către utilizatorii potențiali. Un produs al TI care este greu de utilizat are mai puține șanse de a reuși atât pe piață, cât și în îndeplinirea scopului său. Prin urmare, contextul și elementele factorului uman sunt printre cerințele principale în proiectarea interfeței cu utilizatorul. Factorul uman are un rol și mai important, deoarece eficiența percepută a SSD poate fi direct legată de acest factor. Factorul uman trebuie luat în considerare de la procesul de identificare și evaluare a unui risc cibernetic, până la procesul decizional.

În plus, dacă SSD este analizat ca o aplicație, atunci capacitatea de adaptare ar asigura un timp și cost redus pentru rezolvarea unei probleme, dar și îmbunătățirea calității aplicației software [11]. Având un sistem care poate învăț, valida și clasifica tipul de date de intrare, va eficientiza procesul de proiectare, dezvoltare și utilizare a sistemului, prin intervenții manuale minime. Acest lucru va asigura că SSD-ul propus să corespundă designului modular propus, astfel încât să poată fi adaptat la diferite tipuri de IC, precum și la cerințe specifice în ceea ce privește gestionarea riscurilor cibernetice.

O altă condiție importantă care trebuie luată în considerare la proiectarea arhitecturii SSD este contextul. Ținând cont de faptul că SSD-ul propus are un rol și un scop foarte specific, trebuie să fie luate în considerare și criteriile care ar asigura ca SSD să fie adecvat scopului pentru oricare dintre domeniile de IC. Contextul dictează des cerințe asupra sistemelor TI, începând de la hardware și software utilizat, conectivitate la rețea, până la tipurile de date care pot fi consumate în cadrul sistemului.

Dimensiunea umană are de asemenea un rol critic în contextul unui SSD în IC, datorită caracteristicilor domeniului. Întrucât SSD reprezintă un sistem socio-tehnic, acesta trebuie să fie proiectat și adaptat continuu necesităților utilizatorilor, rolurilor acestora în organizație, precum și contextului. Elementele factorului uman, cum ar fi percepția, abilitățile, capacitatea de a lua decizii corecte în situații de presiune sau cultura profesională joacă un rol critic pentru SSD propus. O imagine de ansamblu multidimensională și corectă a impactului dimensiunii umane asupra sistemelor informaționale ar facilita abordarea adecvată a riscurilor sau problemelor cunoscute, precum și la identificarea soluțiilor.

Dependența și impactul factorului uman asupra sistemelor informaționale sunt foarte largi. Pe de o parte, acestea pot influența negativ și pot reduce eficiența deciziilor recomandate sau luate de SSD. Pe de altă parte, luând în considerare toate constrângerile sau riscurile cunoscute începând cu faza de proiectare, se poate îmbunătăți și maximiza eficiența percepută oferită de un astfel de sistem. Constrângerile comune, cum ar fi costurile, timpul de livrare, precum și cultura organizațională pot influența calitatea SSD-ului final. De asemenea, sunt recomandate utilizarea standardelor existente, precum ISO 9241 sau ISO 27001, deoarece acestea sunt o soluție verificată pentru reducerea costurilor și timpului de livrare/implementare a produsului, dat fiind faptul că majoritatea cerințelor funcționale pot fi acoperite de standardele în vigoare. Urmând bunele practici se pot evita anumite probleme cunoscute sau constrângeri impuse de elementele factorului uman. Mai mult, tehnologiile computerizate moderne, precum cele care citesc parametrii biometrici, reprezintă o oportunitate de a recunoaște și minimiza riscurile prezentate de om. SSD poate sprijini și activități organizaționale, cum ar fi evaluările sau formările angajaților, precum și exercițiile practice. Acestea ar contribui la creșterea culturii securității cibernetice, dar și a abilităților profesionale ale utilizatorilor finali, care s-ar reflecta pozitiv asupra eficienței și utilizării percepute a SSD.

O altă soluție posibilă de reducere a anumitor riscuri sau erori umane în procesul de luare a deciziilor este automatizarea. Acest lucru are multe beneficii în ceea ce privește reducerea costurilor, precum și îmbunătățirea eficienței. Cu toate acestea, prin definiție, o IC nu îndeplinește cerințele pentru utilizarea automatizării deciziilor de către un SSD în procesul de gestionare a

riscurilor cibernetice. Anumite acțiuni pot fi identificate pentru automatizare anticipând astfel apariția unor probleme. Activitățile de evaluare, supraveghere a operatorilor devin critice pentru o automatizare sigură, perfecționarea calității automatizării, reducerea erorilor sau a limitărilor umane cunoscute, reducerii costurilor finale. De asemenea, merită menționat faptul că DSS sunt considerate soluții durabile [12], ceea ce înseamnă că efortul de a dezvolta astfel de sisteme ar fi justificat și ar ajuta la coordonarea eforturilor în soluționarea problemelor și riscurilor emergente.

Elementele identificate sunt aplicabile unui SSD care este utilizat în domeniul IC. Cu toate acestea aceste rezultate pot fi aplicate și pentru orice alt tip de sistem TI din acest domeniu.

Capitolul III descrie modelul de evaluare a maturității securității cibernetice a IC [13] și studiile de caz a integrării securității informatice în domeniul medicinei, nuclear și radiologic din Republica Moldova. Aceste domenii sunt în prezent considerate IC și se numără printre țintele de top pentru criminalii cibernetici. Pentru realizarea obiectivelor activitatea planificată a inclus și o analiză comparativă a cadrului legislativ și a controalelor tehnice existente în securitatea cibernetică din țară cu bunele practici, standarde sau ghiduri internaționale.

Au fost prezentate rezultatele analizei cadrului legislativ în domeniul securității nucleare și radiologice în Republica Moldova, prin prisma evoluției cronologice. Aceste constatări au fost corelate cu evoluția recomandărilor internaționale și celor mai bune practici în acest domeniu punctate de AIEA. De asemenea, a fost cercetat modul în care legislația națională în domeniul securității cibernetice a afectat domeniul IC inclusiv conex celui nuclear și radiologic. A fost efectuata o analiză a diverselor mecanisme de la nivel legislativ, cum ar fi cerințele minime pentru securitate cibernetică, și cum acestea influențează domeniul IC. Per general, nivelul de securitate în sectorul guvernamental este evaluat ca fiind în stare incipientă [14]. Acest lucru a contribuit la construirea unei imagini obiective asupra nivelului securității cibernetice pentru acest domeniu IC. Aceste rezultate sunt aliniate cu cele obținute în urma evaluării dezvoltării securității la nivel național în alte lucrări [15]. Evoluțiile au fost analizate din punct de vedere critic și au fost propuse recomandări privind îmbunătățirea cadrului legal, impactul cooperării pe verticală, schimbul de expertiză și bunele practici la nivel orizontal, precum și programul general de securitate cibernetică. Constatările sunt aliniate cu modelul propus și confirmă aplicabilitatea și autenticitatea acestuia.

De asemenea a fost dezvoltat și prezentat modelul pentru evaluarea nivelului de maturitate al securității cibernetice pentru organizațiile din IC (Figura 4). Acest model este complementar conceptului de SSD propus în capitolul II și înglobează elementele și aspectele critice identificate. Modelul combină patru dimensiuni cheie care pot descrie maturitatea securității cibernetice. Modelul este ușor de citit și înțeles și poate fi adaptat la cerințele fiecărei organizații din domeniul

IC. Simplitatea și claritatea cresc probabilitatea integrării unui sistem TI, ținând în același timp costurile și efortul la un nivel scăzut.

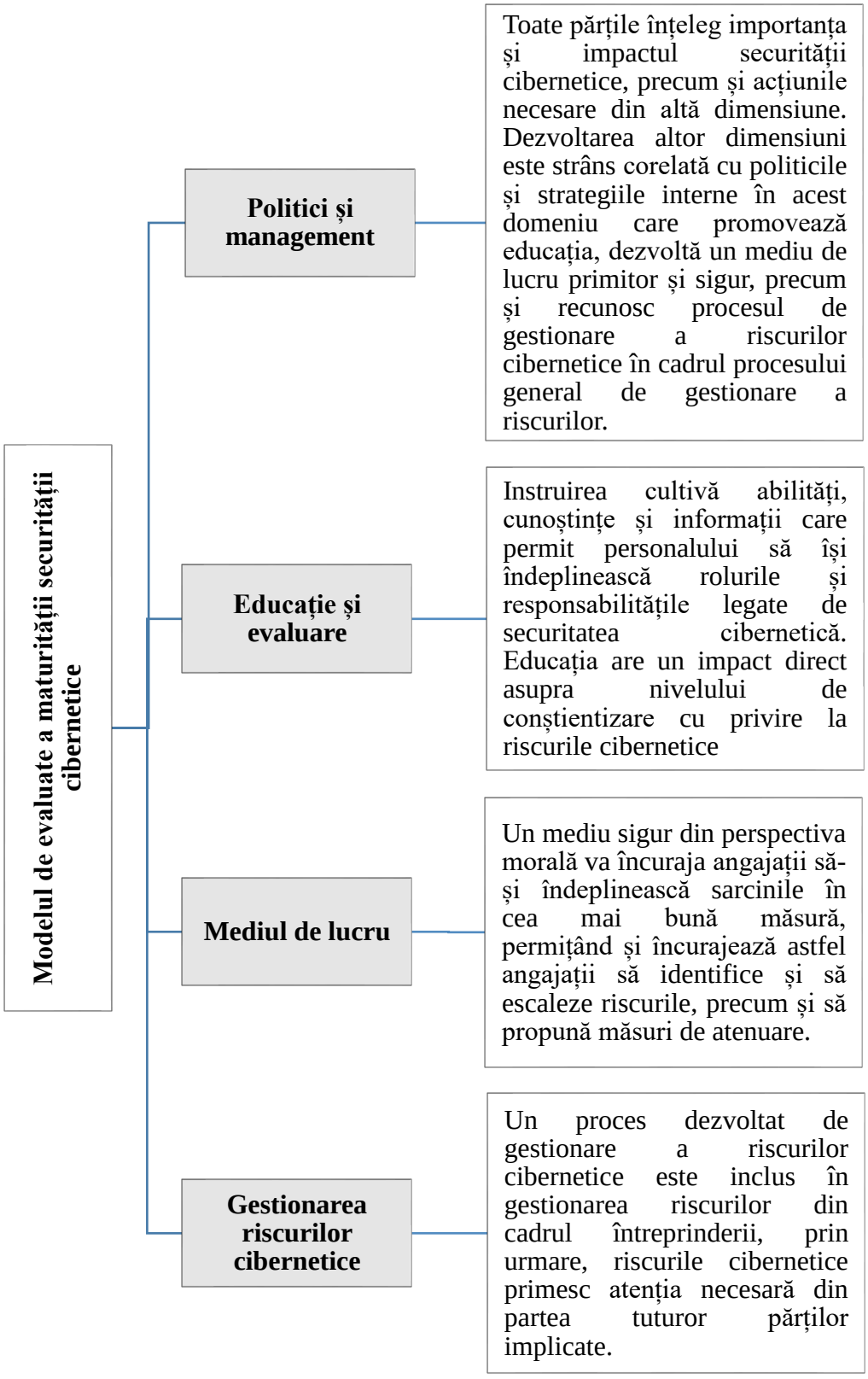

Fig. 4. Interdependența dimensiunilor securității cibernetice

Acest model poate susține un proces mai bun de luare a deciziilor în ceea ce privește gestionarea riscurilor cibernetice, deoarece poate arăta zonele care necesită atenție pentru a crește nivelul de maturitate. Modelul este multidimensional și poate fi utilizat atât pentru a evalua eficiența SSD propus din punct de vedere tehnologic și dimensiunea umană, dar și pentru a servi drept bază pentru caracteristicile sau algoritmii dezvoltați în cadrul sistemului de rezolvare a problemelor într-un SSD. Evaluarea poate sprijini implementarea SSD și revizuirea aspectelor organizaționale în legătură cu riscurile cibernetice pentru a se asigura că SSD este eficient și îndeplinește așteptările, precum și utilizat în timpul diferitelor procese sau necesități din organizație (Figura 5). Capitolul include și prezentarea bazei de cunoștințe „Securitatea cibernetică în infrastructuri critice" și a sistemul formal metric inteligent „Securitatea cibernetică în infrastructuri critice", care au fost dezvoltate în premieră pentru acest domeniu. Sistemul formal metric inteligent utilizează și aplică elementele din modelul propus, pentru a crea un proces de evaluare a securității cibernetice. De asemenea, sistemul formal metric inteligent „Securitatea cibernetică în infrastructuri critice" a fost înregistrat la AGEPI cu drept de autor (Seria 0, Nr. 7305 din 04.08.2022).

A fost elaborat și prototipul aplicației „Securitatea cibernetică în infrastructuri critice". Programul evidențiază versatilitatea și opțiunile de integrare a modelului în orice sistem TI de gestionare a riscurilor.

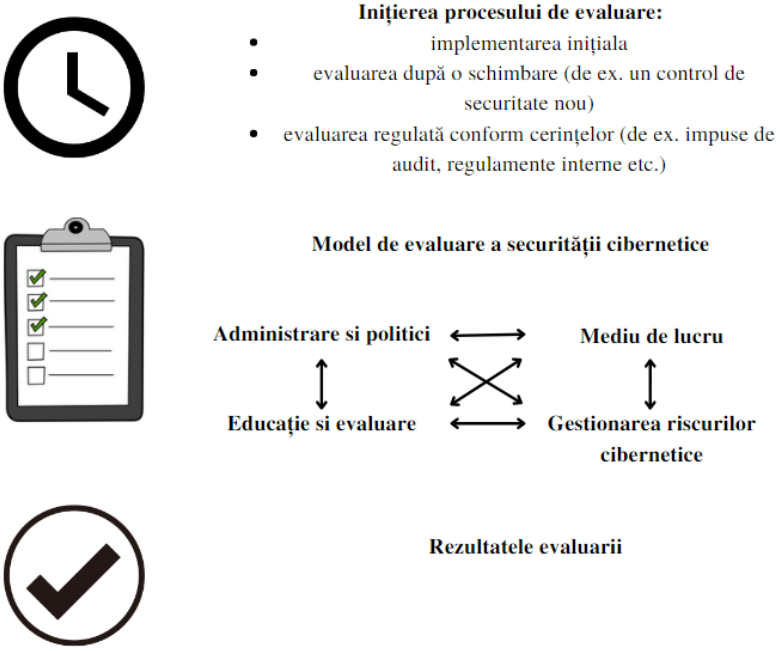

Fig. 5. Procesul și declanșarea evaluării securității cibernetice

Adițional, programul denotă potențialul modelului de a fi translat într-o aplicație simplă, care poate fi utilizată de decidenți în timpul procesului de evaluare. Formatul interfeței și limbajul de programare utilizat de acest program (clase, biblioteci și funcții) au fost atent selectate pentru a facilita integrarea și adaptarea modelului de către organizații.

Mai jos este prezentat Meniul Principal al aplicației, precum și opțiunile meniului ce descriu acțiunile corespunzătoare:

MENIU PRINCIPAL

1. Informații generale

2. Evaluare: Politici și administrare

3. Evaluare: Formare și Educație

4. Evaluare: Mediul de lucru

5. Evaluare: Managementul riscurilor cibernetice

6. Imprimați cele mai recente rezultate

7. Schimbați organizația

8. Comparați maturitatea

9. Ieșire

În timpul dezvoltării s-au identificat și implementat noi posibilități de îmbunătățire a modelului, cum ar fi amplificarea rezultatelor evaluării cu recomandări sau avertismente atunci când nivelul de maturitate este sub un prag minim prestabilit. Un exemplu a acestei funcționalități este redat mai jos:

Choose a menu option

> 1

****** General information about cyber security maturity level ******

Last assessment performed on: 2021-05-19

Latest average score: 2.9

****WARNING****

Overall cyber security maturity is below average. Actions are required to improve the security stance. To view the results per dimension select PRINT LATEST RESULTS

Programul poate fi utilizat în evaluarea a multiple organizații precum și selectarea dimensiunilor de securitate cibernetică dintr-o organizație care necesită atenție sau ameliorări. În plus, aplicația poate fi combinată și cu SSD propus inițial pentru gestionarea riscurilor cibernetice, ca o componentă principală. Această activitate experimentală a ajutat la dezvoltarea unor perspective noi asupra arhitecturii SSD, performanței acestuia, precum și impactului și integrării unui astfel de sistem într-o organizație.

Au fost prezentate și rezultatele aplicării retroactive a modelului la evoluțiile din domeniul nuclear și radiologic. Rezultatele obținute au confirmat încă o dată aplicabilitatea și eficiența modelului, precum și o viziune asupra căilor și a pașilor privind dezvoltarea programului de securitate cibernetică la nivel național. Se constată faptul că politicile și managementul, precum și conștientizarea riscurilor cibernetice, se numără printre factorii inițiali care duc la dezvoltarea unui program de securitate avansată. În continuare, se evidențiază cum alte dimensiuni se dezvoltă, precum formarea utilizatorilor și gestionarea riscurilor cibernetice pe baza legilor, reglementărilor și cerințelor organizaționale sau naționale.

În **Concluzii** au fost evidențiate principalele rezultate ale acestei teze de doctorat. Metoda logică a fost utilizată pentru a rezuma cercetările în utilizarea SSD în scopul propus, precum și pentru a propune direcții viitoare de cercetare în acest domeniu.

Conceptul de SSD poate fi utilizat pentru a identifica și gestiona riscurile cibernetice, precum și pentru a răspunde la incidente. SSD a fost propus ca un modul pentru a facilita integrarea sa în alte cadre de management al riscului, precum și pentru a minimiza costurile. Acest concept se concentrează pe toate rolurile din cadrul unui IC, de la operatori până la decidenți, și se bazează pe analiza impactului elementelor factorului uman asupra sistemelor informaționale pentru domeniul dat. Modelul, sistemul formal inteligent și aplicația de evaluare a securității cibernetice au fost dezvoltate pornind de la condițiile necesare dezvoltării unui program eficient de securitate cibernetică, ținând cont de rolul tehnologiilor și al factorilor umani în domeniul IC.

Rezultatele obținute reprezintă o soluție originală la provocările actuale privind gestionarea riscurilor cibernetice în domeniul IC. Rezultatele sunt cuprinzătoare și multilaterale și includ un concept de SSD, un model de evaluare a maturității securității cibernetice, un sistem formal metric inteligent și o aplicație prototip ce implementează acest sistem. Rezultatele sunt universale pentru domeniul IC și reprezintă o soluție modernă pentru a crește nivelul de securitate cibernetică și a minimiza riscurile aferente. Conceptul, modelul, sistemul formal metric inteligent sau aplicația pot fi utilizate separat sau complementar și pot fi adaptate pentru orice tip de IC, în funcție de cerințe.

Rezultatele acestei teze sunt soluții practice și ușor de utilizat pentru evaluarea securității cibernetice și pot contribui operativ și direct la asigurarea securității cibernetice a infrastructurilor critice. Acest lucru este important pentru menținerea și dezvoltarea continuă a TI în domeniul IC. Rezultatele nu conțin produse software sau programe care pot deveni cu ușurință învechite, în timp ce conceptul și sistemul formal metric inteligent pot fi ușor utilizate și adaptate pentru fiecare IC. Toate rezultatele obținute, dezvoltate, prototipurile și conceptele au fost publicate în reviste *peer-review*, lucrări ale conferințelor sau a seminarelor științifice.

CONCLUZII GENERALE ȘI RECOMANDĂRI

Managementul riscurilor cibernetice în IC este un subiect de cercetare prioritar datorită actualității amenințărilor cibernetice în toate domeniile. Numărul de atribute și cantitatea de date care trebuie luate în considerare în procesul de gestionare a riscurilor cibernetice depășesc adesea abilitățile umane. Luarea deciziilor asistată de computer reprezintă soluții moderne la această problemă și pot contribui semnificativ la îmbunătățirea eficienței și a resurselor consumate pentru acest proces. În urma cercetărilor efectuate, se pot face următoarele patru concluzii generale:

1. **SSD reprezintă soluții viabile pentru managementul riscurilor cibernetice în IC**. Pe baza cercetării efectuate prin analiza sistematică a literaturii, se poate afirma că, deși procesele de management al riscurilor sunt de interes în cercetare, nu a existat niciun SSD care să abordeze întreg procesul de management al riscurilor cibernetice în domeniul IC, începând cu identificarea riscului până la clasificare, atenuare și evaluare. Este recomandată includerea elementelor cheie pe parcursul dezvoltării conceptului de SSD propus, și anume: factorul uman, publicul țintă, reziliența, modelarea și simularea, complexitatea și interdependența. Este propusă și dezvoltarea SSD ca modul, pentru a spori eficiența costurilor și rata de implementare. A fost identificată, ca necesitate critică evaluarea factorului uman în timpul proiectării, dezvoltării și utilizării SSD.
2. **A fost dezvoltat un concept de SSD pentru managementul riscurilor cibernetice în domeniul IC,** care este unul dintre rezultatele originale ale acestei teze. S-a decis pentru a evita problemele de securitate cibernetică create de SSD ca program în situațiile în care o aplicație devine depășită și conține vulnerabilități cunoscute într-o perioadă foarte scurtă de timp, ca SSD să fie descris la nivel conceptual. Una dintre cerințele conceptului de SSD este să permită și să fortifice utilizatorul final, decidentul sau operatorul să ia în mod eficient și rapid o decizie informată cu privire la modul de abordare a riscurilor cibernetice identificat. Acest rezultat este susținut prin recomandarea unor aspecte tehnice și metodologii privind construirea SSD-ului, cum ar fi respectarea standardelor pentru proiectarea unei interfețe prietenoase și utilizabile, evaluarea elementelor factorului uman și utilizarea automatizării acolo unde tipul de sarcini o permit și riscul este redus. Din punct de vedere arhitectural, a fost proiectat sistemul de limbaj și de prezentare și propuse tipuri de date pentru a fi utilizate de aceste sisteme, care sunt corelate cu contextul și domeniul de aplicare al SSD. Aceste componente arhitecturale sunt plasate în centrul SSD și sunt direct responsabile de eficiența și performanța percepută a SSD. De asemenea, au fost incluse ca cerințe evaluarea contextului IC și a procesului de management a riscurilor în timpul proiectării SSD pentru a asigura că acestea sunt abordate încă din fazele inițiale. Acest lucru asigură că SSD este adecvat scopului. A fost analizat impactul dimensiunii umane, atât pozitiv, cât și negativ,

asupra SSD care urmează să fie utilizat în domeniile securității și siguranței. Sunt prezentate recomandări cu privire la modul de reducere a impactului negativ al elementelor factorului uman asupra SSD propus, și în principal: utilizarea unui SSD modular; utilizarea standardelor pentru dezvoltarea interfeței cu utilizatorul și codificarea, pentru a reduce costurile și a îmbunătăți gradul de utilizare a platformei; utilizarea tehnologiilor moderne, cum ar fi biometria, pentru a evalua starea fizică a operatorilor atunci când se iau decizii critice. Ca o soluție pentru a depăși limitările cunoscute cauzate de elementele factorului uman precum percepția, abilitățile, capacitatea de a lua decizii corecte în condiții de stres, precum și pentru a reduce costurile și a îmbunătăți eficiența, se propune utilizarea luării autonome a deciziilor. Au fost identificate beneficiile și criteriile pentru automatizarea anumitor tipuri de sarcini, pentru a reduce oboseala utilizatorului și pentru a îmbunătăți eficiența generală a utilizării SSD.

3. **A fost dezvoltat un model de evaluare a maturității securității cibernetice** care a demonstrat aplicabilitate și eficiență pentru diferite tipuri de IC. Modelul a fost dezvoltat pentru a estima eficiența SSD utilizată în domeniul IC. Un rezultat original suplimentar atins prin intermediul acestui model reprezintă capacitatea de a oferi soluții pe mai multe dimensiuni, modelul fiind capabil de a identifica aria ce necesită investiții – tehnologiile sau formarea utilizatorilor. Modelul poate fi utilizat pentru a facilita auditurile periodice de securitate a informațiilor, fiind aliniat cu ISO 27001. Modelul a fost revizuit de organizații externe, care au confirmat originalitatea, aplicabilitatea aspectelor inovatoare în domeniul IC precum și eficiența acestuia. Atributele modelului au fost incluse în seminarele programului de master pentru cursul „Securitate nucleară și radiologică” la Universitatea Tehnică a Moldovei. În premieră a fost dezvoltată Baza de cunoștințe „Securitatea cibernetică în infrastructuri critice”, în baza căreia a fost dezvoltat sistemul formal metric inteligent „Securitatea cibernetică în infrastructuri critice”. Sistemul formal metric inteligent a fost înregistrat la AGEPI cu Drept de autor. De asemenea, a fost elaborat prototipul aplicației „Securitatea cibernetică în infrastructuri critice”. Prototipul amplifică rezultatele procesului de evaluare prin adăugarea de recomandări în dependență de situație. A fost prezentată dezvoltarea programului de securitate cibernetică în domeniile de IC din Republica Moldova, iar aplicarea retroactivă a modelului la domeniile IC a validat utilizarea acestuia în astfel de scenarii și, în plus, a ajutat la definirea recomandărilor privind îmbunătățirea maturității securității cibernetice la nivel național.

4. **Au fost identificate tendințele și pașii în stabilirea unui program de securitate cibernetică în domenii de IC**, prin analiza retroactivă a dezvoltării securității cibernetice în Republica Moldova. Astfel, se propun recomandări cu privire la modul de îmbunătățire și simplificare a acestui proces. A fost efectuată o cercetare aprofundată a dezvoltării cadrului

legislativ nuclear și radiologic în Republica Moldova, în urma căreia s-a identificat rolul din ce în ce mai mare al securității cibernetice la țintele critice și a accentului necesar asupra elementelor de securitate cibernetică în evaluarea sistemelor de securitate fizică. A fost realizată și o analiză cronologică a rolului și atenției acordate securității cibernetice în cadrul legislativ nuclear și radiologic. Securitatea cibernetică în domeniul medicinii a fost evaluată dintr-o prezentare generală la nivel înalt. Ca urmare, au fost identificate vulnerabilități comune împotriva sistemelor din medicină, precum și limitările legate de elementele factorului uman. Au fost propuse recomandări din perspectiva controalelor tehnice care trebuie implementate, precum și pe partea de politici și management pentru a îmbunătăți cooperarea orizontală la nivel național și internațional. Au fost de asemenea prezentate tendințele pe care organizațiile le urmează în procesul de creștere a nivelului de maturitate a securității cibernetice.

Recomandări de cercetări viitoare

Deși cercetarea s-a axat pe utilizarea SSD în IC, s-a observat că această problemă poate fi analizată din diferite puncte de vedere. În baza acestor cercetări se recomandă următoarele:

- Evaluarea din alte perspective a impactului dimensiunii umane asupra DSS în IC;
- Identificarea standardelor sau a cadrelor de interoperabilitate care ameliorează managementul riscurilor în IC;
- Perfecționarea cadrului legislativ a securității cibernetice în domeniul medicinii și revizuirea eficienței modelului propus pentru țări sau regiuni selectate;
- Implementarea controalelor de securitate integrate.

BIBLIOGRAFIE

1. Legea nr. 257 din 22.11.2018 *privind aprobarea Strategiei de securitate a informațiilor a Republicii Moldova pentru anii 2019-2024*, MO al RM nr.13-21 din 18.01.2019
2. European Commission 2020, Joint communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade, [Online] la adresa: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN. accesat la 3 august 2021
3. European Commission 2020, Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities, COM(2020) 829, [Online] la adresa: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN, accesat la 3 august 2021
4. United Nations 2021, Report of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security (A/76/135), accesat la 20 iulie 2021
5. World Economic Forum 2020. The Global Risks Report 2020. [Online] la adresa: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf accesat la 20 martie 2020
6. European Medicine Agency 2018, Data anonymization - a key enabler for clinical data sharing, [Workshop report], 2018, [Online] la adresa: https://www.ema.europa.eu/en/documents/report/report-data-anonymisation-key-enabler-clinical-data-sharing_en.pdf pp 14-15, accesat la 3 august 2021
7. ENISA 2020, ENISA Threat Landscape 2020, [Online] la adresa, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport, accesat la 3 august 2021
8. VERIZON - 2021 Data Breach Investigations Report, 2021
9. VERIZON - 2019 Verizon Incident Preparedness and Response Report. 2019
10. **BUZDUGAN, A**. Integration of Cyber Security in Healthcare Equipment. In: Tiginyanu I., Sontea V., Railean S. (eds) 4th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2019, IFMBE Proceedings, vol 77, pp 681-684, Springer Nature Switzerland AG (2020), DOI:10.1007/978-3-030-31866-6_120
11. CĂPĂŢÂNĂ, Gh., CIOBU, V., PALADI, F.: Adaptive Application for Complex Systems Modeling. In: Conference of Mathematical Society of the Republic of Moldova. 4, Chişinău. Chişinău: Centrul Editorial-Poligrafic al USM, pp. 487-490. ISBN 978-9975-71-915-5. (2017)
12. FILIP, F.G. (2020). *DSS - A Class of Evolving Information Systems*. In: Dzemyda G., Bernatavičienė J., Kacprzyk J. (eds) Data Science: New Issues, Challenges and Applications. Studies in Computational Intelligence, vol 869. Springer, Cham. DOI:10.1007%2F978-3-030-39250-5_14
13. **BUZDUGAN, A.,** CĂPĂȚÂNĂ, Gh. (2022) Cyber Security Maturity Model for Critical Infrastructures. In: Ciurea, C., Boja, C., Pocatilu, P., Doinea, M. (eds) Education, Research and Business Technologies. Smart Innovation, Systems and Technologies, vol 276. Springer, Singapore. The 20th International Conference on Informatics in Economy, Bucharest University of Economic Studies, https://doi.org/10.1007/978-981-16-8866-9_19
14. CERNEI, V., Models and methods for governmental cyber risk management. In: The Collection. Economic security in the context of sustainable development. Ediția 6, 10 dec 2021, Universitatea de Stat „Alecu Russo" din Bălți, pp. 258-261. ISBN 978-9975-155-01-4.
15. BOLUN, I., CIORBA, D., ZGUREANU, A., BULAI, R., CALIN, R., BODOGA, C.: Informatics security assessment in the Republic of Moldova. In: Journal of Engineering Sciences. vol. XXVII, no. 4 (2020), pp. 103-119. ISSN 2587-3474. DOI:10.5281/zenodo.4288297

ADNOTARE

Teza „Sisteme de suport decizional pentru identificarea și diminuarea riscurilor cibernetice în infrastructuri critice” este scrisă în limba română de dl Aurelian BUZDUGAN pentru îndeplinirea cerințelor pentru doctorat în informatică, specialitatea 121.03 – Programarea calculatoarelor. Teza a fost elaborată la Universitatea de Stat din Moldova, Chișinău, 2022.

Structura tezei: Teza constă din Introducere, trei capitole, concluzii și recomandări. Bibliografia cuprinde 191 de titluri. Lucrarea conține 131 de pagini de text de bază, 17 figuri, 4 tabele și 7 anexe. Rezultatele obținute au fost publicate în 28 de lucrări științifice cu un volum de peste 7 coli autor.

Cuvinte cheie: sisteme suport decizionale, infrastructuri critice, managementul riscurilor cibernetice, sistem limbaj, sistem de prezentare, dimensiune umană, model pentru evaluarea maturității securității cibernetice, baza de cunoștințe, sistem formal metric inteligent, arhitectura aplicației.

Scopul: dezvoltarea, evaluarea și validarea potențialului și a utilizării SSD în gestionarea riscurilor cibernetice în IC.

Obiective de cercetare: evaluarea utilizării SSD în gestionarea riscurilor în contextul IC; identificarea elementelor și a cerințelor specifice pentru dezvoltarea conceptului de SSD în corelare cu contextul dictat de cerințele de siguranță și securitate în IC; evaluarea factorilor și impactul acestora asupra eficienței percepute a sistemelor informaționale; dezvoltarea și validarea unui model, sistem formal metric inteligent și aplicație pentru evaluarea maturității securității cibernetice în IC; evaluarea și propunerea recomandărilor privind cadrul legal de securitate cibernetică a IC în Republica Moldova.

Noutatea și originalitatea științifică: un concept SSD, un model de evaluare a maturității securității cibernetice și a eficienței SSD, o bază de cunoștințe, un sistem formal metric inteligent și un prototip software ce implementează acest sistem. Prototipul permite totodată aplicarea modelului de evaluare a securității cibernetice și prezintă rezultatele printr-o interfață ușor de utilizat și metrici ușor de înțeles.

Principala problemă științifică rezolvată: asigurarea securității cibernetice IC printr-o soluție inovativă bazată pe un concept de SSD dezvoltat ca modul și destinat identificării, clasificării și managementului riscurilor cibernetice în IC.

Semnificația teoretică: A fost dezvoltat un concept de SSD pentru evaluarea maturității securității cibernetice. Conceptul este suplimentat de un model aplicabil pentru evaluare externă sau autoevaluare a securității cibernetice IC. Adițional, a fost dezvoltat un sistem formal metric inteligent și un prototip software care implementează procesul de evaluare selectat.

Valoarea aplicativă: un model pentru evaluarea eficienței SSD, un sistem formal metric inteligent și un prototip software.

Implementarea rezultatelor științifice: Modelul SSD a fost premiat cu Medalia de bronz la Salonul Internațional al Inovării și Cercetării Științifice CadetINOVA 2021, Medalia de bronz la Salonul Internațional de Invenții și Inovații „Traian Vuia” 2022, avizat pozitiv de Administrația Slovenă pentru Securitate Nucleară, Institutul Național de Metrologie din Moldova, Universitatea Tehnică a Moldovei, precum și inclus în curriculumul de master al disciplinei „Securitate nucleară și radiologică” din cadrul UTM. Dreptul de autor privind sistemul formal metric inteligent a fost înregistrat la AGEPI.

ANNOTATION

The thesis „Decision Support Systems for Identification and Minimizing Cyber Security Risks in Critical Infrastructures" is written in Romanian by Mr. Aurelian BUZDUGAN for fulfilling the requirements for PhD in informatics, speciality 121.03 - Computer Programming. The thesis has been elaborated at the Moldova State University, Chisinau, 2022.

The structure of the thesis: The thesis consists of an Introduction, three chapters. Conclusions and Recommendations, Bibliography of 191 titles. The main text amounts to 131 pages, including 17 figures, 4 tables and 7 annexes. The obtained results were published in 28 scientific papers with a volume of over 7 sheets of author.

Keywords: decision support systems, critical infrastructures, cyber risk management, language system, presentation system, human dimension, a model for cyber security maturity assessment, knowledge base, intelligent formal metric system, application architecture.

Research purpose: develop, evaluate and validate the use of a decision support system (DSS) in managing cyber risks in critical infrastructures (CI).

Research objectives: review the use of DSS in risk management in the context of CIs; identify the elements and peculiar requirements when developing the concept of using a DSS in a context and environment where safety requirement is critical; evaluate the factors and their impact upon perceived efficiency of information systems; develop and validate a model, metric intelligent formal system and application to evaluate cyber security maturity in CI; evaluate and propose recommendations on the cyber security legal framework in CI in the Republic of Moldova.

The scientific novelty and originality: an innovative DSS concept, an evaluation model of cybersecurity maturity and DSS efficiency, a knowledge base, a metric intelligent formal system, and a software prototype implementing this system. The prototype also enables the application of the cybersecurity assessment model and presents the results through an easy-to-use interface and easy-to-understand metrics.

The main scientific problem solved: ensuring CI cyber security through an innovative solution based on an DSS concept developed as a module and intended to identify, classify and manage cyber risks in CI.

The theoretical significance: a developed concept of DSS for cybersecurity maturity assessment. The concept is supplemented by an applicable model for external assessment or self-assessment of CI cybersecurity. Additionally, a metric intelligent formal system and a software prototype implementing the selected evaluation process were developed.

The applicative value: a model for DSS efficiency evaluation, a metric intelligent formal system and a software prototype.

The implementation of results: the DSS model has been awarded the Bronze Medal at CadetINOVA 2021 - Innovation and Scientific Research Exhibition, Bronze medal at the International Exhibition of Inventions and Innovations „Traian Vuia" 2022, has been positively evaluated and assessed as applicable for the CI domain by the Slovenian Nuclear Security Administration, National Institute of Metrology from Moldova, Technical University of Moldova, as well as included in the master's degree curriculum in „Nuclear and Radiological Safety" within Technical University of Moldova. The copyright on the intelligent formal metric system has been registered with AGEPI.

АННОТАЦИЯ

Диссертация «Системы поддержки принятия решений для идентификации и минимизации киберрисков в критических инфраструктурах» написана на румынском языке г-ном Аурелиан БУЗДУГАН в соответствии с требованиями докторской программы в информатике, специальность 121.03 - компьютерное программирование. Диссертация разработана в Государственном Университете Молдовы, Кишинев, 2022 г.

Структура диссертации: Диссертация состоит из введения, трех глав, выводов и рекомендаций, библиографии из 191 названий. Работа содержит 131 страницы основного текста, 17 рисунков, 4 таблиц и 7 приложений. Полученные результаты опубликованы в 28 научных работах объемом более 7 авторских листов.

Ключевые слова: системы поддержки принятия решений (СППР), критические инфраструктуры (КИ), управление киберрисками, языковая система, система представления, человеческое измерение, модель оценки зрелости кибербезопасности, база знаний, интеллектуальная формальная метрическая система, архитектура приложения.

Цель исследования: разработка, оценка и апробация потенциала и использования СППР в управлении киберрисками в КИ.

Задачи исследования: оценка использования СППР в управлении рисками в контексте КИ; определение специфических элементов и требований для разработки концепции СППР в соответствии с контекстом, продиктованным требованиями безопасности в КИ; оценка факторов и их влияние на воспринимаемую эффективность информационных систем; разработка и валидация модели, формальной системы и приложения для оценки зрелости кибербезопасности в КИ; оценка и предложение рекомендаций по нормативно-правовой базе кибербезопасности в КИ в Республике Молдова.

Научная новизна и оригинальность: оригинальная концепция СППР, модель оценки зрелости кибербезопасности и эффективности СППР, база знаний, интеллектуальная формальная система и программный прототип, реализующий эту систему. Прототип также позволяет применять модель оценки кибербезопасности и представляет результаты с помощью простого интерфейса и простых показателей для понимания.

Главная решенная научная проблема: обеспечение кибербезопасности КИ за счет инновационного решения, основанного на концепции СППР, разработанного в виде модуля и предназначенного для выявления, классификации и управления киберрисками в КИ.

Теоретическая значимость. Концепция СППР была разработана для оценки зрелости кибербезопасности. Концепция дополняется применимой моделью внешней оценки или самооценки кибербезопасности КИ. Кроме того, были разработаны интеллектуальная формальная система и прототип программного обеспечения, реализующие выбранный процесс оценки.

Практическая ценность работы: модель оценки эффективности СППР, формальная система и прототип программного обеспечения.

Внедрение научных результатов: Модель СППР была награждена Бронзовой медалью на международном конкурсе инноваций и исследований CadetINOVA 2021, Бронзовой медалью на Международной выставке изобретений и инноваций „Traian Vuia” 2022, положительно оценена Управлением Ядерной Безопасности Словении, Национальным Институтом Метрологии Молдовы, включена в учебную программу мастерата ТУМ по дисциплине «Ядерная и Радиационная Безопасность». Авторское право на интеллектуальную формальную метрическую систему было зарегистрировано AGEPI.

BUZDUGAN AURELIAN

SISTEME DE SUPORT DECIZIONAL PENTRU IDENTIFICAREA ȘI DIMINUAREA RISCURILOR CIBERNETICE ÎN INFRASTRUCTURI CRITICE

121.03 Programarea calculatoarelor

Rezumatul tezei de doctor în informatică

Aprobat spre tipar: 25.10.2022
Hârtie ofset. Tipar ofset.
Coli de tipar.: 1,8

Formatul hârtiei 60x84 1/16
Tiraj 50 ex
Comanda nr. 170

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