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

Cu titlu de manuscris
C.Z.U.: 004.056(043.3)

BUZDUGAN AURELIAN

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

121.03 Programarea calculatoarelor

Teza de doctor în informatică

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

Membrii Comisiei de îndrumare:
Beldiga Maria, doctor în informatică,
conferențiar universitar
Cerbu Olga, doctor în științe fizico-matematice, conferențiar universitar
Ciobu Victor, doctor în științe fizice
conferențiar universitar

Autor: Buzdugan Aurelian

CHIȘINĂU, 2022

Cuprins

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.

LISTA ABREVIERILOR

ACM – Asociația pentru Mașini de Calcul

AGEPI - Agenția de Stat pentru Proprietatea Intelectuală

CVE – Common Vulnerability Enumerator

DPC – Controler de Proces Direct

SSD – Sistem Suport Decizional

HFI – Human Factor Integration

AIEA – Agenția Internațională pentru Energie Atomică

IC – Infrastructură Critică

ICS – Sisteme Industriale de Control

ISO – Organizația Internațională de Standardizare

IoT – Internetul lucrurilor

TI – Tehnologia informației

NIST – Institutul Național de Standarde și Tehnologie

CNSSN – Centrul Național de Suport pentru Securitate Nucleară

CRN – Comisia de Reglementare Nucleară din SUA

TO – Tehnologii Operaționale

PLC – Controler Logic Programabil

SCADA – Control de Supraveghere și Achiziție de Date

TAM – Modelul de Acceptare a Tehnologiilor

TTP – Tactici, tehnici și proceduri

INTRODUCERE

Actualitatea și importanța temei selectate

Evoluția impresionantă a tehnologiilor informaționale (TI) au transformat lumea într-una interdependentă cu avantaje enorme, dar însoțită și de dezavantaje prin dependența tot mai mare de sistemele TI. Protecția infrastructurilor critice este o prioritate la nivel național [1], european [2, 3] și global [4]. Această teză în domeniul securității cibernetice se încadrează în prioritatea strategică de Competitivitate Economică și Tehnologii Inovatoare, TI și dezvoltare digitală a Programului Național de Cercetare și Inovare al Republicii Moldova pentru 2020-2023. Cel mai recent raport al Grupului de experți guvernamentali al Națiunilor Unite privind promovarea comportamentului responsabil al statului în spațiul cibernetic în contextul securității internaționale, a identificat, de asemenea, riscurile cibernetice față de infrastructurile critice (IC) și a propus norme privind stoparea oricăror atacuri împotriva infrastructurii IC din alte țări, asigurarea unei protecții adecvate a IC, precum și cooperarea cu alte state în schimbul de cunoștințe și expertiză în acest sens [5]. Pandemia din anul 2020 și trecerea la munca la distanță au expus și mai mult acest tip de organizații la atacuri cibernetice. Având în vedere faptul, că majoritatea operatorilor încă nu aplică proceduri standard de securitate, cum ar fi analiza amenințărilor [6], se constată că numărul și impactul atacurilor cibernetice asupra organizațiilor din sectorul IC este în creștere.

Sectorul de sănătate, critic în ultimii ani din cauza pandemiei, nu este o excepție în acest caz. S-a demonstrat anterior că atacurile cibernetice pot avea un impact asupra unui sistem cu TO utilizat în asistența medicală [7]. Numai în perioada pandemiei din anul 2020, au existat multiple incidente de *ransomware* în instituții medicale precum în România în iunie 2020 [8], Düsseldorf în septembrie 2020 [9] sau Finlanda în octombrie 2020 [10]. În această perioadă, aceste instituții, suprasolicitate și în pragul colapsului operațional, au jucat un rol cheie în tratarea celor afectați de virusul SARS-CoV-2. Mai mult, diverse instituții care sunt considerate IC, precum Ministerul Afacerilor Externe austriac sau Thyssen-Krupp, au fost și ele victime ale atacurilor cibernetice [8]. Pe lângă importanța pentru activitatea societății și a economiei, multe dintre IC prelucrează și date cu caracter personal. Acest lucru induce o obligație legală și constituțională de a proteja confidențialitatea, integritatea și disponibilitatea acestor date, precum și de a răspunde eficient în cazul incidentelor de securitate.

Riscurile pentru IC pot proveni din interiorul organizației, intenționat sau neintenționat, precum și din exterior. 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 deteriora fizic

sistemul informațional. Atacurile actorilor statali creează riscuri și mai mari, deoarece acești actori pot avea un nivel înalt și sofisticat de expertiză și cunoștințe, precum și acces și resurse suficiente pentru a-și atinge obiectivele. Mai mult decât atât, dezvoltarea rapidă a sistemelor de inteligență artificială și internet of things (IoT) contribuie nu doar la securitatea IC, ci deschid și o nouă sferă de amenințare mult mai complexă și inteligentă, momentan neconsiderată în securitatea sistemului.

Sistemele TI care susțin operațiunile în IC sunt supuse continuu riscurilor. Anterior, analiza riscului a vizat funcționarea în siguranță a sistemelor IC și prevenirea daunelor fizice. În prezent, însă, acestea includ și sisteme informatice (active digitale) ca parte a sistemelor de securitate. De asemenea, interconectarea IC 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* a fost de 10%, ceea ce reprezintă o creștere dublă față de 2020. De asemenea, rata incidentelor care au afectat zonele corespunzătoare IC este de aproximativ 10% din numărul total de incidente [11]. Dacă se analizează timpul de răspuns la incident, peste 90% dintre incidente au avut loc în câteva minute, dintre care 70% au fost depistate abia după câteva luni. Astfel, timpul necesar pentru a efectua un atac cibernetic este redus în comparație cu eforturile necesare pentru a securiza și monitoriza aceste componente digitale.

În plus, un interes personal îl reprezintă progresul în domeniul TI în programele de colectare și analiză a unui volum mare de date, care oferă posibilități organizațiilor și persoanelor fizice în detectarea anomaliilor care pot corespunde incidentelor de securitate. Aceste modele și tehnici necesită adaptări și îmbunătățiri regulate, ca răspuns la identificarea de noi metode sau tehnici de atac. Securitatea cibernetică devine adesea o cursă contra cronometru pentru a asigura oportunitatea și eficacitatea acestor controale de securitate. Pe de altă parte, numărul tehnicilor de atac se dezvoltă exponențial. Inteligența artificială și *machine learning* sunt câteva aspecte care ar putea fi și sunt aplicate de ambele părți. Sinergia 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 compromite securitatea unui sistem la un nivel mult mai înalt. Cu toate acestea, multe dintre riscurile de securitate cibernetică care există în prezent în infrastructurile critice ar putea fi minimizate prin implementarea unor bune practici de securitate care pot fi preluate și adaptate din domeniul TI tradițional.

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 noastre, majoritatea rezultatelor au fost prezentate sub formă narativă 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 maturității securității cibernetice pentru domeniile IC (Anexa 1) a fost dezvoltat și poate fi utilizat pentru entități individuale de IC. În plus, a fost dezvoltat un sistem formal metric inteligent și un prototip software în Python care facilitează utilizarea și integrările viitoare în metodologiile generale de management al riscului (Anexa 7). Modelul a fost validat de următoarele organizații:

1. Autoritatea Slovenă de Securitate Nucleară, abilitată de procesul de autorizare a entităților nucleare și radiologice din Slovenia, a confirmat aplicabilitatea și utilitatea acestui model. (Anexa 2).
2. Institutul Național de Metrologie din Moldova a confirmat utilitatea ca metodă expresă de evaluare a maturității securității cibernetice a entităților critice. Modelul de evaluare propus a fost, de asemenea, identificat ca fiind util în timpul auditurilor ISO în domeniul securității informațiilor (Anexa 3)
3. Salonul Internațional al Inovării și Cercetării Științifice Studențești Cadet INOVA'21, organizată de Academia Forțelor Terestre Nicolae Bălcescu (Sibiu, România), a conferit acestui model Medalia de Bronz (Anexa 4).
4. Centrul Național de Suport al Securității Nucleare de la Universitatea Tehnică a Moldovei (Anexa 5), care se ocupă de educația și conștientizarea riscurilor în domeniul nuclear și radiologic, a testat și apreciat modelul ca aplicativ în domeniul IC. Criteriile propuse care fac parte din model au fost confirmate a fi utile atunci când se efectuează evaluări specifice de securitate nucleară. Modelul este inclus în curriculumul și fișa disciplinei „Securitate nucleară și radiologică” (F.02.O.007) pentru activități practice și seminare pentru Programul de Master la specialitățile „Ingineria Biomedicală” și „Microelectronica și Nanotehnologii” [12].
5. AGEPI a înregistrat dreptul de autor privind sistemul formal metric inteligent „Securitatea cibernetică în infrastructurile critice” (Seria 0, Nr. 7305 din 04.08.2022) [189].
6. Salonul Internaţional de Invenţii şi Inovaţii „Traian Vuia” 2022, Timișoara, România, a conferit acestui model Medalia de Bronz [191].

Pe baza celor de mai sus, rezultatele reprezintă soluții practice și ușor de utilizat pentru evaluarea securității cibernetice și contribuie operativ și direct la asigurarea securității cibernetice a IC. Acest fapt este critic pentru menținerea și dezvoltarea continuă a tehnologiilor informaționale în domeniul IC. Rezultatele nu conțin produse software sau coduri care pot deveni cu ușurință învechite, în timp ce sistemul formal metric inteligent și prototipul pot fi ușor utilizate și adaptate pentru fiecare IC. Rezultatele reprezintă o contribuție în realizarea prevederilor titl. I, pct. 10; pct.11, al. 7; titl. IV, pct 22, al. 3) ale Planului de Acțiuni pentru implementarea Strategiei de securitate a informațiilor pentru anii 2019-2024, aprobate de Parlamentul Republicii Moldova prin Legea 257 din 22 noiembrie 2018 [38].

Rezultate științifice înaintate spre susținere

- Argumentarea și descrierea utilizării SSD în managementul riscurilor cibernetice în domeniul IC, ce a condus la definirea conceptului teoretic ce poate fi ulterior utilizat în implementarea și adaptarea sistemelor informaționale pentru rezolvarea problemei identificate. Au fost identificate și argumentate elementele cheie care definesc arhitectura și funcționarea unui SSD în IC, și anume: factorul uman, publicul țintă, reziliența, modelarea și simularea, complexitatea și interdependența și factorii mediului de lucru.
- Evaluarea și analiza impactului elementelor factorului uman asupra SSD propus în domeniul IC, care a ajutat la identificarea tendințelor și a celor mai bune practici în faza de proiectare, dezvoltare și utilizare a sistemelor TI. Îmbunătățirea eficienței SSD se realizează prin:
    - utilizarea unui SSD modular pentru a facilita interoperabilitatea și integrarea;
    - utilizarea standardelor pentru dezvoltarea interfeței cu utilizatorul și codificare, pentru a reduce costurile și îmbunătățirea gradului de utilizare a platformei;
    - utilizarea tehnologiilor moderne, cum ar fi biometria, pentru evaluarea stării fizice a operatorilor în condiții de stres.
- Identificarea dimensiunilor și atributelor care au direcționat spre dezvoltarea și validarea unui model de evaluare a maturității securității cibernetice pentru IC. De asemenea, a fost elaborată în premieră Baza de cunoștințe „Securitatea cibernetică în infrastructuri critice”.
- Sistemul formal metric inteligent „Securitatea cibernetică în infrastructuri critice”, dezvoltat în premieră, cât și prototipul aplicației „Securitatea cibernetică în infrastructuri critice”.
- Evaluarea securității cibernetice în domeniile IC din Republica Moldova din perspectiva cadrului legal, care a contribuit la validarea modelului de evaluare a maturității securității

cibernetice. Rezultatele au confirmat aplicabilitatea retroactivă pentru un anumit domeniu al IC sau entitate individuală, precum și au contribuit la definirea unor recomandări privind îmbunătățirea maturității securității cibernetice la nivel național.

Aprobarea rezultatelor tezei

Rezultatele obținute în urma cercetării au fost prezentate și discutate la 24 de conferințe naționale și internaționale:

1. International Exhibition of Inventions and Innovations „Traian Vuia" 2022, 8-10 octombrie 2022, Timisoara, Romania.
2. 5th International Conference on Nanotechnologies and Biomedical Engineering (ICNBME 2021), 3-5 noiembrie 2021, Chișinău, Republica Moldova.
3. CTBT: Science and Technology 2021 Conference (SnT2021), 28 iunie – 1 iulie 2021, Viena, Austria.
4. 20th International Conference on Informatics in Economy (IE 2021), 14-15 mai 2021, București, România.
5. All Ukrainian scientific and technical conference young scientists - "Condition, Achievements and Prospects of Information Systems and Technologies", 22-23 aprilie 2021, Odessa, Academia Națională de Tehnologii Alimentare din Odesa, Ukraina.
6. Conferința științifică națională a doctoranzilor dedicată aniversării a 75 de ani ai USM „Metodologii contemporane de cercetare și evaluare", 22-23 aprilie 2021, Universitatea de Stat din Moldova, Chișinău, Republica Moldova.
7. The International Student Innovation and Scientific Research Exhibition Cadet INOVA'21 - Academia Forțelor Terestre Nicolae Bălcescu, Sibiu, 15 - 17 aprilie 2021, România.
8. 9th International Workshop on Soft Computing Applications, 27-29 noiembrie 2020, Arad, România.
9. Workshop on Intelligent Information Systems WIIS2020, 4-5 decembrie 2020, Chișinău, Republica Moldova.
10. Conferință științifică națională cu participare internațională - 2020, Institutul pentru Dezvoltare și Inovare, Universitatea de Stat din Moldova.
11. 4-th International Conference on Nanotechnologies and Biomedical Engineering (ICNBME 2019), 18-21 septembrie 2019, Chișinău, Republica Moldova.
12. CTBT: Science and Technology 2019 Conference (SnT2019), 24-28 iunie 2019, Viena, Austria (Poster de prezentare).

13. Vienna Cyber Security Week 2019 - Protecting Critical Infrastructure. 11-15 martie 2019, Viena, Austria.
14. Conference Telecommunications, Electronics and Informatics. Ediția a VI-a, 24-27 mai 2018, Chișinău, Republica Moldova.
15. NATO Advanced Research Workshop - "Functional Nanostructures and Sensors for CBRN Defense and Environmental Safety and Security "FNS-CBRN Defense - 2018", Chișinău, Republica Moldova.
16. Conferința Națională în Securitate Cibernetică, organizată de ISACA România cu sprijinul Băncii Naționale a României, 8 decembrie 2017, București, România (vorbitor invitat).
17. 9th International Conference on Microelectronics and Computer Science, 19-21 octombrie 2017, Chișinău, Republica Moldova.
18. IAEA International Conference on Nuclear Security, 5-9 decembrie 2016, Viena, Austria (Prezentare interactivă a posterului de conținut).
19. 3rd International Conference „Health Technology Management", 6-7 octombrie 2016, Chișinău, Republica Moldova (Prezentare poster).
20. 3rd International Conference on Nanotechnologies and Biomedical Engineering: ICNBME-2015, 23-26 septembrie 2015, Chișinău, Republica Moldova.
21. Conferința internațională a AIEA privind securitatea computerelor într-o lume nucleară: discuții și schimburi de experți, 1-5 iunie 2015, Viena, Austria.
22. Conferință internațională - Dezvoltarea și inovarea IMM-urilor: construirea unui viitor competitiv al Europei de Sud-Est, Ohrid (Macedonia de Nord), 3-4 octombrie 2014.
23. IAEA International Conference on Challenges Faced by Technical and Scientific Support Organizations (TSOs) in Enhancing Nuclear Safety and Security: Strengthening Cooperation and Improving Capabilities, 27 – 31 octombrie 2014, Beijing, China.
24. IAEA International Conference on Challenges Faced by Technical and Scientific Support Organizations (TSOs) in Enhancing Nuclear Safety and Security, 25-29 octombrie 2010, Tokyo, Japonia.

Rezultatele cercetării au fost de asemenea prezentate în cadrul expoziției din cadrul Parlamentului Republicii Moldova organizate în iulie 2022.

Publicații științifice

La tema prezentei teze de doctorat au fost publicate 28 lucrări (Anexa 6) dintre care: 22 ca autor principal, 6 în capacitate de coautor; 8 articole mono-autor și 3 rezumate mono-autor; 3 publicații în reviste științifice de specialitate, dintre care 2 în străinătate și 1 în Moldova (B+); 2

publicații indexate de Web of Science și 6 articole indexate în Scopus; 7 articole publicate în Springer și 2 articole acceptate pentru publicare în Springer la momentul depunerii tezei; 25 de articole, inclusiv rezumate, publicate în lucrările conferinței (în 19 articole ca autor principal).

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

Conținutul principal al tezei

În Introducere este prezentată actualitatea și importanța acestui subiect. S-a identificat scopul tezei de doctorat, obiectivele cercetării, metodologiile de cercetare, rezultatele științifice noi obținute în urma cercetării și valoarea lor aplicativă.

Capitolul I reflectă stadiul actual al cunoștințelor și cercetărilor în domeniu, privind amenințările cibernetice asupra infrastructurilor critice, elementele de bază în managementul riscurilor în acest domeniu și oportunitatea de a utiliza SSD pentru a ajuta la luarea deciziilor în procesul de management al riscurilor cibernetice din cadrul IC.

Capitolul II conține descrierea metodelor de cercetare utilizate. Acestea au stat la baza identificării lucrărilor existente pe această temă pentru a evita dublarea și suprapunerea cercetărilor, identificarea potențialelor direcții de cercetare și domenii care nu au fost suficient analizate. Capitolul conține descrierea elementelor care sunt luate în considerare pe parcursul elaborării conceptului pentru SSD propus, precum și în cercetările ulterioare. Este descrisă arhitectura propusă pentru acest SSD, precum și elementele specifice ale IC care stau la baza sistemului de limbaj și a sistemului de prezentare al SSD. Sunt prezentate aspectele legate de impactul factorului uman asupra proceselor din organizațiile de tip IC, precum și în cadrul utilizării SSD-ului propus. De asemenea sunt prezentate soluții sau recomandări pentru minimizarea riscurilor factorului uman asupra utilizării SSD. Au fost descrise cerințele pentru automatizarea unor procese, potențialul oferit precum și riscurile aferente.

Capitolul III propune un model de evaluare a nivelului de securitate cibernetică în cadrul IC, prin combinarea a patru valori cheie care afectează securitatea cibernetică: procesele și tipul de administrare, educația și evaluarea personalului, politicile privind condițiile de muncă și managementul riscurilor cibernetice. De asemenea este prezentat un sistem formal metric inteligent inovativ ce implementează acest model și o aplicație prototip. Este prezentat un studiu de caz privind necesitățile și metodele de ameliorare a securității cibernetice în cadrul sistemului medical și sunt descrise rezultatele unei analize a dezvoltării securității cibernetice în domeniul nuclear și radiologic în Republica Moldova. Au fost identificate și descrise principalele acte legislative, impactul acestora asupra securității cibernetice, precum și recomandări și soluții pentru

o integrare mai armonioasă a elementelor de securitate cibernetică în cadrul IC nuclear și radiologic din Republica Moldova.

În Concluzii au fost evidențiate principalele rezultate ale acestei teze de doctorat.

În anexe sunt prezentate modelul propus spre evaluare (Anexa 1), rezultatele evaluărilor externe ale modelului de către autoritatea de reglementare nucleară din Slovenia și autoritatea națională în domeniul metrologiei (Anexa 2, Anexa 3), rezultatul evaluării externe și implementării modelului prin prisma programului de studii de master a Universității Tehnice din Moldova (Anexa 4), medalia oferită pentru modelul prezentat la Salonul Internațional al Inovării și Cercetării Științifice Studențești Cadet INOVA'21 (Anexa 5), lista de publicații științifice pe tema acestei teze (Anexa 6) și codul sursă pentru programul dezvoltat (Anexa 7).

1. IMPACTUL SECURITĂTII CIBERNETICE ASUPRA INFRASTRUCTURILOR CRITICE

În acest capitol este prezentată o imagine de ansamblu asupra rolului IC în contextul societal actual și a provocărilor în gestionarea riscurilor cibernetice din acest domeniu. Au fost analizate detaliat impactul riscurilor cibernetice asupra domeniului IC. De asemenea sunt explorate cerințele în ceea ce privește gestionarea riscurilor cibernetice în cadrul IC, prin raportare la peisajul actual al amenințărilor la nivel mondial. Pe baza constatărilor din analiza literaturii de specialitate, se estimează măsura în care securitatea cibernetică este inclusă în managementul riscurilor pentru IC, precum și identificarea potențialelor direcții de cercetare.

Metodele și metodologiile de cercetare utilizate în acest capitol constau din procese de cercetare pozitiviste, precum și interpretative. Având în vedere caracterul multidisciplinar al acestui subiect, aceste metodologii au fost aplicate în mod interdependent pe parcursul întregii cercetări. Metodele au fost selectate și aplicate în funcție de tipul și volumul datelor analizate în vederea îndeplinirii obiectivelor propuse. Utilizarea materialelor și metodologiilor de cercetare științifică ajută la obținerea de rezultate și date tangibile pentru a asigura o prezentare independentă a situației actuale și pentru a identifica cea mai bună soluție pentru adaptarea SSD pentru managementul riscurilor cibernetice în domeniul IC. Acest tip de cercetare a fost atât translațional, pentru a rezolva chestiuni practice bazate pe cercetări fundamentale existente, precum procesele de management al riscului sau arhitectura SSD, cât și practic informat, pentru a identifica conceptul de SSD pentru managementul riscurilor cibernetice în IC, având în vedere specificul acestei întrebări de cercetare.

Pentru a asigura relevanța și calitatea rezultatelor obținute, s-a utilizat cercetarea prin analiza literaturii de specialitate, pentru a identifica cercetările existente, noi direcții de cercetare și caracteristicile unui SSD și impactul factorului uman asupra acestui lucru. Având în vedere tipul cercetării științifice, s-a utilizat analiza secundară a cercetărilor și lucrărilor elaborate în acest domeniu. În plus, a fost realizată și documentată o interpretare proprie a studiilor identificate.

Scopul principal al analizei selective a literaturii a fost identificarea și definirea scopurilor și întrebărilor care vor fi abordate în timpul studiilor. Analiza selectivă al literaturii a permis obținerea de date valoroase și critice pentru această teză.

Managementul riscurilor cibernetice depinde în mare măsură de procesarea unei cantități mari de informații despre risc și de un proces complex de analiză, clasificare și luare a deciziilor. Interconectarea, interdependența și digitizarea IC cresc considerabil cantitatea de date care trebuie evaluate pentru managementul riscurilor. Cunoașterea securității cibernetice este necesară pentru

a putea reflecta riscurile unui sistem TI în IC. Prelucrarea datelor în procesul de luare a deciziilor depășește limitele umane și ar trebui utilizate sisteme informatice pentru a sprijini acest proces. Acest lucru necesită o înțelegere profundă a impactului atacurilor cibernetice asupra domeniului IC, precum și a implicațiilor pe care aceasta le-ar putea avea. Una dintre întrebările cheie evaluate este dacă procesul existent de gestionare a riscurilor abordează în mod adecvat riscurile cibernetice. Această cercetare permite analiza provocările și necesitățile în managementul riscurilor cibernetice pentru IC. Accentul se pune pe identificarea și definirea soluțiilor pentru contracararea sau reducerea acestor riscuri prezentate printr-un sistem de sprijinire a deciziei.

Scopul acestui capitol este de a defini contextul riscului de securitate cibernetică și impactul pentru diferite domenii IC din puncte de vedere al cadrului legal și al managementul riscurilor. De asemenea este prezentată o argumentare mai cuprinzătoare a obiectivelor tezei, ce a servit ca reper pentru analiza și ajustarea obiectivelor inițiale.

1.1. Infrastructuri critice și societatea digitală

Spațiul cibernetic nu se limitează la granițele geografice, astfel încât rolul actorilor nestatali devine din ce în ce mai pronunțat. Infrastructurile critice, de exemplu cele din domeniul nuclear, energetic, medical, etc., conțin sisteme bazate pe computer care controlează și monitorizează majoritatea operațiunilor și funcționalităților lor. Securitatea cibernetică a acestor IC și a datelor prelucrate sunt necesare pentru menținerea securității naționale și a securității societății, precum și a prosperității și dezvoltării acestora.

Discuția privind protecția IC naționale este acum din ce în ce mai concentrată pe dimensiunea cibernetică, datorită faptului că toate infrastructurile au fost afectate de revoluția informațională și includ componente TI, în principal pentru funcțiile de comandă și control. Protecția IC este un subiect care depășește cu mult domeniul tehnic, fiind o provocare majoră legată de strategii și politici. Astfel, acest subiect necesită o abordare interdisciplinară, având în vedere impactul și nivelul de integrare a TI în IC, precum și moștenirea riscurilor de securitate cibernetică în acest domeniu. Analizând noile riscuri, se observă că sistemele TI sunt adesea necunoscute în ceea ce privește numărul posibil de vulnerabilități pe care le conțin. Aceste vulnerabilități pot duce la incidente de securitate sau atacuri cibernetice, care pot deteriora sau chiar interfera cu operațiunile de bază din cadrul unui IC. Astfel de atacuri cibernetice pot duce, de asemenea, la acces neautorizat, modificarea sau ștergerea datelor sensibile cu consecințe dezastruoase pentru securitatea națională, economică sau societală etc.

IC se află la baza funcțională a societății noastre, economiei, securității naționale și a altor domenii. Domeniile exemplificate în Figura 1.1 sunt considerate vitale pentru sănătatea, siguranța

și bunăstarea financiară a cetățenilor. Aceste domenii de activitate sunt fundamentale pentru funcționarea și dezvoltarea economiei, administrației publice și chiar a securității naționale. Definiția infrastructurii critice se referă la facilitățile fizice sau TI din domeniile menționate mai sus care, dacă sunt perturbate sau deteriorate, ar putea avea un impact asupra siguranței, securității sau economiei cetățenilor, precum și asupra funcționării efective a guvernului [13]. Prin urmare, orice intervenție neautorizată, întrerupere sau distrugere a echipamentului TI din cadrul unui IC ar putea duce la riscuri operaționale cu impact asupra securității sau chiar siguranței. Definiția de mai sus și elementele menționate sunt similare celor adoptate în țări precum SUA și Canada [14, 15]. Acest lucru se aplică și IC de care o țară este dependentă și nu este neapărat deținută sau controlată direct [16].

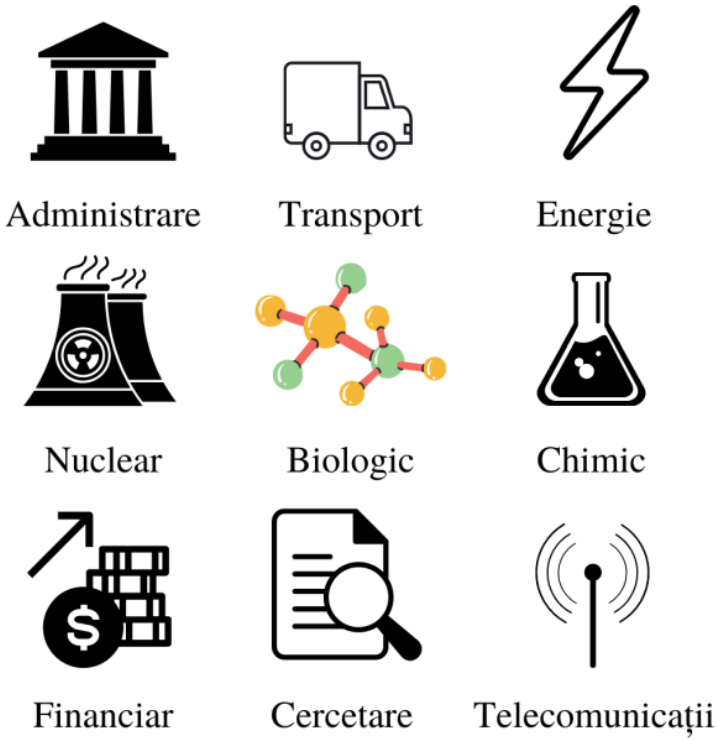

Fig. 1.1. Domeniile infrastructurii critice

Pe lângă importanța pentru activitatea societății și a economiei, multe dintre IC prelucrează și date cu caracter personal. Acest lucru induce o obligație legală și constituțională de a proteja confidențialitatea, integritatea și disponibilitatea acestor date, precum și de a răspunde eficient în cazul incidentelor de securitate.

Pe baza acestei descrieri se poate deduce că există diferite domenii ale IC, cum ar fi financiar, energetic, bancar, sau serviciile guvernamentale cheie. Acestea pot fi clasificate diferit în fiecare țară, totuși converg către definiția de mai sus.

Datorită proceselor masive de digitalizare, implicarea ciberneticii în IC poate fi considerată ca fiind tradițională în zilele noastre. Definiția securității cibernetice este încă discutabilă între diferite părți, dar este legată de ideea de a avea o anumită protecție împotriva utilizării greșite a datelor electronice sau a măsurilor luate pentru a apăra împotriva vătămării intenționate [17]. Securitatea cibernetică în IC este un domeniu relativ nou în care investițiile și cunoștințele pentru proiectarea, construirea și testarea sistemelor de securitate rentabile adesea lipsesc. IC utilizate astăzi nu au fost proiectate și construite pentru securitatea datelor, ci doar pentru siguranța operațională. Drept urmare, securitatea este adesea inclusă retroactiv, numai după anumite incidente sau amenințări evidente de securitate cibernetică. În prezent, deciziile inițiale de proiectare nu mai pot fi inversate. Când vine vorba de software, remedierea erorilor este costisitoare și dificil de implementat. În mod ideal, IC ar trebui proiectate pe baza cerințelor de securitate și confidențialitate încă de la început - asigurând astfel conceptele de securitate și confidențialitate prin proiectare. Implementarea și testarea acestor noi controale de securitate ar asigura alinierea la bunele practici actuale de securitate. Cu toate acestea, contextul în care s-au dezvoltat IC face adesea dificilă implementarea bunelor practici.

În sectoarele IC pot exista diferite niveluri de dependență de sistemele TI: de exemplu, în domeniul bancar sau financiar, sistemele TI joacă un rol crucial în majoritatea proceselor, în timp ce în sectorul de producție sau energie sistemele TI sunt integrate cu tehnologiile operaționale (TO) și formează așa-numita interfață ciber-fizică.

Prin definiție, TO se referă la computerele din sistemele de control industrial care sunt responsabile de acțiuni fizice precum monitorizarea liniei de producție, încălzirea/răcirea sistemului sau chiar procesul de producție. TO cuprind sisteme și tehnologii precum ICS, care sunt de obicei gestionate de sisteme SCADA prin sisteme PLC sau DPC. O reprezentare a TO este redată în Figura 1.2.

Prin urmare, rolul TI poate varia de la reprezentarea sistemului sau software-ul principal, la roluri auxiliare precum detectarea, detectarea anomaliilor sau îndeplinirea anumitor funcții în cadrul TO. Acesta din urmă ar avea o legătură puternică cu sistemele fizice, iar TI îndeplinește funcții precum monitorizarea, luarea deciziilor sau chiar controlul componentelor fizice.

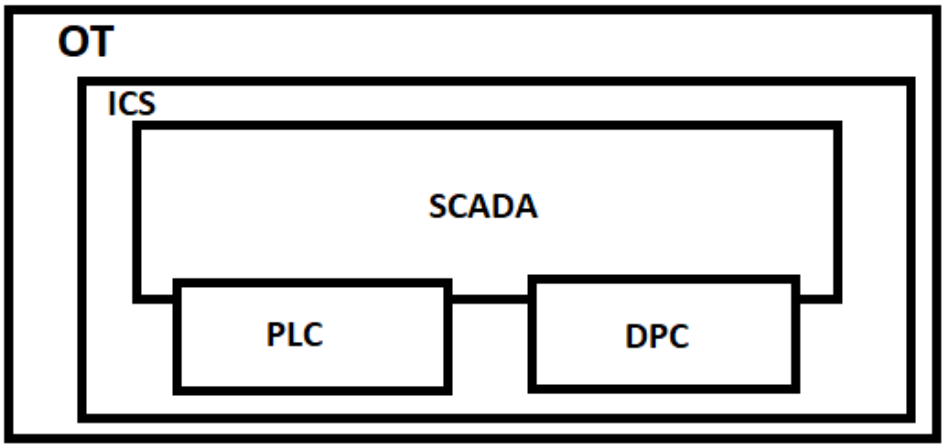

Fig. 1.2. Relația dintre TO, ICS, SCADA, PLC și DPC

Din punct de vedere istoric, sistemele TO au fost deconectate de la TI și s-au concentrat în principal pe integritatea și disponibilitatea operațiunilor sistemului. Acest lucru poate fi observat în Figura 1.3, care prezintă Modelul Purdue dezvoltat inițial în anii 1990 pentru a reprezenta relația dintre sistemele de control, limite și niveluri, precum și zonele de securitate [18].

Odată cu digitalizarea, sistemele din zona de producție conform Modelului Purdue tind să evolueze către o utilizare masivă a sistemelor computerizate. Datorită mărfurilor și altor necesități, granița dintre zonele inițial separate, cunoscute și sub denumirea de zone demilitarizate și rețeaua întreprinderii, tinde să se estompeze și astfel aceste zone au interconexiuni multiple. Prin urmare, un atac cibernetic asupra unei IC ar putea duce la evenimente ce afectează siguranța, cum ar fi daune fizice, scurgerea apei în baraje, supraîncărcarea rețelelor electrice în rețelele inteligente sau chiar controlul proceselor industriale (de exemplu, chimice, nucleare etc.) cu scopul de a crea dăuna. Astfel de atacuri sunt reale și actuale și reprezintă riscuri pentru economie, societate și cetățeni, atât la nivel național, cât și regional.

Următoarele provocări rezultă din interacțiunea dintre TI și TO:

1. Conceptele de siguranță și securitate necesită cooperarea între inginerii TI și TO, precum și factorii de decizie.
2. Controalele și conceptele de securitate TI trebuie adaptate și eventual reproiectate la necesitățile și specificul TO.
3. Gestionarea amenințărilor asupra sistemului TI și fizic necesită cooperare orizontală între echipele respective, cât și analiza unor cantități mari de diferite tipuri de date.

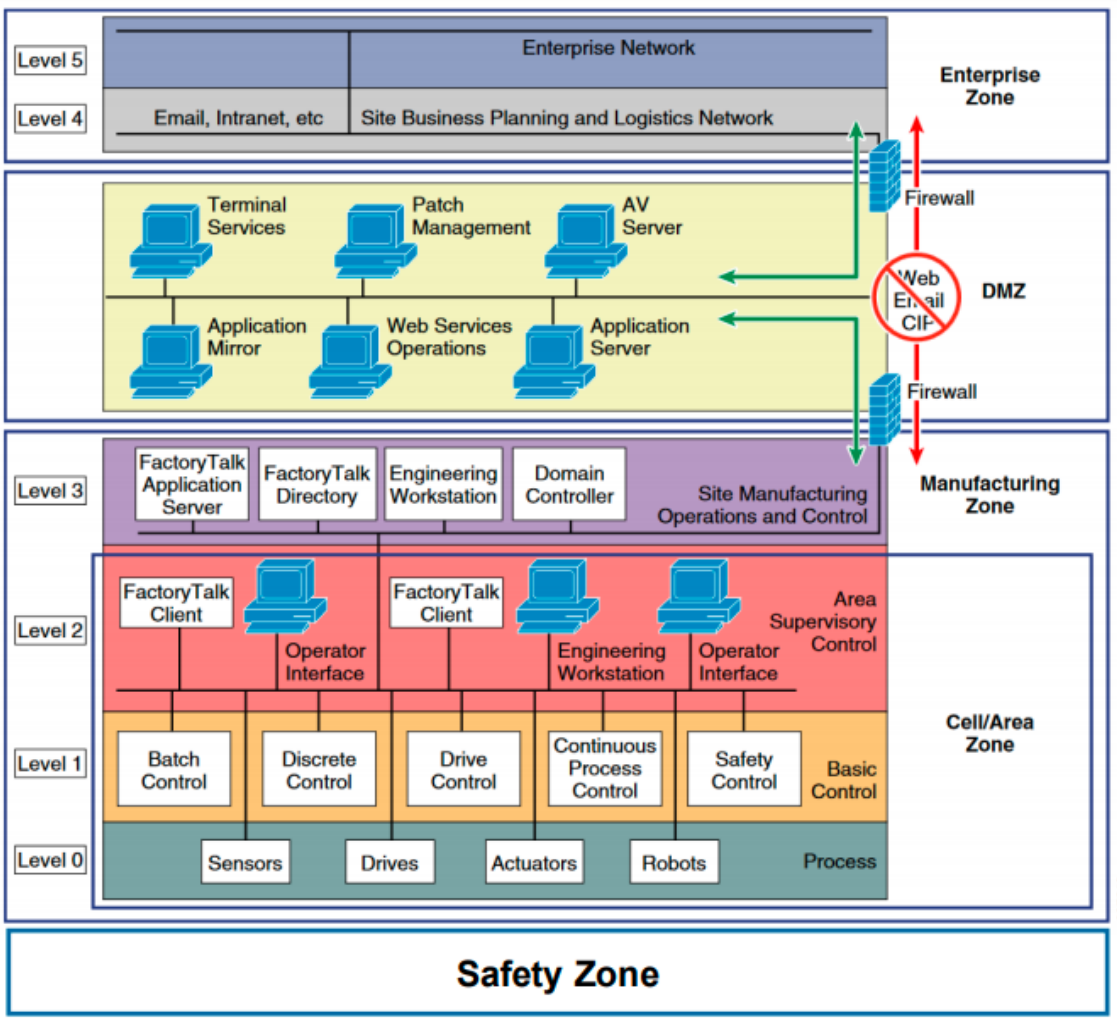

Fig. 1.3. Modelul Purdue [6]

Provocările de mai sus creează un context în care experții în securitate cibernetică și inginerii de instalații ar trebui să coopereze, pentru a putea defini vulnerabilitățile pe care sistemele TI le introduc în TO. De asemenea, este necesar un sistem de feedback pentru ca experții în securitate cibernetică să înțeleagă funcțiile și importanța componentelor fizice. Este necesară și o modelare detaliată a proceselor și a infrastructurii pentru a genera o perspectivă de ansamblu asupra riscurilor cibernetice în IC pentru factorii de decizie.

În plus, interconectarea dintre TI și TO mărește suprafața de atac și numărul de vulnerabilități care pot fi exploatate de către actorii amenințărilor. Un atac de la distanță asupra unei rețele izolate anterior a devenit acum posibil, deoarece multe dintre aceste sisteme sunt digitale și au conectivitate sporită, adesea chiar și la Internet. Acest lucru crește cerințele de a proteja datele sensibile, uneori chiar personale, precum și disponibilitatea și integritatea proceselor de bază din domeniul IC.

Domeniul IC este de asemenea direct corelat cu riscurile majore de dezastre naturale sau provocate de om cu care s-ar putea confrunta UE [19]. Amenințările cibernetice specifice IC sunt un subiect în evoluție datorită caracterului dinamic și global. În studii recente la nivel global, atacurile cibernetice asupra IC au fost clasate pe locul 5 în 2020, având potențialul de a afecta orașe sau chiar țări [4]. În comparație cu mediile TI tradiționale în care măsurile de atenuare sunt proporționale cu impactul și probabilitatea riscurilor potențiale, în IC contextul devine mult mai complex de definit. În plus, controlul unui risc este mult mai serios, deoarece atacurile cibernetice ar putea duce chiar și la un eveniment de siguranță. Această tendință este observată pentru sistemele esențiale pentru societate, cum ar fi în domeniul sănătății, unde atacurile cibernetice sunt în creștere în ultimul deceniu [20, 21].

Fig. 1.4. Rolul computerelor în IC

În zilele noastre, cu cât o societate este mai informatizată, cu atât ar putea fi mai vulnerabilă. Interconectarea și interdependența dintre aceste sisteme sunt inevitabile în acest moment. În Figura 1.4 este prezentat rolul componentelor calculatorului în contextul unei IC. Figura 1.4 este o reprezentare realistă a complexității procesului de protecție a IC, în care sistemele TI au un rol central în activitățile de monitorizare sau control.

Integrarea TI, împreună cu cerințele specifice ale IC, creează noi provocări atât pentru factorii de decizie, cât și pentru operatori. Evaluarea riscurilor pentru IC are un anumit accent care este dictat de aceste medii, cum ar fi operarea și disponibilitatea. Tehnologiile emergente provoacă abordările existente, deoarece apar noi vulnerabilități și ferestre pentru actorii rău intenționați pentru a perturba sistemele critice. Prin urmare, procesele de identificare, clasificare și atenuare a riscurilor necesită evaluare prin prisma noilor tehnologii și provocări.

O mică întrerupere a oricăreia dintre infrastructuri ar putea provoca un efect domino, de exemplu, întreruperea rețelei energetice ar putea duce la perturbări în alte sectoare, precum transportul sau telecomunicațiile [22]. Se poate observa o creștere a atacurilor cibernetice împotriva sectorului energetic, deoarece acesta este adesea sistemul motor pentru alte IC [23]. De exemplu, instalațiile din sectorul nuclear au trecut printr-un proces masiv de digitalizare, care impun ca operatorii nucleari și radiologici, cât și organismele de reglementare să asigure că activele digitale sunt protejate în mod adecvat. Cu toate acestea, ținând cont de ritmul de dezvoltare prin care trec IC, se consideră că managementul riscurilor necesită o abordare complexă pentru tot domeniul. Prognoza consecințelor integrării cibernetice în IC este mai dificilă din cauza tehnologiilor emergente, care măresc considerabil suprafața de atac, dar și din maturitatea relativ scăzută a securității cibernetice în sectorul guvernamental, care influențează indirect securitatea cibernetică a multor domenii de IC [24].

Accentul asupra managementului riscurilor cibernetice se bazează pe apariția acestor amenințări asupra IC și pe necesitatea de a identifica și controla aceste riscuri. Anterior TO erau asociate cu sistemele fizice, iar securitatea fizică a unei entități era considerată a fi obiectivul principal al echipei de securitate a infrastructurii critice. Odată cu introducerea sistemelor TI, domeniile securității fizice și cibernetice converg și impun cooperarea între experți cu cunoștințe din două domenii diferite. Ținând cont de acest lucru, se poate considera că procesele de management al riscurilor pentru asigurarea securității fizice sunt suficient de mature și asigură un nivel adecvat de protecție în conformitate cu amenințările și riscurile actuale. Prin urmare, s-a decis o concentrare asupra managementului riscurilor cibernetice în astfel de infrastructuri, deoarece se observă că TI și riscurile aferente creează provocări în asigurarea siguranței și securității unei IC. Accentul este de asemenea influențat de creșterea continuă din ultimul deceniu în numărul și varietatea atacurilor cibernetice, cât și potențialele daune asupra infrastructurilor critice [25].

Peisajul amenințărilor cibernetice actuale este bine definit și a fost evaluat ca fiind înaintea reacțiilor defensive în domeniul IC [26]. Acest lucru necesită investiții pe termen scurt pentru descurajarea amenințărilor cibernetice, nemaivorbind de investițiile necesare pentru ca sistemele

de apărare sa fie mai avansate decât tehnicile de atac. Se poate considera că acestea conturează peisajul amenințărilor, probabilitatea unui atac, precum și necesitatea de a întreprinde acțiuni pentru îmbunătățirea procesului de management al riscurilor cibernetice în IC.

Declarația de mai sus în ceea ce privește percepția amenințărilor cibernetice în infrastructurile critice este aplicabilă majorității, dacă nu tuturor țărilor. Acest lucru oferă contextul necesar pentru a extrage faptele că amenințările cibernetice devin un tip de atac comercial și se dezvoltă rapid. Pe de altă parte, apărarea rămâne cu un pas în urmă. Astfel, sunt necesare acțiuni pentru îmbunătățirea poziției de securitate a sistemelor informaționale subiacente în IC.

În plus, există diferite necesități și strategii adoptate care se referă la securizarea sistemelor informaționale de bază ale serviciilor critice care stau la baza IC [27]. De exemplu, obiectivul principal reflectat de NIST este de a se asigura că sistemele TI sunt fiabile și sigure în mod adecvat pe tot parcursul ciclului de viață al dezvoltării, oferă rezistența necesară și, astfel, sprijină economia și securitatea națională [27]. În plus, sunt specificate și alte obiective precum modernizarea sistemului, creșterea gradului de utilizare a automatizării, precum și standardizarea și optimizarea sistemelor în vederea întăririi protecției pentru activele de mare valoare. Acțiunile și strategiile descrise de anumite țări relaționează și poziționează amenințările cibernetice ca riscuri emergente pentru infrastructurile critice.

Situația actuală intensifică necesitatea înțelegerii fiecărui risc cibernetic în raport cu infrastructura critică și a modului de a o controla eficient. Datorită complexității acestui proces și cantității de date, industriile caută acum soluții TI pentru îndeplinirea acestor necesități. Luând în considerare interesul crescut și utilizarea sistemelor de sprijinire a deciziilor și potențialul acestora de a aborda domenii specifice de aplicație [28], soluțiile TI ar fi o soluție fezabilă pentru gestionarea sarcinilor complexe.

1.2. Securitatea cibernetică în Republica Moldova

Tematica securității cibernetice este discutată activ la nivel internațional, de autoritățile naționale, sau organizațiile din domeniul cercetării. Legislația Republicii Moldova privind securitatea cibernetică este în curs de revizuire și perfecționare, datorită progresului semnificativ pe care țara îl are în acest domeniu. Cu toate acestea, dezvoltarea tehnologică a avut loc mult mai rapid în comparație cu dezvoltarea instituțională și a resurselor umane, ceea ce se reda prin riscuri cibernetice sporite. Printre acestea, putem aminti nivelul scăzut de cultură a securității [25], sau actualizarea întârziată a cursurilor/programelor de master specializate pentru îmbunătățirea securității TI la nivel național.

În octombrie 2015, Guvernul a aprobat Programul Național de Securitate Cibernetică pentru anii 2016-2020, care descrie printre obiective – consolidarea capacităților de apărare cibernetică și educația, învățarea pe tot parcursul vieții și formarea în domeniul securității cibernetice [1]. Aceste obiective se referă și la IC de exemplu din domeniul medical, nuclear și radiologic și vor fi susținute de următoarele acțiuni enumerate în program:

- definirea autorităților responsabile și dezvoltarea capacității de apărare,
- înființarea unui centru de cercetare și formare în domeniul securității cibernetice,
- actualizarea curriculum-ului de securitate cibernetică,
- creșterea gradului de conștientizare în ceea ce privește riscurile de securitate cibernetică,
- definirea cerințelor pentru competențe profesionale pentru practicienii în securitate informatică din sectorul public și privat și
- desfășurarea de ateliere și sesiuni de formare pentru personalul din infrastructurile critice.

Aceste acțiuni abordează riscurile de securitate cibernetică atât din punct de vedere tehnologic, asigurându-se că există instrumente și sisteme adecvate pentru asigurarea securității, cât și aspectul dezvoltării resurselor umane, care include creșterea gradului de conștientizare a utilizatorilor cu privire la riscurile cibernetice. Este necesar să existe o abordare globală în asigurarea securității cibernetice – fapt care este reflectat suficient în programul național. Obiectivele și acțiunile propuse vor ghida autoritățile în ajustarea programelor lor de lucru și vor concentra eforturile și resursele acestora în consolidarea securității cibernetice prin îndeplinirea criteriilor de bază stabilite de regulamentul privind cerințele minime de securitate cibernetică. Mai mult, acest lucru se va reflecta și asupra sectorului privat, deoarece acest ghid național ar putea fi luat ca referință sau, cel mai probabil, utilizat ca o cerință în achiziționarea sistemelor TI.

Fără a privi aceste acțiuni, efectele nu vor fi instantanee - întrucât cultura de securitate, atât în domeniul cibernetic, cât și în cel nuclear, este în general scăzută la nivelul implementării. În plus, concentrându-se pe conștientizarea utilizatorilor, cercetarea și educația în acest domeniu, acțiunile ar trebui să aibă un efect atât pe termen scurt, cât și pe termen lung. Totodată, este necesar un progres uniform în acest domeniu [24]. Datorită importanței acestui subiect, există deja un rezultat vizibil de menționat - deschiderea în octombrie 2016 a Laboratorului de Securitate Cibernetică din cadrul Universității Tehnice din Moldova în cooperare cu Serviciul pentru Tehnologii Informaționale și Securitate Cibernetică, care este unicul furnizor de servicii TI pentru autoritățile publice, precum și reprezintă Echipa Guvernamentală de Răspuns la Incidente de Securitate. Acest succes a fost posibil cu asistența externă din partea Programului NATO „Știință pentru pace și securitate”, Ambasada SUA în Moldova și Ambasada Estoniei în Moldova. Astfel

de acțiuni sunt dictate atât de dezvoltarea rapidă a sectorului TI, cât și de numărul sporit de incidente și sisteme afectate de diverse tipuri de coduri malițioase depistate în Republica Moldova [29].

În mai 2016, Ministerul Tehnologiilor Informaționale și Comunicațiilor din Republica Moldova a publicat propunerea privind cerințele minime de securitate pentru asigurarea securității cibernetice a sistemelor informatice, care a fost aprobată de Guvern în 2017 [30]. Documentul se referă la o listă de subiecte de securitate informatică și stabilește cerințe pentru dezvoltarea și utilizarea sistemelor TI. Prin definiție, cerințele sau reglementările pot fi *bazate pe performanță*, atunci când acestea sunt descrise la un nivel înalt, sau *prescriptive,* atunci când sunt enumerate mai multe detalii. Nu există cea mai bună soluție în acest caz deoarece depinde de maturitatea culturii de securitate, de resursele de care dispune o organizație precum și de motivația de a implementa anumite controale. Prin urmare, nu este întotdeauna ușor de găsit abordarea potrivită și, de obicei, aceasta este o combinație a celor două tipuri de cerințe.

Aceste reguli sunt utilizate în reglementarea nucleară și radiologică, dar sunt aplicabile și în alte domenii complementare precum securitatea cibernetică [31, 32, 33, 34]. Acest document a fost elaborat combinând atât abordările prescriptive, cât și cele bazate pe performanță și conține o listă de controale de securitate la nivel administrativ și tehnic care trebuie implementate de către toate autoritățile statului, precum Agenția Națională de Reglementare a Activităților Nucleare și Radiologice, de operatorii nucleari și radiologici de categoria I și II, care pot fi clasificați drept infrastructuri critice datorită naturii activităților lor și a securității naționale. De asemenea, definește sistemele care ar trebui să îndeplinească aceste cerințe și introduce un sistem obligatoriu de management al securității informațiilor pentru circumscripție, precum și separă între controalele de securitate de bază și controalele avansate de securitate bazate pe o evaluare a riscurilor. Această abordare este binevenită pentru instituțiile care au doar un sistem informațional de bază cu importanță scăzută și riscuri evaluate, pentru a evita implementarea controlului doar pentru conformitate și nu pentru asigurarea nivelului de securitate. Cerințele minime de securitate ajută, de asemenea, utilizatorii să clasifice sistemele într-o categorie de risc, luând în considerare următorii factori: disponibilitatea sistemului, tipul de informații procesate și importanța acestor sisteme în cadrul organizației. Documentul include și cerințele de securitate pentru utilizarea sistemelor informatice, cum ar fi complexitatea parolei, conexiunea la Internet, politica de utilizare a e-mailului, cerința de a crea copii de siguranță sau condiții pentru externalizarea managementului acestor sisteme.

Putem face o paralelă cu publicația-seria de securitate nucleară a AIEA - NSS 17-T, deoarece recomandări similare pot fi găsite în această propunere de document, cum ar fi crearea

unei politici de securitate impusă de conducere sau deținerea unui ofițer responsabil pentru securitatea cibernetică [32, 33].

Prin implementarea acestor cerințe, nivelul general de securitate cibernetică pentru autoritățile publice va crește, inclusiv pentru IC din domeniul nuclear și radiologic. Acest lucru ar putea servi drept îndrumare pentru implementatori și evaluatori, cu toate acestea, unele dintre cerințele prescriptive ar putea crea dificultăți în înțelegerea și implementarea lor, precum și aceste cerințe ar putea deveni depășite într-o perioadă scurtă de timp din cauza peisajului amenințărilor în schimbare rapidă și a soluțiilor de securitate. Această dezbatere este comună în statele cu un nivel scăzut de cultură de securitate, deoarece fiecare nouă cerință este percepută ca o necesitate a mai multor resurse și cunoștințe din partea implementatorului. Cerințele prescriptive din document ar fi ușor de auditat, totuși ar putea reduce procesul de audit la o verificare a conformității, mai degrabă decât la creșterea conștientizării și a culturii în materie de securitate. Cu toate acestea, propunerea în sine ar putea ajuta administratorii sistemului TI să creeze o listă de verificare în raport cu mediul lor pentru a evalua controalele existente sau pe cele care trebuie implementate.

În plus, o reglementare națională privind astfel de cerințe mobilizează instituțiile în identificarea și clasificarea resurselor în asigurarea unui nivel adecvat de securitate cibernetică prin implementarea controalelor de securitate de bază. Un aspect necesar în ceea ce privește cerințele prescriptive este că, pe lângă facilitarea procesului de audit, aceste cerințe ar putea reduce domeniul de aplicare al unei astfel de reglementări la o verificare a conformității, mai degrabă decât să se uite la obiectivul de a ridica nivelul. de securitate.

Pe termen lung sunt necesare eforturi și resurse pentru a menține astfel de documente actualizate, precum și a menține un anumit nivel de flexibilitate din partea auditorilor. De asemenea, se salută faptul că aceste cerințe de securitate ar putea fi aplicate la un nivel înalt și, prin urmare, vor ghida autoritățile publice, inclusiv operatorii IC. Acest document sprijină aplicarea într-un fel a cerințelor de bază pentru securitatea computerelor în cadrul autorităților publice, ceea ce ar îmbunătăți considerabil apărarea generală și rezistența împotriva incidentelor cibernetice.

Sunt observate rezultate pozitive ale cerințelor minime de securitate sub forma politicii interne de securitate cibernetică aprobată de Ministerul Economiei și Infrastructurii. În plus, au fost identificate sistemele și importanța acestora, precum și numirea de către conducerea superioară [35] a biroului responsabil de securitate.

Aceștia sunt primii pași în elaborarea unui program de securitate cibernetică în orice organizație. Un astfel de sistem de management al securității informațiilor, menționat în mod obișnuit de standardul din seria ISO 27000, este un bun punct de plecare în identificarea resurselor

care sunt critice pentru organizație și pentru a se asigura că procesele existente sunt documentate, urmate și pot fi evaluate dacă este necesar [36]. Majoritatea programelor de securitate, dacă nu toate, au pornit de la definirea la nivel de politici a obiectivelor organizației în materie de securitate cibernetică, care este urmată de proceduri și îndrumări tehnice în vederea îndeplinirii politicii la nivel înalt.

În general, astfel de reglementări și acțiuni contribuie la crearea unei linii de bază de securitate informatică în cadrul autorităților publice, care să îmbunătățească considerabil apărarea generală și rezistența împotriva incidentelor cibernetice la nivel național.

De asemenea, Parlamentul Republicii Moldova a aprobat Legea privind Conceptul Securității Informaționale [37]. Legea a servit drept bază pentru elaborarea de către Guvern a Strategiei de Securitate Informațională pentru anii 2019 – 2024, Planul de acțiuni pentru implementarea acesteia, aprobate de către Parlament [38] care asigură respectarea conceptelor descrise în Legea sus-menționată. Acest document subliniază fără îndoială prioritatea statului de a proteja domeniul IC.

Se observă o perfecționare continuă a cadrului normativ, astfel I.P. Serviciul Tehnologia Informaţiei şi Securitate Cibernetică fiind desemnat în calitate de Centru guvernamental de reacţie la incidente de securitate cibernetică (CERT Gov). De asemenea, conform prevederilor Strategiei de securitate a informațiilor a Republicii Moldova pentru anii 2019-2024, prin recenta Hotărîre de Guvern din 06 iulie 2022 va fi instituit și un Consiliul coordonator pentru asigurarea securității informaționale.

1.3. Gestionarea riscurilor cibernetice în domenii cu risc sporit

În acest paragraf este prezentată definiția termenilor aferenți riscurilor cibernetice și a fost clarificat contextul procesului de analiză.

Ghidul ISO 73:2009 definește termenii risc, management al riscului și proces de management al riscului după cum urmează [39]:

- Un risc este efectul incertitudinii asupra obiectivelor, care poate avea diferite aspecte (siguranță, financiar etc.) și poate fi aplicat la diferite niveluri (strategic, produs, proces). Termenul de incertitudine, conform ISO, se referă la starea, parțială sau de lipsă de informații pentru înțelegerea unui eveniment, consecințele sau probabilitatea acestuia.
- Managementul riscurilor se referă la activități coordonate pentru a conduce și controla o organizație în ceea ce privește riscul.

- Procesul de management a riscurilor este o aplicare sistematică a politicilor, procedurilor și practicilor de management la activitățile de comunicare, consultare, stabilire a contextului și identificarea, analiza, tratarea, monitorizarea și evaluarea riscului.

În timp ce terminologia ISO legată de riscuri are anumite particularități, se observă că mulți dintre termeni sunt des utilizați cu semnificații similare în lucrări, literatură și mass-media. Definiția termenilor și proceselor specific de management al riscurilor au fost inițial analizate. Totuși se presupune că de multe ori se face referire la semnificația de bază a unui risc ca rezultat al amenințării, probabilității și consecințelor.

O altă înțelegere comună a gestionării riscurilor este reducerea riscului. Costurile totale sunt considerabil mai mici atunci când se reduc riscurile la un nivel acceptabil, în comparație cu costul incidentului și al pericolului pe care acest risc l-ar fi putut provoca. Prin urmare, managementul riscurilor cibernetice un subiect actual și emergent. În analiza dată s-a concentrat asupra riscurilor cibernetice ca amenințări care apar din spațiul cibernetic sau utilizarea TI. Noțiunea de „risc cibernetic” nu este definită în mod explicit de ISO, dar a devenit foarte populară și utilizată în mod obișnuit în industrie.

Scopul principal al managementului riscului este de a preveni pierderile, daunele sau pierderea funcționalității unui sistem, în cazul dat într-o IC. Este evident că un risc nu poate fi eliminat complet. Acest fapt poate fi corelat și cu teorema incompletei lui Gödel, întrucât niciun set de controale de securitate nu ar elimina toate riscurile cunoscute, întrucât mereu va exista un risc nou ce nu poate fi atenuat sau redus prin controalele existente (adaptat după [40]). Astfel, atenuarea riscurilor cibernetice este un proces continuu.

În schimb, după identificarea riscului, analiza și implementarea anumitor măsuri de atenuare, acesta ar putea fi redus la un nivel acceptabil prin intermediul unor măsuri. Întrucât spațiul cibernetic generează permanent noi riscuri, este necesară o evaluare periodică și continuă a riscurilor asociate pentru a asigura protecția eficientă a datelor, serviciilor și funcționalității IC, ținând cont de schimbările care apar.

În procesul de gestionare a riscurilor cibernetice într-o IC, trebuie să înțelegem că sistemele computerizate sunt la baza sistemelor de control, monitorizare și detectare.

1.4. Sisteme suport decizionale

În această secțiune este descris conceptul și definiția SSD. Acest tip de sisteme informaționale este propus a fi utilizat pentru a aborda amenințările cibernetice moderne și

emergente, prin sprijinirea și îmbunătățirea procesului de management al riscurilor cibernetice în domeniul IC.

Definiția unui SSD este relativ ușor de perceput prin semnificația fiecăruia dintre termenii săi. În cadrul tezei un SSD este considerat conform definiției date de F. G. Filip, ca un sistem informațional în evoluție, antropocentric și adaptiv, care este conceput să simuleze funcțiile de consiliere pentru a sprijini factorii de decizie [41]. SSD este o soluție potențială în depășirea limitelor umane în ceea ce privește rezolvarea unor decizii complexe sau analizarea unei cantități mari de date [42, 43]. Această definiție este preferabilă, deoarece acoperă elementele necesare în contextul analizei riscurilor cibernetice în infrastructurile critice. SSD se referă la o gamă de sisteme care includ diverse tehnologii și vizează ghidarea și sprijinirea procesului de luare a deciziilor [28, 43]. Astfel de sisteme pot face față unor subiecte multidimensionale și complexe și pot fi considerate ca înlocuirea unei echipe de experți cu medii diferite [42, 43].

Acest tip de sisteme a fost selectat datorită interesului în creștere exponențială a SSD pentru cercetare [28]. Pe de altă parte, un SSD poate fi legat de termeni înrudiți, cum ar fi luarea de decizii sau sistemele expert. S-a concentrat asupra termenului de SSD, deoarece este cuprinzător și acoperă factorii necesari în cercetarea curentă. Acest tip de sistem poate sprijini concentrarea pe o soluție durabilă și pe termen lung în gestionarea riscurilor cibernetice din acest domeniu.

Oportunitățile oferite de un SSD îndeplinesc, de asemenea, recomandările NIST privind creșterea utilizării automatizării ori de câte ori este posibil, datorită unor factori precum viteza și eficiența executării acțiunilor care fac parte din procesul de management al riscului. Un SSD ar putea sprijini și implementa această recomandare în practică, deoarece aceste sisteme sunt capabile conceptual să asigure evaluarea și monitorizarea continuă în timp real a controalelor și, de asemenea, să amelioreze procesul de management al riscurilor cibernetice.

Un alt factor de utilizare a SSD sunt tendințele care au fost identificate în integrarea continuă între entități, diversitatea culturilor și tehnologiilor care sunt interconectate, precum și urmărirea unei dezvoltări durabile [44]. Aceleași tendințe și factori pot fi observați în dezvoltarea și digitalizarea IC și a proceselor aferente de management al riscului.

În teză au fost descrise elementele arhitecturale specifice, cerințele, conceptele de securitate, precum și factorii necesari în timpul proiectării și utilizării acestui SSD. Acesta reprezintă conceptul pentru soluția de gestionare și atenuare a riscurilor cibernetice în domeniul IC. Dezvoltarea oricărui sistem informațional urmează pași standard, de la proiectare până la produsul gata de piață. Faza de proiectare este critică deoarece asigură că sistemul final este ajustat la necesitățile și cerințele clientului.

Implementarea unui produs TI are un ciclu de dezvoltare relativ standard. Acesta începe cu definirea întrebării, urmată de analiză, proiectare, implementare și testare și, în final, utilizarea sistemului. Sistemul final vizează rezolvarea întrebării inițiale [45].

Un SSD reprezintă un sistem informațional, astfel, urmează abordări similare. Pe baza definiției că un sistem reprezintă un ansamblu de elemente într-o relație structurală de interdependență și interacțiune reciprocă, formând un tot organizat [46], se poate afirma că proiectarea și implementarea unui SSD este un proces complex. În plus, fiecare sistem informațional este proiectat pentru a rezolva o anumită chestiune sau întrebare, într-un anumit domeniu de aplicație.

Un domeniu de aplicație este format din obiecte, relațiile dintre obiecte precum și procesele utilizate pentru modificarea obiectelor [47]. Aceste articole descriu la nivel conceptual orice arhitectură și, în cazul dat, un sistem de sprijinire a deciziilor. Dintr-un alt punct de vedere, arhitectura ar putea include și alte aspecte precum tehnologii și tip de utilizatori finali.

Dacă în fazele incipiente sunt luate în considerare aspectele necesare, inclusiv, dar fără a se limita la, scopul, arhitectura și costul SSD, se va asigura că SSD-ul dezvoltat este adecvat scopului. Aceste aspecte trebuie luate în considerare atunci când se ia decizia de a introduce un sistem informațional nou [48]. În faza de proiectare, este, de asemenea, important să fie luate în considerare tehnologiile și tendințele moderne din TI. Este esențial să se țină cont de necesitățile și cerințele față de SSD și să se identifice cerințele funcționale și nefuncționale. Designul ar putea acoperi o gamă largă de subiecte, de la plasarea SSD în rețea, limbaje de programare, cerințe hardware, politici de securitate, aspecte de cost până la modul în care ar trebui să funcționeze sistemul și ce ar trebui să ofere. Acest lucru va asigura că sistemul va fi capabil să rezolve chestiunea inițială într-un mod eficient.

Un alt element important în faza de proiectare, care este adesea trecut cu vederea, este elementul uman. Fiecare sistem trebuie proiectat și adaptat la diferitele categorii de utilizatori, precum utilizatorii finali (factori de decizie sau operatori), beneficiari (proprietari ai IC), precum și susținut de conducerea superioară pentru a asigura utilizarea acestuia în cadrul organizației [49]. Alte aspecte precum echipa de implementare și strategia, potențialii utilizatori implicați în definirea cerințelor și chiar studiile de fezabilitate sunt necesare pentru a fi luate în considerare [49].

De asemenea, au fost descrise elementele de arhitectură ale unui SSD destinat managementului riscurilor cibernetice în infrastructurile critice. Întrucât scopul principal al acestui SSD este de a sprijini procesul de management al riscurilor cibernetice, care depășește adesea

capacitatea umană de a analiza din perspectiva cantității de date, arhitectura este una dintre primele întrebări care apar în timpul dezvoltării conceptului.

Scopul SSD este de a rezolva atât chestiunile de tip structurat, când vine vorba de riscuri cibernetice care au o sintaxă și o soluție relativă, cât și tipul de chestiuni nestructurate atunci când anumite concepte TI trebuie să fie valorificate, cum ar fi inteligența artificială sau învățarea automată.

O descriere din literatura de specialitate pentru arhitectura SSD conține patru aspecte: sistemul de limbaj, sistemul de prezentare, sistemul de cunoștințe și sistemul de procesare a cunoștințelor [50]. Conform definiției, ultimul element este componenta principală a SSD, deoarece conține logica, algoritmii și abilitățile care vor defini SSD-ul propus. Sistemul de procesare utilizează toate funcționalitățile primelor trei sisteme enumerate: limbaj, prezentare și cunoaștere [50]. Deoarece poate fi dedus pe baza termenului, procesarea va rezolva întrebarea reală. Primele trei elemente contribuie la scopul SSD. Deși este o arhitectură SSD tipică aceasta ar putea fi extinsă cu diferite elemente și funcționalități.

O altă definiție a arhitecturii SSD este combinația a patru straturi: diagrama fluxului procesului de decizie de afaceri, arhitectura sistemelor, arhitectura tehnică și interfața cu utilizatorul [51]. Definiția conține elemente din diferite domenii de cercetare cum ar fi arhitectura sistemului, hardware-ul, fluxurile de date ș.a. Acesta reprezintă un alt punct de vedere asupra modului în care poate fi dezvoltată și structurată o arhitectură de sistem.

Ultima definiție se referă la arhitectură ca metodologie de rezolvare a clasei de probleme care integrează următoarele elemente: definirea limbajului, soluția de probleme, baza de cunoștințe, baza de date, proiectarea interfeței inteligente cu utilizatorul și modulele auxiliare [47]. Definiția menționată mai sus a unei arhitecturi SSD este cea mai potrivită pentru această cercetare și este utilizată pe tot parcursul tezei.

Logica și pașii de rezolvare a unei clase de probleme, corespund unei extensii a unui model de arhitectură oferit [50], totuși ultimul ia în considerare module suplimentare pentru scalare și aplicații ulterioare. O reprezentare la nivel înalt a arhitecturii SSD propuse poate fi văzută în Figura 1.5.

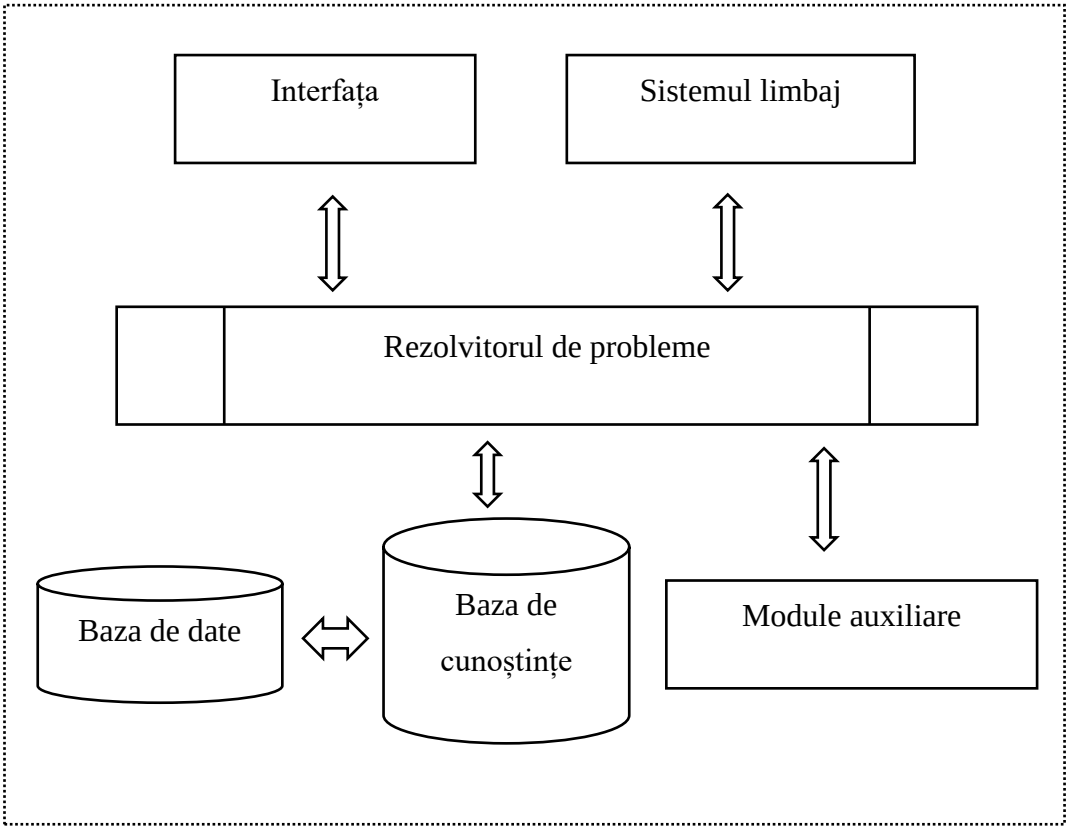

Fig. 1.5. Arhitectura unui sistem de suport decizional

1.5. Impactul digitalizării în domeniul medicinii

Tehnologiile digitale reprezintă o oportunitate și un vector de promovare și asigurare a dezvoltării IC pe exemplul sectorului sănătății prin furnizarea de servicii medicale eficiente. Multe țări s-au angajat în digitalizarea serviciilor, inclusiv Republica Moldova. Unul dintre elementele de bază în digitalizarea serviciilor în medicină este fișierul electronic al pacientului care conține datele istorice medicale ale unui pacient. Acest lucru poate sprijini interoperabilitatea între operatorii de asistență medicală pentru a ajuta la reducerea sarcinii inutile pentru pacient, cum ar fi colectarea și reținerea tuturor rezultatelor testelor sau efectuarea aceluiași test la un alt loc. Mai mult, un sistem centralizat la nivel național ar putea ajuta, de asemenea, să protejeze mai bine datele pacienților, să monitorizeze și limiteze, de exemplu, dozele de radiații primite în investigații sau tratament, deoarece acest sistem ar fi probabil deținut și controlat de stat, care are mecanisme de reglementare și control mai bune în comparație cu micii operatori de asistență medicală care s-ar putea lupta pentru a proteja în mod adecvat aceste date. Un astfel de sistem electronic a fost considerat și în Moldova. Cu toate acestea, digitalizarea în asistența medicală nu se referă doar la datele pacienților, ci și la tehnologiile utilizate în tratament, precum și alte tehnologii deținute de orice alt furnizor care ar putea fi implicat în implementarea sau furnizarea de servicii digitale. Din perspectiva riscurilor cibernetice, aceasta deschide o nouă sferă de elemente care trebuie evaluate.

Compromiterea datelor personale despre un pacient reprezintă un risc critic, atât din perspectiva încălcării confidențialității, cât și a potențialei fraude financiare sau excluderii societale. Cu toate acestea, în contextul domeniului IC, este, de asemenea, important să se evalueze modul în care tehnologiile digitale sunt implementate pentru operatorii de asistență medicală și sistemele utilizate. O perioadă de întrerupere a internetului ar putea duce la erori de funcționalitate pentru un operator, dacă sunt utilizate tehnologii cloud. Cu toate acestea, în impactul mai sever al unui atac cibernetic țintit sau de tip ransomware, astfel de tehnologii ar putea fi utilizate pentru a crea rău.

Integrarea TI în medicină, care este unul dintre domeniile IC, a adus nenumărate aplicații și integrări care reprezintă o îmbunătățire pentru sănătatea individului, bunăstarea societății și a creat noi oportunități pentru furnizorii de servicii medicale. Astfel de tehnologii medicale pot fi văzute în zilele noastre nu numai în țările dezvoltate, ceea ce înseamnă că sunt necesare acțiuni globale pentru a aborda riscurile cibernetice care vin împreună cu astfel de tehnologii. Pandemia de Covid-19 a subliniat, de asemenea, oportunitățile și necesitățile soluțiilor TI pentru domeniul sănătății, cum ar fi livrarea electronică a certificatelor de concediu medical, de vaccinare, etc., pentru a minimiza călătoriile sau contactele inutile.

Cu toate acestea, digitalizarea a dus și la noi riscuri datorită faptului că operațiunile sunt controlate de un computer sau dispozitiv digital. Majoritatea echipamentelor medicale care au sisteme TI încorporate și care răspund anumite procese, sunt *supuse unor vulnerabilități și predispuse la atacuri cibernetice similare computerelor*. Capacitățile de dezvoltare și integrarea TI în diverse operațiuni oferă capacitatea de a introduce noi caracteristici, de exemplu pentru monitorizare, care nu erau posibile înainte sau aveau un cost foarte mare. Cu toate acestea, sistemele de sănătate au fost concepute cu accent pe funcționare și siguranță. În plus, echipamentele medicale care utilizează surse nucleare sau radiologice pentru tratament reprezintă o amenințare la un nivel complet diferit.

Dintr-un alt punct de vedere, asistența medicală este unul dintre *domeniile de vârf* în care inovațiile digitale s-au schimbat în ceea ce privește modul în care sunt utilizate sistemele și le-au crescut eficiența. Dispozitivele computerizate ajută la citirea și analizarea intrării, de exemplu radiografia, procesarea acesteia și furnizarea diagnosticului sau a anumitor date care ar ajuta medicul. Prin urmare, computerul este o parte intrinsecă a dispozitivului medical. Diverse organizații, cum ar fi Healthcare Information and Management Systems Society, s-au specializat deja în digitalizarea asistenței medicale și au diferite metode pentru a evalua maturitatea unor astfel de procese, analizând fișierul de date ale pacientului, imagistica digitală, lanțul de aprovizionare sau analiză.

Beneficiile *directe* ale utilizării tehnologiilor TI sunt sprijinirea operatorului și îmbunătățirea calității diagnosticului, precum și asistența cu date și recomandări de tratare a anomaliilor detectate. Aceste tipuri de dispozitive medicale sunt utile în alertarea când anumite condiții sunt îndeplinite și sporesc șansele de detectare precoce și prevenire a anumitor boli sau situații critice. Dezvoltarea aplicațiilor corespunzătoare este relativ simplă – *machine learning* și colectarea de date pot fi utilizate pentru a colecta, agrega și analiza date. Aceste sisteme pot procesa, de asemenea, seturi mari de date, de exemplu scanări anterioare și diagnosticarea acestora, precum și tipul de tratament pentru fiecare tip de anomalie detectată.

Digitalizarea asistenței medicale este observată și în dispozitivele portabile inteligente care au capacități de detectare și sunt utilizate pentru monitorizarea și colectarea datelor de sănătate despre utilizator. Acest lucru permite dezvoltarea unor noi cazuri de utilizare. De exemplu, interconectarea dispozitivelor portabile inteligente cu operatorii din domeniul sănătății creează oportunități și capacități atât pentru utilizator, cât și pentru instituția medicală. Un alt exemplu de digitalizare este schimbul de date între operatori, cum ar fi clinicile și farmaciile, unde rețeaua dintre aceste entități ar ajuta la schimbul de date în direct și ar oferi funcționalități suplimentare.

Din păcate, nu toate controalele tehnice de securitate sunt implementate corespunzător din cauza riscului ridicat perceput de un risc operațional. Cercetările recente au demonstrat că un sistem TO poate fi compromis printr-un atac cibernetic. Astfel controalele și atenuarea de securitate nu mai pot fi neglijate [31, 52]. De asemenea, multe dintre aceste tehnologii sunt furnizate prin *cloud* [53]. Prin urmare, aceste dispozitive utilizează tehnologia *cloud* pentru interconectarea dispozitivelor portabile pentru pacienți și a operatorilor din domeniul sănătății. Cu toate acestea, în alte cazuri de utilizare, același dispozitiv de asistență medicală ar putea fi interconectat în sediul operatorului, utilizând și tehnologii *cloud*. Analizând acest lucru în contextul dispozitivelor care utilizează radiații ionizante, securitatea cibernetică a întregului ecosistem devine o cerință obligatorie din cauza riscurilor și implicațiilor potențiale de siguranță asupra pacientului sau a societății în general.

1.6. Securitatea cibernetică în domeniul nuclear și radiologic

În această secțiune este prezentată o privire de ansamblu asupra stării actuale a securității cibernetice în domeniul nuclear și radiologic din perspectivă legislativă și tehnică, precum și a legislației din domeniul nuclear și radiologic cu accent pe elementele de securitate cibernetică. Este important de menționat că peste 90% din sursele radiologice, precum și materialele radioactive și nucleare din Moldova sunt utilizate în asistența medicală. Prin urmare, din această perspectivă, domeniile IC considerate în teză sunt puternic interconectate la nivel național.

A fost evaluată implicația cerințelor de securitate cibernetică pentru operatori majori nucleari și radiologici din Republica Moldova, iar rezultatele au fost corelate cu modelul propus pentru evaluarea maturității securității cibernetice ale operatorilor. În plus, a fost analizat contextul internațional și motivația recunoașterii securității cibernetice ca parte intrinsecă a securității nucleare [31], precum și acțiunile pe care Republica Moldova le-a întreprins până acum pentru implementarea, inclusiv a cerințelor înaintate pentru securitatea cibernetică ca parte intrinsecă a securității fizice nucleare, autorizării activităților, supravegherii și controlului, protecției bazelor de date în activități nucleare și radiologice [52, 54-56].

1.6.1. Context și motivație

Securitatea nucleară este unul dintre cele mai discutate subiecte de comunitatea internațională relevante IC. Beneficiile versus potențialele incidente negative, tentative de proliferări, amenințări recente sunt fapte care necesită atenție pentru a asigura o utilizare sigură și securizată a unor astfel de tehnologii. Riscurile cibernetică reprezintă o amenințare de top pentru toate domeniile și sunt recunoscute ca parte intrinsecă a securității și siguranței nucleare datorită numeroaselor computere încorporate utilizate în domeniul nuclear civil în sisteme precum securitatea fizică, sistemele de control industrial, bazele de date privind evidența și cantitățile de materiale nucleare, care conform Convențiilor și Tratatelor la care suntem parte se raportează trimestrial către AIEA.

Măsurile de prevenire, detecție și prim răspuns la acțiunile neautorizate în domeniul nuclear și radiologic revin primar operatorilor. Sarcinile operatorilor sunt de a asigura controlul materialelor nucleare sau radiologice și de a preveni orice acțiuni neautorizate, iar un operator poate realiza acest lucru prin implementarea politicii de securitate specifice sau a măsurilor de control în cadrul organizației. Acest lucru este valabil nu numai pentru combaterea traficului ilicit, ci și pentru desfășurarea în siguranță a activităților nucleare și radiologice. Prin urmare, operatorii trebuie să se ghideze după strategia, politica, legislația și reglementările naționale pentru domeniul lor de activitate și să transpună aceste cerințe în politici și proceduri interne pentru a asigura siguranța și securitatea sistemelor. În general, reglementările la nivel național stabilesc cerințele minime care trebuie implementate, care conform bunelor practici sunt dezvoltate pe baza amenințării bazate pe proiectare, proces cunoscut și ca *design basis threat*. Conform conceptului de amenințare bazată pe proiectare [32], autoritățile de reglementare și alte organizații cu responsabilități în domeniu trebuie să evalueze amenințările actuale pentru a dezvolta contramăsuri eficiente, cu toate acestea, legislația națională actuală și alte aspecte precum costurile pot, de asemenea, să fie luate în considerare la definirea cerințelor de securitate.

Pe de altă parte, sistemele TI sunt utilizate de majoritatea operatorilor, de exemplu în sistemele de securitate fizică, de contabilizare a cantităților materialelor nucleare și radiologice, dar și de către autoritățile de reglementare [33] care dețin baza de date națională respectivă. Definirea cerințelor de securitate a sistemelor informatice, utilizate și în astfel de medii, ar simplifica sarcinile operatorului sau ale autorității de reglementare în înțelegerea și alegerea controalelor corecte complexe de implementat și ar completa regulamentul respectiv al Guvernului privind securitatea fizică a activității nucleare și radiologice. Acest lucru ar putea facilita procesele de evaluare în scopul autorizării, controlului și supravegherii. În schimb, aceasta ar adăuga o povară suplimentară pentru operatori, care mențin astfel de cerințe pentru a le ajusta periodic în conformitate cu evaluările amenințărilor sau design-basis-threat. În general, recunoașterea securității cibernetice ca parte a securității nucleare a motivat statele membre să își ajusteze cadrele legale și să includă securitatea cibernetică ca parte a autorizării activităților, inclusiv efectuate de Republica Moldova [52, 54-56].

În plus, potrivit unei companii de top ce oferă servicii de securitate cibernetică, domeniul nuclear poate fi un motor sau o motivație pentru atacuri cibernetice, în combinație cu motive politice și economice [53, 57]. Mai mult, pot fi stabilite unele legături între grupurile de amenințări cibernetice și motivația nucleară [57], care reprezintă date valoroase care pot fi utilizate în timpul evaluărilor de risc pentru instalațiile nucleare și radiologice. Atacurile cibernetice care vizează sectorul energetic, sau mai exact sistemele de control industrial [58], pot fi legate și de instalații nucleare/radiologice, deoarece acestea tind să utilizeze același tip de echipamente pentru controlul și monitorizarea funcționalității instalației. Acesta este unul dintre principalele motive pentru care securitatea cibernetică este obligatoriu luată în considerare în prezent la proiectarea și întreținerea diferitelor sisteme industriale, inclusiv cele utilizate în instalațiile nucleare și radiologice, sau precum sistemele de securitate fizică utilizate de operatori.

Multitudinea eforturilor în securitatea cibernetică în sistemele de securitate fizică în context nuclear și radiologic, este o motivație serioasă pentru a lua în considerare implicațiile securității cibernetice în domeniul nuclear. De exemplu, atacurile cibernetice pot fi un instrument pentru sabotaj, furt sau deturnare a cantităților de material nuclear special strategic, de exemplu în timpul transportării sau protecției fizice inadecvate [59]. Având în vedere că Republica Moldova nu dispune de resurse suficiente pentru a efectua studii mai aprofundate asupra implicațiilor securității cibernetice în entitățile cu activități nucleare/radiologice, precum și specificul țării, publicațiile și ghidurile externe, de exemplu ale AIEA, servesc drept bază pentru cele mai bune practici necesare de implementat în legislația națională și aplicarea practică în Republica Moldova, de exemplu a transportării în siguranță a materialelor radioactive [32, 56, 60].

Pe de altă parte, potrivit campaniei de atacuri cibernetice, denumită „Red October” de către compania Kaspersky, au fost vizate diverse domenii precum cercetarea, guvernarea, armata și agențiile nucleare. Se poate deduce cu ușurință că în zilele noastre atacurile cibernetice au un caracter internațional și țintele pot fi în orice domeniu. Prin urmare, este necesar să fie luate măsuri adecvate mai întâi din punct de vedere legal și apoi din punct de vedere practic, pentru a atenua riscurile de securitate cibernetică pentru operatorii nucleari și radiologici din Republica Moldova. Aceasta se referă la sistemele de securitate fizică, precum și la orice alt sistem care are componente TI și poate fi susceptibil la un atac cibernetic.

1.6.2. Legislația națională

Domeniul securității nucleare se află într-un proces de îmbunătățire continuă. În februarie 2013 în cadrul Universității Tehnice din Moldova a fost înființat Centrul Național de Suport al Securității Nucleară (CNSSN) cu sprijinul tehnic al Autorității Suedeze pentru Securitate Radiologică, dar și al Oficiului de Securitate Nucleară al AIEA pe domeniul perfecționării cadrelor. Centrul are obiectivele de a pregăti tineri specialiști în securitatea nucleară și radiologică și neproliferare prin programe de masterat, de a contribui la perfecționarea de personal din organizațiile relevante, de a oferi suport tehnic și de a efectua cercetări în acest domeniu. În anul 2017, ulterior și în 2020 a fost actualizat curriculum-ul disciplinei „Securitate nucleară și radiologică” pentru programul de Master în „Inginerie Biomedicală și Microelectronică și Nanotehnologii” [12]. Noul curriculum conține programe de studii privind securitatea și siguranța nucleară, sistemul de garanții nucleare și neproliferare, inclusiv a armelor de distrugere în masă și materialelor, tehnologiilor tangibile. Este important că pentru prima dată este reflectat sinergismul progresiv a subiectelor menționate cu domeniul securității cibernetice.

O altă realizare în domeniul nuclear și radiologic, care include aspecte de securitate cibernetică, este aprobarea (după 3 ani de promovare a proiectului) a Regulamentului privind securitatea fizică în activități nucleare. În prezent, cerințele privind obținerea autorizării pentru activități ale operatorilor nucleari și radiologici conțin elemente de securitate cibernetică ca parte intrinsecă a sistemelor de securitate fizică [56].

Analiza s-a concentrat pe aspectele care se referă la securitatea cibernetică pentru entitățile nucleare sau radiologice, în contextul sistemelor de securitate fizică. La baza acestui regulament a stat prevederea art. 35 (d) din Legea nr.132 despre una dintre condițiile obligatorii pentru autorizarea procesului de securitate fizică care include securitatea cibernetică a obiectelor nucleare și radiologice [31]. De asemenea, regulamentul este în conformitate cu cerințele și recomandările AIEA [32, 61] și descrie următoarele:

- rolul securității cibernetice la stabilirea unui sistem de securitate fizică;
- cerințele de securitate a informațiilor, precum și cerințele tehnice pentru software și hardware utilizate în aceste sisteme de securitate fizică;
- dezvoltarea planului de securitate cibernetică al operatorului ca plan distinct sau ca parte a securității fizice sau nucleare a activelor operatorului;
- responsabilitatea operatorului de a defini securitatea pe niveluri, controalele de securitate și a nivelurilor de securitate cibernetică, pe baza unei evaluări a riscurilor pentru a asigura un nivel ridicat de securitate fizică și nucleară.
- cerința de a raporta autorităților relevante cu privire la
    - orice încercare de a extrage informații legate de securitatea fizică,
    - orice atac cibernetic sau fizic care ar putea duce la oprirea sau alterarea unuia sau mai multor computere responsabile cu securitatea fizică și nucleară a obiectivului sau a materialelor nucleare și radiologice;
    - orice atac hibrid (cibernetic și fizic) asupra computerelor de bază,
    - furt de materiale nucleare și radiologice,
    - orice altă încălcare a sistemului de securitate fizică.
- cerința de gestionare a informațiilor de a securiza informațiile privind securitatea fizică a obiectivului nuclear și/sau radiologic, precum și datele materialelor nucleare clasificate ca „restricționat” sau mai strict, în raport cu categoria obiectivului;
- asigurarea confidențialității datelor privind sistemele de securitate fizică, instalațiile nucleare și radiologice și materialele nucleare și radiologice protejate ca responsabilitate a operatorului;
- cerința de a stabili controale de securitate adecvate pentru a asigura confidențialitatea datelor privind securitatea fizică în timpul utilizării, transportului sau depozitării materialelor nucleare și radiologice în funcție de categoria acestora;
- cerința de a restricționa accesul la date care ar putea compromite sistemele de securitate fizică ale obiectivului, instalațiilor sau materialelor nucleare și radiologice;
- cerința de a trata ca date secrete sau confidențiale orice informații potențiale de vulnerabilitate ale sistemelor de securitate fizică;
- includerea procedurilor de securitate cibernetică în sistemul de securitate fizică, precum și protejarea caracteristicilor de confidențialitate, integritate și disponibilitate a bazelor de date electronice sau a sistemelor și proceselor cibernetice care ar putea influența negativ sistemul de securitate fizică a obiectivului sau materialelor protejate;

- identificarea activelor și sistemelor, inclusiv a celor TI, care sunt vitale pentru instalare și obiecție. Acest proces trebuie efectuat de către operatorul autorizat împreună cu experți în acest domeniu la implementarea sistemului de securitate fizică nucleară.

Acest exemplu de reglementare demonstrează cum securitatea cibernetică se îmbină armonios cu alte domenii decât TI, precum și importanța definirii responsabilităților în astfel de cazuri. În contextul securității cibernetice, în care cunoștințele sunt specifice și informațiile din sistem trebuie cunoscute atunci când se descriu astfel de parametri, este necesar să existe cerințe clare care să poată fi implementate de un operator și pe baza cărora un sistem poate fi auditat. De asemenea, este necesară actualizarea continuă a legislației, iar implementarea ar trebui să fie susținută de procese și inspecții riguroase pre-autorizare adecvate. Fără aceasta, există o probabilitate redusă ca operatorii să implementeze suficiente autoevaluări de securitate pentru a descuraja amenințările actuale. Cu toate acestea, apreciem că regulamentul aprobat este în general în conformitate cu recomandările și bunele practici ale AIEA și stabilește cerințele de securitate cibernetică față de sistemele de securitate fizică sau sistemele care conțin date legate de acesta în activități nucleare sau radiologice. Această reglementare este un pas progresiv în legislația nucleară și radiologică din Republica Moldova și este necesară continuarea cooperării între domeniile cibernetice și alte domenii, pentru a dezvolta politici și reglementări pentru îmbunătățirea poziției de securitate în conformitate cu peisajul amenințărilor IC.

Mai sus a fost menționat că securitatea cibernetică a fost recunoscută ca parte componentă a sistemelor de protecție fizică în activitatea nucleară/radiologică [31]. Acest nou aspect este luat în considerare la autorizarea de către instituția de reglementare și stă la baza dezvoltării ulterioare a legislației conform recomandărilor AIEA și Agenției Europene Nucleare. De exemplu, instituția de reglementare a elaborat și promovat adoptarea regulamentelor pentru descrierea acțiunilor și responsabilităților tuturor actorilor privind bazele de date și securitatea fizică în activități nucleare și radiologice [54, 56]. Cu toate acestea, lipsa resurselor la nivel de stat și operator, precum și securitatea cibernetică fiind un domeniu străin de activitate în acest domeniu, creează impedimente în îndeplinirea atribuțiilor de reglementare. Prin urmare, soluțiile posibile sunt multilaterale și necesită acțiuni din partea părților interesate, dintre care unele ar putea necesita timp. De obicei, în cadrul legislativ sunt stabilite cerințe minime pe care trebuie să le îndeplinească un operator pentru cerințele de autorizare, totuși, în practică, acestea sunt singurele cerințele pentru care operatorul are controale sau instrumente. Mai mult, natura dezvoltării tehnologiei informației creează noi provocări pentru cadrul legislativ, deoarece acesta poate deveni depășit într-o perioadă scurtă de timp. Prin urmare, este necesar să fie efectuate studii viitoare cu privire la modul de

aplicare a cerințelor minime pentru a permite și încuraja operatorii să adapteze și să implementeze continuu controale pentru a atenua riscurile de securitate.

Instituția de reglementare poate fi susținută fie extern, de organizații specializate sau programe de suport tehnic, fie intern, prin promovarea și crearea unui serviciu special și a unei poziții de personal de experți în securitate TI, după modelul, de exemplu, CRN al SUA. Această nouă poziție ar contribui și la menținerea unui nivel de securitate în cadrul instituției de reglementare, precum și în procesul de autorizare în auditarea și coordonarea planurilor și infrastructurii de securitate cibernetică a operatorilor. De asemenea, acest lucru ar ajuta instituția de reglementare să îmbunătățească legea privind sistemele de securitate fizică cu mai multe detalii și cerințe din aspectul securității cibernetice, întrucât ar avea un expert intern în domeniu în acest domeniu. De asemenea, este obligatoriu în timpul procesului de autorizare derulat de instituția de reglementare să se verifice dacă planul de securitate cibernetică pe care l-a elaborat operatorul este actual, precum și să se efectueze auditul tehnic al componentelor informatice aleatorii ale sistemelor operatorului care sunt responsabile sau ale sistemelor de securitate fizică. Aceasta ar putea fi o soluție viabilă în contextul activităților limitate din sistemul de sănătate și în domeniul managementului deșeurilor nucleare și surselor neutilizabile.

Pe de altă parte, este necesar să existe o echipă specializată care să aibă cunoștințele necesare atât în domeniul cibernetic, cât și în domeniul nuclear/radiologic, pentru a răspunde și a atenua un atac cibernetic în astfel de IC. Întrucât îmbunătățirea securității cibernetice în sistemele de control industrial din Moldova este o prioritate a planului de acțiuni al programului național de securitate cibernetică, este necesară consolidarea inițiativei legislative în practică. În momentul de față nu există suficiente resurse umane specializate pentru monitorizarea și detectarea atacurilor cibernetice în IC.

Centrul Național de Suport al Securității Nucleare (CNSSN) al UTM cum a fost menționat servește și ca Organizație de Suport Tehnico-Științific pentru entitățile autorităților de stat interesate, pentru operatori și deschide noi oportunități de cooperare între experții în securitate cibernetică și securitate nucleară, care ar duce la dezvoltarea personalului în această nișă TI [62]. Un alt plan pe termen scurt și mediu a inclus sprijin din surse externe pentru eforturile CNSSN în modernizarea în continuare a programelor nucleare și radiologice, de neproliferare, precum și promovarea educației în domeniul securității cibernetice în programul de master [63, 64, 65, 66]. Acest lucru permite divizarea modulelor cursului în funcție de responsabilitățile ulterioare sau prezente ale masteranzilor, de exemplu pentru studenți, practicieni, responsabili de radioprotecție sau factori de decizie.

1.7. Concluzii la capitolul I

Această cercetare a permis o mai bună înțelegere a tematicii, precum și identificarea ariilor care au fost deja cercetate și gradului de cercetare a acestora. Riscurile de securitate cibernetică în IC reprezintă un subiect emergent din cauza atacurilor recente, precum și a rolului critic al componentelor TI în sistemele fizice. Luând în considerare numărul de abordări în IC, managementul riscurilor ar trebui să fie cuprinzător și fie scenarii care să acopere și riscurile cibernetice. Această constatare evidențiază potențialele cercetări în definirea unui sistem de sprijinire a deciziilor pentru identificarea, clasificarea și propunerea de controale care ar gestiona eficient riscurile cibernetice în IC.

Se recomandă facilitarea acestui proces prin utilizarea sistemelor suport de decizie. Elementele care ar trebui luate în considerare de acest sistem sunt: cunoștințele despre sistemul IC și componentele sale digitale, metodologiile și instrumentele de atac cibernetic, reziliența, interconectarea, dependența și rezultatele care pot fi ușor citite și înțelese. Întrucât aceste elemente ar putea implica cantități mari de date specializate, sistemul de suport decizional ar asista decidenții în identificarea riscurilor și selectarea celui mai bun pachet de măsuri de atenuare. Acesta ar fi, un sistem care ar promova utilizarea sigură a tehnologiilor emergente în contextul IC, contribuind la o poziție de securitate mai bună și care ar mări rezultatele generale de securitate.

Au fost identificate câteva domenii, care nu au o acoperire extinsă, precum și subiecte viitoare de cercetare. Înțelegerea riscurilor cibernetice și a tuturor implicațiilor asupra unei infrastructuri critice, în combinație cu sistemul de suport decizional, permite operatorilor și decidenților 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 necesare pentru susținerea obiectivelor pe termen lung în gestionarea riscurilor emergente.

În timp ce evenimentele fizice și daunele din infrastructurile critice s-au concentrat ani de zile pe sistemele de sprijinire a managementului riscurilor în identificarea și evaluarea riscurilor, nu acoperă în mod exhaustiv noua natură a riscurilor pe care o aduce spațiul cibernetic. Având 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 SSD să fie adoptat de alte sisteme și utilizat în scenarii de caz real. Un astfel de sistem modular ar completa procesele de management al riscului în domenii precum nuclear, radiologic sau sănătate [67, 68].

Aceste rezultate constituie date valoroase asupra posibilității de a utiliza SSD pentru managementul riscurilor cibernetice în infrastructurile critice, care validează și confirmă actualitatea întrebării de cercetare selectate. Studiul a oferit, de asemenea, date de încredere în

înțelegerea stării actuale, precum și a modului de avansare a studiului în întrebarea principală de cercetare din această analiză sistematică a literaturii.

Cunoștințele acumulate au permis identificarea lacunelor și servește drept bază pentru planificarea agendei de cercetare în acest domeniu.

S-a identificat de asemenea necesitatea de a explora factorii pentru care un SSD trebuie să fie luat în considerare atunci când se analizează managementul riscurilor cibernetice în domeniul IC.

2. SISTEM SUPORT DECIZIONAL PENTRU MANAGEMENTUL RISCURILOR CIBERNETICE ÎN INFRASTRUCTURI CRITICE

Cercetarea din acest capitol începe cu analiza sistematică a literaturii referitoare utilizării SSD pentru gestionarea riscurilor cibernetice în domeniul IC. Pentru a asigura calitatea analizei, au fost evaluate la cele mai recente evoluții, cercetări și rezultate în acest domeniu.

Pe baza acestor rezultate a fost descris conceptul de SSD propus pentru managementul riscurilor cibernetice în IC. Cercetările și discuțiile inițiale cu privire la rolul securității cibernetice și modalitățile de îmbunătățire a controalelor securității cibernetice într-un domeniu atât de critic precum nuclear și radiologic au demarat în 2010 [69]. Interesul și necesitatea unui astfel de concept pentru îmbunătățirea managementului riscurilor cibernetice în vederea prevenirii atacurilor cibernetice în infrastructurile IC rezultă de asemenea din activitatea ca lector invitat (2015-2017) al Departamentului de Siguranță și Securitate Nucleară al AIEA. În această perioadă, autorul prezentei teze de doctor a participat la pregătirea și prezentarea unei serii de prelegeri privind securitatea cibernetică din cadrul cursurilor de formare pentru operatori nucleari și radiologici oferite de AIEA în Kazahstan, Slovenia și Moldova. Scopul principal a fost de a prezenta și conștientiza rolul securității cibernetice în sistemele de operare și securitate fizică utilizate de operatorii nucleari și radiologici. Aceste sisteme variază de la sisteme de suport fizic, până la sisteme TI generice de întreprindere a IC care ar putea fi utilizate în oricare dintre operatorii sau organizațiile cu oportunități de conectate la acestea. Adițional, acest subiect a fost cercetat în cadrul consultărilor CNSSN și în capacitatea de evaluator expert în cadrul proiectelor de cercetare Horizon 2020 și a Consiliului European de Inovare. De asemenea, autorul tezei a fost lector invitat pe această tematică la Conferința Națională de Securitate Cibernetică organizată de Information Systems Audit and Control Association și Banca Națională a României (2017), cât și ca membru de juriu a Black Sea Science Competition din Odesa, Ucraina (2022) în care au fost prezentate lucrări din acest domeniu.

În această teză sunt evaluate principalele elemente și etape critice care trebuie luate în considerare în managementul riscurilor cibernetice pentru domeniul IC, considerentele arhitecturale pentru SSD în sfera de aplicare, precum și o analiză cuprinzătoare a impactului dimensiunii umane. Scopul este de a dezvolta un concept care poate fi adoptat și adaptat la necesitățile oricărei IC, rezolvând în același timp provocările actuale în ceea ce privește riscurile cibernetice. Evitând limitarea unui software sau aplicații care ar putea deveni depășită foarte repede, precum și să provoace dificultăți de integrare din cauza limbajelor de programare sau

tehnologiilor utilizate, se asigură o integrare eficientă, interoperabilitate, precum și o economie de costuri, pentru implementările viitoare ale acestui concept.

În acest capitol analiza sistematică a literaturii a fost principală metodă de cercetare științifică. Metodologia selectată permite identificarea, evaluarea și rezumă un număr de studii primare, pentru a extrage date care să ajute la formularea de concluzii despre un anumit subiect. Ca parte a acestei teze, s-a utilizat analiza sistematică a literaturii, ca proces cuprinzător, precum și analiza selectivă a literaturii, ca un proces mai puțin solicitant, care ar ajuta la confirmarea stării actuale a unei anumite întrebări.

Analiza sistematică a literaturii este un tip de studiu secundar care utilizează o metodologie predefinită pentru a identifica, analiza și interpreta toate studiile existente și disponibile cu privire la o anumită întrebare [70]. Chiar dacă analiza sistematică a literaturii este utilizată frecvent în cercetări din domenii precum mediul înconjurător sau medicina, procedurile pot fi ajustate pentru alte domenii precum TI sau dezvoltarea de software [71].

Acest model de studiu a fost selectat deoarece reduce probabilitatea unei părtiniri, precum și creează o imagine de ansamblu cuprinzătoare asupra subiectului dorit. Rezultatele analizei sistematice a literaturii vor sprijini capacitatea de evaluare a stadiului actual a studiilor cu privire la întrebarea principală abordată. Pașii repetabili a unei analize sistematice a literaturii în identificarea, extragerea și agregarea informațiilor sunt considerați a fi un tip de cercetare științifică. A fost documentat protocolul pentru cele mai importante analize efectuate. Acest lucru asigură că procesul de identificare și analiză a literaturii poate fi repetat în mod transparent de oricine.

Avantajul acestei proces este că permite identificarea critică a stadiului actual al artei unui anumit subiect, identificarea lacunelor de cercetare și a domeniilor care pot fi potențial explorate, precum și eliminarea cercetărilor duplicate. Acesta este motivul principal pentru alegerea acestui tip de cercetare științifică, având în vedere tema discutată în această teză.

Procesul de realizare a unei analize sistematice a literaturii începe cu informațiile generale despre un subiect sau întrebare care trebuie abordată. Aceasta poate fi urmată de întrebări sau obiective secundare care vor fi abordate prin acest proces. Definiția întrebării este un punct de plecare critic, deoarece trebuie să acopere în mod adecvat întrebarea de cercetare dorită și să evite orice ambiguitate sau dublu sens. În caz contrar, există riscul ca rezultatele studiului să nu abordeze întrebarea inițială.

Procesul continuă prin definirea strategiei utilizate în realizarea acestei analize. În cazul dat s-a utilizat ca strategie pentru a identifica elementele cheie care să constituie procesul de căutare. Se presupune alegerea cuvintelor cheie potrivite astfel, încât să fie afișate rezultatele

căutării relevante, dar și să fie excluse rezultatele irelevante. Acest lucru va facilita procesele viitoare de citire pe diagonală, și deciderea în includerea rezultatului în procesul de evaluare.

Un alt aspect important este identificarea surselor care să fie utilizate pentru identificarea și extragerea literaturii relevante pentru procesul de analiză sistematică. Sursele trebuie evaluate pentru a se asigura că acestea sunt credibile. Sursele utilizate în cadrul acestei teze au fost articole sau lucrări științifice, cărți, reviste, lucrări de conferințe, standarde sau alte teze și recenzii. Acestea au fost atent selectate pentru evitarea riscului de părtinire.

Procesul de analiză trebuie să conțină și criteriile de includere și excludere pentru lista de rezultate obținute inițial. Acest proces asigură că studiile semnificative și relevante sunt incluse în procesul de analiză, în timp ce sunt excluse studiile care ar fi putut corespunde cuvintelor cheie relevante, dar se concentrează pe un subiect diferit. Acest lucru asigură că s-au selectat studiile în funcție de criterii inițial predefinite, minimizând astfel riscurile de selecție subiectivă și părtinire.

Înainte de a efectua analiza, care a și fost documentată, s-au efectuat o serie de încercări pentru a asigura că metoda selectată de studiu permite satisfacerea necesităților abordate cu cerințele noastre. De asemenea, a fost documentat numărul total de rezultate returnate inițial pentru fiecare sursă, precum și numărul final de articole incluse în recenzie.

Deoarece au fost analizate în principal reviste științifice din surse online de încredere, se consideră că publicațiile au fost deja supuse unor evaluări de calitate. Cu toate acestea, a fost efectuată și o validare de bază a fiecărui studiu înainte de analiza cuprinzătoare, pentru a asigura că setul de lucrări conține date relevante care pot fi considerate veridice.

După selectarea studiilor finale pentru analiză, acestea au fost evaluate dacă abordează întrebarea și obiectivele cercetării inițiale. Analiza a fost atât calitativă, cât și cantitativă, bazată pe scopul evaluării. Extragerea datelor a fost documentată sub formă de text sau tabel, pentru a fi în conformitate cu metodologia de analiză a literaturii de specialitate. Acesta conține, printre altele, o scurtă descriere a studiului sau modul în care acesta abordează întrebările noastre de cercetare, asemănările sau diferențele dintre studiile selectate, precum și rezultatele pe care acestea le reflectă. Analiza cantitativă, acolo unde este posibil, a ajutat la identificarea unui anumit decalaj. Având în vedere natura și domeniul cercetării noastre, majoritatea rezultatelor au fost prezentate sub formă narativă în urma analizei calitative.

În urma aplicării metodologiei s-au formulat concluzii cu privire la rezultatele obținute, punctele tari și punctele slabe ale studiului efectuat, relația cu rezultatele anterioare, precum și importanța acestor date pentru această teză. Acest lucru a permis conturarea obiectivelor de cercetare și dezvoltarea planului pentru cercetarea întrebării inițiale. S-a utilizat metoda logică pentru a rezuma cercetările în utilizarea SSD în scopul propus, iar metoda comparativă pentru a

dezvolta conceptul de SSD, precum și modelul de evaluare a securității cibernetice, pentru IC în orice domeniu, astfel încât acestea să poată să fie aplicate universal.

2.1. Utilizarea sistemelor suport decizionale în managementul riscurilor cibernetice. Analiza sistematică a literaturii

S-a aplicat cercetarea prin analiza sistematică a literaturii pentru a stabili stadiul actual în utilizarea sistemelor de suport decizional pentru managementul riscurilor cibernetice în infrastructurile critice. Acest tip de cercetare permite efectuarea unei analize imparțiale asupra cercetărilor existente și identificarea zonelor care necesită explorare ulterioară. Cercetarea a facilitat rezumarea cunoștințelor și studiilor existente pe această temă pentru a putea poziționa mai bine acțiunile ulterioare de cercetare în acest domeniu. Identificarea, evaluarea și tratarea riscurilor cibernetice ale componentelor tehnologiei informației din cadrul infrastructurii critice au un impact major asupra stării generale de securitate și siguranță. Cantitatea de date care trebuie procesată și analizată depășește adesea capacitatea operatorului sau a factorilor de decizie. De aceea, a fost explorat în ce măsură sunt utilizate în prezent SSD pentru a depăși această limitare în managementul riscurilor cibernetice și pentru a lua decizii rapide și informate față de riscurile identificate.

Deoarece domeniul de aplicare al unei astfel de analize este larg, a fost o provocare de a selecta lucrările și cercetările care urmează să fie analizate. A fost acordată prioritate lucrărilor de analiză legate de managementul riscurilor în protecția IC, pentru a înțelege punctele de vedere și provocările în procesul de luare a unei decizii. S-a acordat prioritate surselor de încredere, cum ar fi reviste de cercetare sau rapoarte de la organizații naționale sau internaționale. Pe baza analizei și observațiilor au fost extrase elementele cheie relevante pentru protecția IC. De asemenea, s-a efectuat o analiză sistematică a literaturii de specialitate pentru a identifica, evalua și rezuma stadiul tehnicii sistemelor de suport decizional pentru managementul riscurilor cibernetice în infrastructurile critice.

2.1.1. Definirea întrebării și protocolul de cercetare

În contextul acestei analize sistematice a literaturii, întrebarea principală este de a evalua măsura utilizării SSD pentru managementul riscurilor cibernetice în IC. Obiectivele sunt următoarele:

- A rezuma dovezile existente ale SSD pentru managementul riscurilor cibernetice în IC.
- A identifica lacunele în cercetarea curentă și pentru a sugera domenii pentru investigații ulterioare.

- A oferi cadrul pentru a poziționa în mod corespunzător noile activități de cercetare.
- A efectua o analiză imparțială asupra întrebării de cercetare propuse.

Criteriile de includere sunt:

- Studii care discută combinația dintre securitatea cibernetică, managementul riscurilor, IC și SSD.
- Studii care menționează analiza sistematică a literaturii de specialitate pentru a evalua și gestiona riscurile cibernetice în IC.
- Studii care descriu SSD utilizate în managementul riscurilor cibernetice în IC.

Criteriile de excludere sunt:

- Studii care nu au legătură cu întrebarea principală de cercetare.
- Studii care menționează necesitatea unui SSD dar nu descriu în mod explicit un asemenea sistem.

Întrebările specifice sunt următoarele:

1. Este descris ori propus un SSD în cadrul lucrării date?
2. Este SSD un prototip sau utilizat în practică?
3. Este lucrarea concentrată în mod explicit pe riscurile cibernetice? Dacă nu, pe ce tip de riscuri se concentrează lucrarea?
4. Ce domenii ale managementului riscurilor sunt discutate?
5. Este studiul orientat pe infrastructuri critice în general sau pe domenii specifice?

2.1.2. Efectuarea analizei. Identificarea cercetărilor existente

Strategia de căutare a fost adaptată pentru a corespunde cu întrebarea principală de cercetare și pentru a identifica toate studiile conexe existente. Preliminar s-au efectuat căutări pentru a vedea dacă analiza sistematică a literaturii de specialitate nu a fost deja efectuată la tema data. Ulterior, s-au efectuat mai multe încercări în identificarea termenilor de căutare potriviți. Toate căutările au fost efectuate utilizând combinația următorilor termeni: „infrastructură critică” și „sistem de suport decizional” și „risc” și „cibernetic”. Deoarece SSD și IC pot fi privite ca o gamă largă de sisteme, nu au fost luați în considerare alți termeni specifici pentru cercetarea dată, cum ar fi SCADA, ICS, sisteme expert, *data mining* sau *business intelligence*. Căutările au fost efectuate prin utilizarea termenilor selectați mai sus în limba engleză.

Diferențele dintre termenii de căutare în comparație cu criteriile de includere au creat o muncă suplimentară. Totuși s-a decis asupra acestei abordări deoarece numărul de rezultate prin căutarea termenilor exacți din rezumat și cuvinte cheie a fost inițial foarte scăzut. Pentru a asigura

că nu lipsesc rezultate relevante, s-a decis să fie incluse mai multe cuvinte cheie generice precum „risc” și „cibernetic” și să fie evaluate manual articolele în funcție de criteriile de includere.

Sursele selectate pentru a colecta studiile existente asupra surselor de întrebări de cercetare sunt ACM, Science Direct și Springer. Acestea sunt platforme ce conțin articole din reviste sau de la conferințe din domenii tehnice precum TI, IC și managementul riscurilor. Majoritatea din aceste articole au fost supuse deja procesului de *peer-review*.

Numărul de articole inițiale găsite și numărul final de articole care au fost păstrate pentru analiza sistematică a literaturii sunt descrise în Tabelul 2.1.

Tabelul 2.1. Sursele pentru analiza sistematică a literaturii și numărul de articole identificate

Sursă	**Descriere**	**Numărul total de studii găsite**	**Numărul de studii selectate pentru a fi analizate**
ACM	Biblioteca digitală ACM este o platformă de cercetare care conține: colecții integrale a tuturor publicațiilor ACM, inclusiv reviste, lucrări ale conferințelor, reviste tehnice, buletine informative și cărți; o colecție de publicații cu text integral organizate și găzduite de la edituri selectate pentru literatura TI. Biblioteca digitală ACM poate fi găsită pe următorul site web: https://www.acm.org	12	1
Science Direct (acces deschis)	O bază de date cu peste 2.900 de reviste și 300.000 de cărți. Baza de date *Science Direct* poate fi accesată prin următorul site web: https://www.sciencedirect.com	13	0
Springer	Baza de date cu reviste și articole. Baza de date *Springer* poate fi accesată prin următorul site web: https://link.springer.com	68	5
Total		93	6

Căutările au fost efectuate în data de 4 aprilie 2020. Din lista inițială au fost eliminate articolele care nu sunt relevante pentru întrebarea de cercetare și se concentrau pe anumite elemente legate de căutarea prin efectuarea unei evaluări în baza titlului și cuvintelor cheie. După acest prim pas al triajului, numărul lucrărilor ce urmau a fi analizate a constituit 42 (ACM – 8, *Science Direct* – 6, *Springer* – 28). Următorul pas a fost lectura pe diagonală pentru a evalua dacă studiul are legătură cu SSD în managementul riscurilor cibernetice pentru infrastructura critică. Lista finală a constituit din 6 lucrări. În timpul procesului inițial s-a observat că există foarte puține studii care abordează tema de cercetare și că cele mai multe dintre ele au fost elaborate cu mai bine de 10 ani în urmă. Procesul a fost repetat pentru a asigura că au fost identificate toate studiile relevante și legate de întrebarea de cercetare.

2.1.3. Extragerea datelor

Studiile care au îndeplinit criteriile de includere au fost evaluate și întrebările specifice au fost răspunse în Tabelul 2.2. Acest lucru a oferit capabilitatea de a sintetiza și rezuma mai ușor rezultatele.

Tabelul 2.2 Evaluarea studiilor identificate.

Referință (Autor și an)	**Se concentrează lucrarea în mod explicit pe riscurile cibernetice? Dacă nu, pe ce tip de riscuri se focusează?**	**Ce subprocese din managementului riscurilor sunt discutate?**	**Studiul se referă la infrastructuri critice generice sau specifice?**	**Număr-rul de citări**
Amantini et al (2012) [72]	Da	Toate	Generic	9
Choraś et al (2009) [73]	Nu toți	Identificarea, Analiza, Evaluarea	Generic	4
Choraś et al (2010a) [74]	Da	Toate	Specific: telecomunicații, energie și transporturi	6
Choraś et al (2010b) [75]	Nu toți	Toate	Generic	8
Setola et al (2017) [76]	Nu toți	Identificarea, Analiza, Evaluarea	Generic	6
Kozik et al (2010) [77]	Nu toți	Identificarea, Analiza, Evaluarea, Tratarea	da	4

Numărul de citări a fost extras din baza de date a platformei în care a fost găsit inițial studiul.

2.1.4. Sinteza narativă

Cercetarea prin analiza este o sarcină destul de complexă și extinsă din cauza subiectului specific. Observația inițială este că s-au identificat un număr mare de rezultate, însă puține articole au fost relevante pentru întrebarea de cercetare.

De asemenea, analizele și rezultatele din toate lucrările sunt dispersate și acoperă diverse obiective sau întrebări de cercetare. S-a identificat un accent pe reziliență și conștientizarea contextuală în mai multe lucrări, denotând importanța acestor factori în domeniul infrastructurii critice. Deși acest lucru nu este neapărat legat de întreaga întrebare de cercetare care a fost abordată în acest capitol, contribuie la susținerea necesității imperative de a avea un studiu complex asupra temei.

Ca rezultat al analizei sistematice a literaturii se pot face următoarele observații [78]:

- Niciunul dintre studii nu descrie un SSD utilizat în practică – toate descriu SSD la nivel de concept sau un prototip.
- Conceptele și metodologiile utilizate în cadrul SSD descrise variază de la ontologie, rețele bayesiene, modelare de interdependență la clasificare și corelație.
- Toate studiile au anumite limitări și nu au fost concepute pentru toate tipurile de amenințări cibernetice.
- Se observă un accent pe sectorul energetic în ceea ce privește managementul riscurilor.
- Mai puțin de jumătate dintre studii se concentrează în mod explicit pe anumite tipuri de riscuri cibernetice.
- Majoritatea studiilor care au fost analizate din perioada 2009-2012 și doar un singur studiu a fost publicat relativ recent în 2017 .
- Sistemele descrise se concentrează pe diferite procese din cadrul managementului riscului.
- Se presupune că experții în securitate au atât cunoștințe TI, cât și TO în domeniu atunci când utilizează SSD [72].
- Două studii se referă la importanța aplicării principiilor de securitate cibernetică în SSD în sine [72, 76].

În plus, unele studii s-au concentrat pe interconectarea și interdependența dintre IC, la pericole din sectoare precum rețelele energetice sau barajele de apă [79, 80, 81, 82, 83], aspectul uman al evaluării riscurilor și luarea deciziilor, evaluarea amenințărilor cibernetice și conștientizarea contextuală [84, 85, 86, 87] și reziliența sau clasificarea investițiilor [88, 89]. Cu toate acestea, doar șase studii sunt corelate cu întrebarea inițială de cercetare. Acestea au fost incluse în domeniul de aplicare a analizei sistematice a literaturii. Studiile care au fost selectate pentru o analiză calitativă sunt sintetizate mai jos.

Choraś et al. propune un SSD care utilizează abordarea descrierii vulnerabilităților bazată pe logica ontologiei [73]. Sistemul propus este axat pe tipul general de riscuri, iar domeniul țintă este telecomunicațiile. Acest tip de domeniu conține o mulțime de rețele interconectate și eterogene, iar SSD-ul propus ar putea servi un cadru de securitate a rețelei care cuprinde diferite instrumente și tehnici pentru detectarea și toleranța intruziunilor.

Următoarele patru studii sunt analizate împreună, deoarece au autori comuni și se referă la același sistem. Choraś et al. propun un SSD axat pe riscul cibernetic pentru domeniile telecomunicațiilor, energiei și transporturilor [74]. SSD este, de asemenea, bazat pe ontologie și se referă la clasificarea și relațiile dintre vulnerabilități și amenințări asupra IC. SSD este conceput pentru a sprijini consolidarea sistemelor SCADA împotriva atacurilor cibernetice. Într-un alt

studiu, este propus un SSD similar, cu accent pe tipul general de riscuri, cu scopul de a evalua și simula securitatea în sistemele reale [75]. Kozik a propus adăugarea rețelei bayesiene la SSD descris, care se bazează pe ontologie [77]. Potrivit autorului, acest lucru ar îmbunătăți motorul de raționament al SSD și ar crea noi rapoarte, cum ar fi clasarea amenințărilor și gravitatea acestora. Amantini et al. se referă la interfața de experiență de utilizator a aceluiași SSD și recomandă ca utilizatorii și experții să aibă cunoștințe TI, pentru a putea face față interfețelor mai complexe [72]. SSD descris se concentrează pe modelarea dependenței și analiza IC și a rețelei de bază. Se concentrează pe monitorizarea, detectarea și răspunsul rețelei (rutare suprapusă *peer-to-peer*, garantarea traficului), precum și propunerea unei arhitecturi automate de detectare și recuperare a erorilor pentru SCADA.

Setola descrie un SSD pentru gestionarea situațiilor de urgență în IC. Acest sistem ar sprijini operatorii în acțiunea de răspuns și autoritățile publice în coordonare precum și planificarea de urgență [76]. Conceptul de SSD este de a utiliza o multitudine de surse de date și de a le corela pentru a estima potențialele daune și consecințe, ceea ce ar sprijini luarea deciziilor în cunoștință de cauză. De asemenea, s-a observat că studiul propune o clasificare a consecințelor potențiale, cum ar fi cele asupra cetățenilor, economiei sau alte IC și mediu. Cu toate acestea, studiul nu abordează în mod explicit atacul cibernetic ca amenințare, impactul sau consecințele acestui tip de amenințări.

În mai multe dintre studiile analizate, SSD nu sunt văzute ca soluții pentru managementul riscurilor cibernetice, dar pot fi adaptate la diverse necesități și cerințe [78]. Chiar dacă există puține rezultate care se potrivesc cu terminii inițiali de căutare și care au abordat întrebarea de cercetare, rezultatele sunt valoroase și prezintă în mod transparent stadiul actual al utilizării SSD pentru managementul riscurilor cibernetice în IC.

S-a constatat, de asemenea, că procesele generale de management al riscului, cum ar fi identificarea, evaluarea și implementarea controlului reprezintă un interes curent în cercetare [90].

2.2. Particularitățile managementului riscurilor cibernetice în infrastructuri critice

În această secțiune sunt prezentate rezultatele evaluării modului în care securitatea cibernetică se încadrează în abordările de gestionare a riscurilor pentru IC, indiferent de domeniu, cum ar fi nuclear, medical, financiar, transport și altele.

Au fost explorați factorii specifici ai managementului riscurilor cibernetice în acest domeniu, precum și provocările pentru operatori și decidenți. Interconectarea, interdependența și digitalizarea IC cresc considerabil cantitatea de date care trebuie evaluată atunci când se gestionează riscurile. Sunt necesare cunoștințe de specialitate în domeniul securității cibernetice

pentru a evalua eficient riscurile reprezentate de un sistem informațional asupra unei entități. Sunt prezentate criteriile identificate pentru un SSD, care pot îmbunătăți managementul riscurilor cibernetice în protecția IC [91].

Pentru a asigura că managementul riscurilor este adecvat în IC și conform bunelor practici, este esențial să fie identificate din faza de evaluare toate elementele necesare, definirea contextului (domeniul IC, relația cu alte IC), identificarea riscurilor potențiale, conceptele de securitate care sunt urmate sau necesare, precum și limitările sistemului [92]. Este vital să fie stabilit contextul și să se identifice parametrii care sunt necesari pentru evaluarea acestor riscuri. În comparație cu managementul riscurilor în sistemele TI tradiționale, elementele de siguranță și reziliență IC sunt unice și creează noi provocări.

Anumite elemente de management al riscului din domeniul IC sunt centrale în perspectiva tehnologiilor TI emergente. Figura 2.1 reprezintă factorii identificați care sunt critici la dezvoltarea unui sistem informațional pentru domeniul IC.

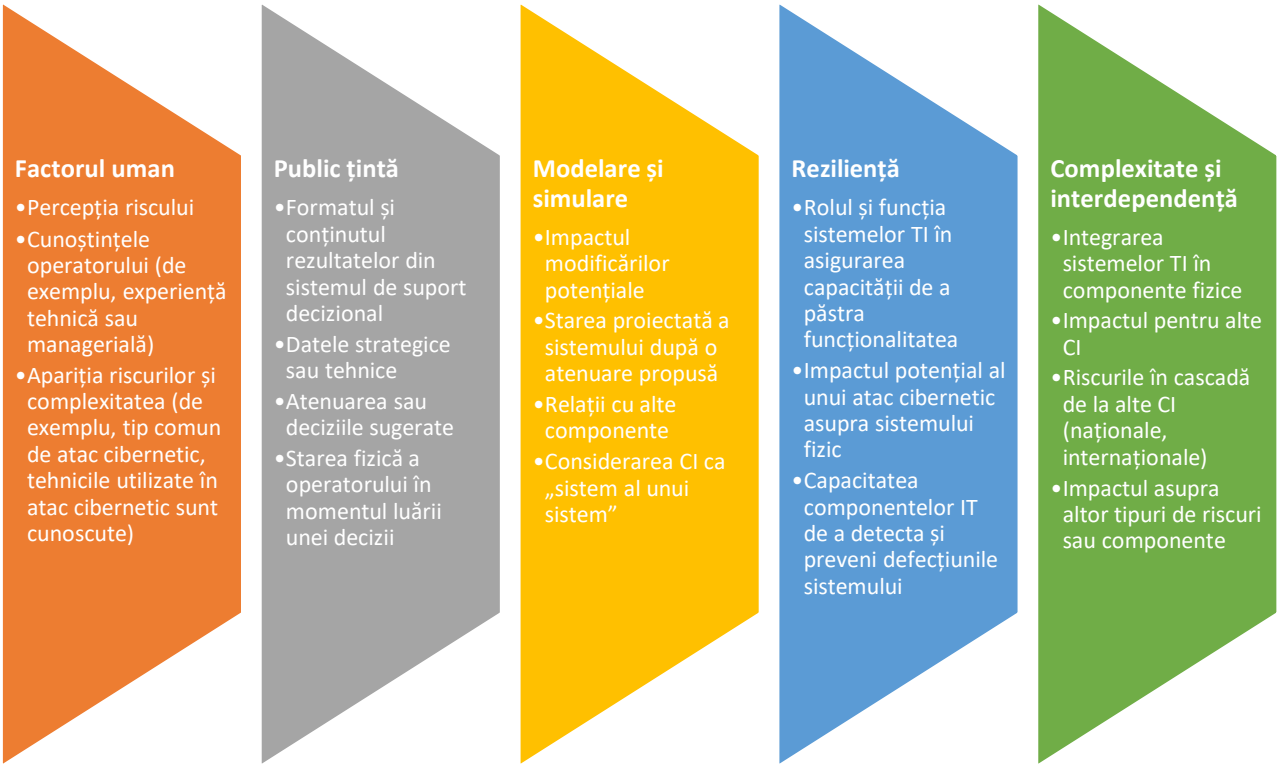

Fig. 2.1. Elemente critice pentru un SSD în managementul riscurilor

Aceste elemente au definit variabile noi care pot îmbunătăți metodologia de definire a riscurilor și de identificare a măsurilor de atenuare adecvate în domeniul IC și pot face parte din conceptul de sistem SSD pentru managementul riscurilor cibernetice. Identificarea factorilor cheie asigură faptul că SSD pentru managementul riscurilor cibernetice în IC să fie adecvat scopului și adaptat contextului.

2.2.1. Factorul uman

Factorul uman joacă un rol vital în managementul riscurilor pentru orice domeniu. Un aspect al factorului uman este că acuratețea scade pe măsură ce complexitatea crește, ceea ce este asociat și cu IC. Metodologiile de evaluare a riscurilor iau adesea în considerare un risc legat de o anumită componentă sau de funcționalitatea acesteia. Când este vorba de un atac cibernetic care ar putea afecta o componentă, adesea interconectată, sunt necesare modelări și simulări pentru a înțelege impactul precis asupra tuturor celorlalte componente și sisteme. Întrucât un IC este considerat un sistem de sisteme, iar componentele TI sunt integrate în majoritatea acestora, aceste circumstanțe creează complexitate pentru decidenți. Acest lucru este valabil și pentru identificarea și selectarea măsurilor de atenuare sau tratare a riscurilor.

Un alt factor uman important în managementul riscurilor cibernetice este percepția. Studiile recente ilustrează că experții sunt mai conștienți de vulnerabilitățile pentru care atacurile au fost raportate mai frecvent [93]. Acest lucru se datorează potențial cunoștințelor specifice acestui sistem bazate pe rapoartele de incident. În plus, percepția spune că este mai greu de efectuat un atac asupra sistemelor care sunt mai mature din punct de vedere tehnologic sau dimpotrivă prin necunoașterea nivelului de maturitate [93]. Aceasta arată necesitatea de cunoștințe de specialitate în diferite domenii, pentru a crește eficacitatea și calitatea procesului de identificare și evaluare a riscurilor.

Managementul riscurilor nu numai că a fuzionat într-un proces mai complex, dar necesită și colaborarea în timp real între mai multe părți în luarea unor decizii complexe [44]. Factorul uman este conex, de asemenea, provocărilor în dezvoltarea culturii securității pentru operatori, managementului și în rezultat cu gestionarea riscurilor în IC. Când este vorba de prezentarea riscurilor și informarea altor părți interesate, trebuie de luat în considerare elementul de factor uman. Aceste recomandări ar trebui să se reflecte în proiectarea unui SSD pentru managementul riscurilor.

Sprijinul pentru luarea deciziilor este obligatoriu pentru a înțelege impactul deplin al riscurilor cibernetice asupra unui sistem IC, precum și pentru a identifica controalele adecvate pentru a reduce aceste riscuri. Se constată că sistemele de modelare sau de sprijinire a deciziilor sunt soluția potrivită în analizarea diferitelor date de intrare și pentru furnizarea de rezultate ușor de înțeles pentru utilizator.

2.2.2. Publicul țintă

Abordările în managementul riscurilor cibernetice tind să fie diferite ca scop și conținut, deoarece acestea captează date pentru a fi luate în considerare de un anumit public. De exemplu,

anumite abordări vizează managementul superior și luarea deciziilor, în timp ce altele sunt adresate operatorilor IC. Ca atare, managementul riscurilor de securitate cibernetică nu trebuie tratat doar ca o funcție tehnică, realizată de experți TI sau TO, ci ca un proces complex orientat spre managementul integral al obiectului sau sistemului IC. Descrierea riscurilor de securitate cibernetică trebuie să fie clară atât pentru factorii de decizie, cât și pentru cei care gestionează adesea riscurile, cât și pentru operatori, care sunt adesea cei care implementează măsuri de atenuare a acestor riscuri.

2.2.3. Reziliență

Managementul riscurilor cibernetice aplicat în domeniul TO și IC aduce o nouă dimensiune, care este reziliența [94]. Reziliența definește capacitatea unui sistem de a absorbi și de a tolera anomaliile în funcționalitate sau modificări neașteptate, precum și de a recupera și continua operațiunile [95]. Acesta este un element nou care nu este des întâlnit în abordările tradiționale de management al riscului TI. În timp ce există tendințe de asigurare a rezilienței sistemelor TI având aceasta ca o cerință de bază, aspectele comune luate în considerare în prezent sunt reprezentate în așa numitul triunghi CIA din limba engleză (Confidențialitate, Integritate, Disponibilitate) care impune indirect și reziliența. Această abordare poate fi aplicată în TI și TO, totuși, din cauza specificului IC, menționarea explicită a cerinței de reziliență este obligatorie pentru a asigura disponibilitatea și funcționarea sistemului în orice moment. În sistemele ciber-fizice, reziliența este legată de toleranța la erori și sugerează că sistemele fizice continuă să funcționeze în diferite condiții, chiar dacă anumiți parametri ar putea lua valori anormale. Din perspectiva IC, se poate deduce indirect că sistemele informatice însărcinate cu o funcție ar trebui să detecteze și să tolereze defecțiunile, pentru a evita orice incidente legate de cibernetica care ar putea duce la funcționarea defectuoasă a sistemului fizic.

Elementul de evaluare a rezilienței în managementul riscurilor este o provocare, deoarece orice componentă a unui sistem trebuie să facă parte dintr-un proces cuprinzător de modelare și simulare pentru a înțelege impactul schimbărilor. Evaluarea acestui element în contextul tehnologiilor TI emergente în IC poate constitui o sarcină și mai complexă [91].

2.2.4. Modelare și simulare

Modelarea și simularea (M&S) reprezintă procedee importante pentru a evalua în timp potențialele schimbări într-un sistem, precum și pentru a crea capacitatea de a prognoza dinamica unui sistem. M&S pot fi utilizate și pentru a analiza interdependența și interconexiunea dintre IC, precum și impactul oricărei modificări a oricărei componente în întregul sistem [90].

Funcționalitățile, tehnologiile și operațiunile IC sunt utilizate pentru a modela efectele implementării controalelor de securitate și pentru a estima rezultatele după o schimbare. Acest lucru este foarte util în contextul atenuării riscurilor și în procesul general de management al riscului în IC. Cu toate acestea, deoarece există abordări diferite în protecția sistemelor IC, este o provocare de selectat cea mai eficientă soluție datorită complexității acestor sisteme.

În plus, M&S pentru IC includ deja ideea de sistem de sisteme. Este greu e vorbit despre IC care, astăzi, există izolat. De exemplu, majoritatea, dacă nu toate, IC ar depinde de furnizarea de energie. Acest lucru complică procesul de management al riscului datorită cantității și ierarhiei sistemelor care trebuie luate în considerare. În plus, îmbogățirea datelor cu conexiunile dintre IC, ale căror elemente pot fi răspândite și transfrontaliere, crește semnificativ volumul datelor de risc. Similar cu domeniul TI, conceptul de sistem de sisteme complică evaluarea și necesită tehnici de modelare.

Modelarea poate fi utilizată în procesele de management al riscului pentru tehnologiile emergente, cum ar fi internet of things, și poate ajuta la evaluarea riscurilor cibernetice [96]. Acest lucru ar sprijini înțelegerea schimbărilor în IC prin utilizarea diferitelor perspective. Cercetările actuale arată că cele mai frecvente tehnici de modelare utilizate în protecția IC sunt bazate empiric, pe experimente [90, 97], în timp ce evaluările atacurilor cibernetice bazate pe protecție sunt mai ușor de adoptat [98]. Aceste constatări ajută la conturarea unei noi abordări în asigurarea securității cibernetice și rafinarea rezultatului unui sistem de sprijinire a deciziilor în evaluarea riscurilor și a atenuărilor.

Un alt element important care trebuie luat în considerare este costul, care poate fi privit ca investiția necesară pentru implementarea unui anumit control al securității cibernetice și indirect ca cost care ar fi necesar pentru operarea sistemului după anumite modificări [99]. Mai mult, factorul de cost ar putea fi integrat în elementul propus de simulări și modelare care ar ajuta factorii de decizie în gestionarea riscurilor cibernetice în IC [91].

2.2.5. Complexitate și interdependență

Complexitatea și interdependența sunt alte particularități ale managementului riscului în IC. Dimensiunea cibernetică este integrată în sistemul fizic, ceea ce creează o nouă necesitate de a avea cunoștințe necesare gestionării riscurilor. IC ar putea fi adesea denumite sisteme ciber-fizice, care derivă din cerința de a avea atât tipuri de cunoștințe, cât și experiență pentru gestionarea riscurilor [100]. Legătura ciber-fizică se reflectă pe scară largă în cercetare ca creșterea suprafeței de atac prin utilizarea computerelor încorporate în sistemele fizice responsabile de operațiuni [101]. Acest lucru duce la o creștere a potențialelor vulnerabilități, precum și a vectorilor de atac.

În consecință, securitatea cibernetică ar trebui să fie deja inclusă în planurile generale de evaluare a riscurilor pentru orice IC și tratată ca o parte intrinsecă.

2.3. Arhitectura sistemelor suport decizionale

În această secțiune sunt descrise două sisteme care fac parte din arhitectura SSD, precum și propuse tipuri de date în raport cu sfera și contextul managementului riscurilor cibernetice în domeniul IC. Sistemele descrise conține elementele de intrare în procesul de decizie de afaceri și a proiectării interfeței cu utilizatorul. Se poate afirma că aceste elemente corespund limbii și interfeței utilizator din cadrul unui SSD, sau interfețelor de intrare și ieșire. În scopul acestei analize, s-a utilizat în mod interschimbabil noțiunile de sistem de intrare sau limbaj, precum și de sistem de ieșire sau de prezentare. Aceste două elemente au un impact semnificativ asupra performanței SSD, precum și asupra eficienței percepute. Au fost inițial identificate proprietățile cheie ale fiecărui element în acest context, apoi au fost definite categoriile de date care ar putea fi utilizate de SSD în sfera de aplicare. De asemenea, a fost propus un concept la nivel înalt al interfeței cu utilizatorul.

Au fost descrise funcțiile și cazurile de utilizare care pot fi implementate prin aceste sisteme. Această analiză se bazează pe rezultatele analizei sistematice a literaturii privind utilizarea SSD în managementul riscurilor cibernetice. A fost acordată o atenție deosebită faptului ca nu există un SSD care să acopere întreg ciclul de management al riscurilor cibernetice, ce reprezintă o oportunitate de a dezvolta un sistem modular care ar putea fi integrat în metodologiile de management al riscului pentru diverse domenii IC [78]. În plus, este necesar să fie luate în considerare elementele identificate în secțiunea anterioară atunci când este proiectat un sistem de management al riscurilor cibernetice în IC [91].

2.3.1. Sistemul limbaj

Primul element adresat în SSD este sistemul limbaj sau de intrare. Acest element este trivial pentru a asigura că SSD operează cu datele necesare și corecte pentru a procesa, a crea cunoștințe, precum și a propune soluții adecvate. Respectiv acest sistem îndeplinește funcția de introducere a datelor, prin colectarea și preluarea datelor necesare pentru alte elemente ale SSD. Clasificarea de mai jos va fi utilizată în întreaga arhitectură și conceptul de SSD propus. Cu toate acestea, tipul de date și criteriile ar trebui considerate ca fiind incomplete, deoarece acestea se pot schimba și pot fi adaptate în funcție de sursele, necesitățile și contextul fiecărei IC.

Luând în considerare diferitele formate, surse, scopuri și conținut al acestor date, suportul informatic este obligatoriu în prelucrarea tuturor datelor. Pot fi de asemenea utilizate și aplicate

tehnologii asistate de computer, cum ar fi *machine learning*, extragerea datelor și inteligența artificială. Pe baza domeniului și domeniului SSD propus, acest sistem poate avea ca intrare trei tipuri de date – datele despre profilul utilizatorului, datele despre riscuri și datele despre IC.

Figura 2.2 prezintă potențiale surse și tipuri de date propuse care sunt introduse în sistemul de limbaj.

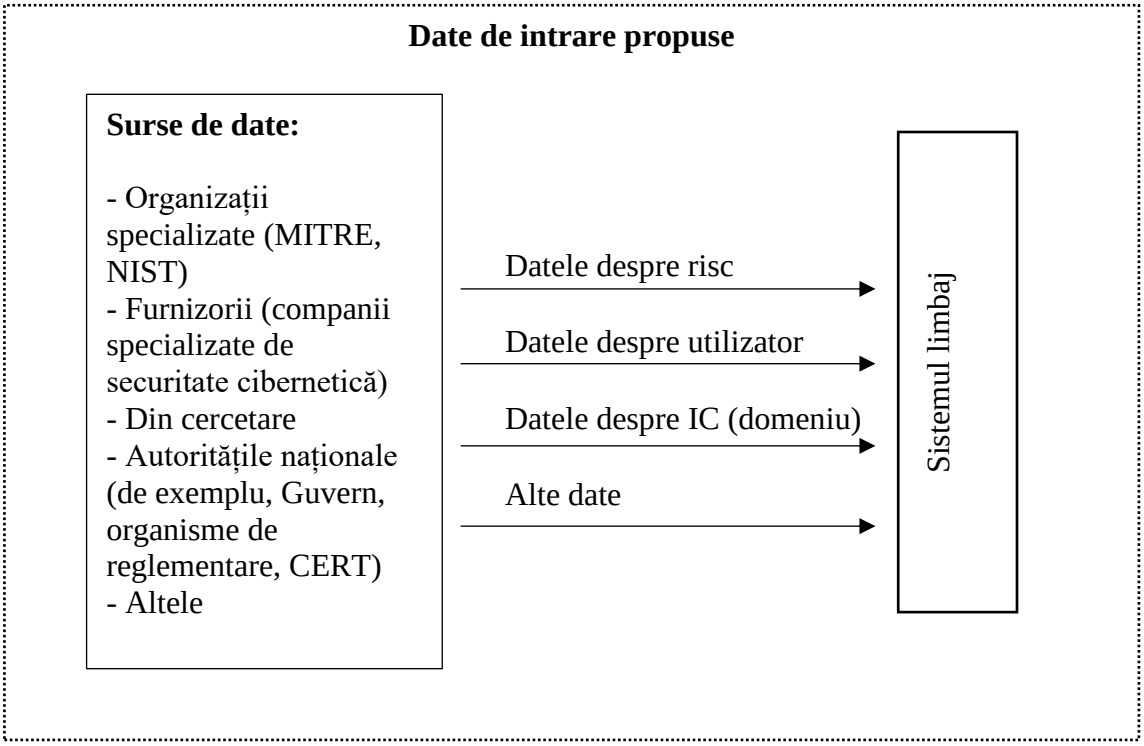

Fig. 2.2. Potențiale tipuri de date de intrare în sistemul de limbaj

2.3.1.1. Date profil utilizator

Datele profilului utilizatorului sunt un subset de date care poate fi identificat și introdus pentru fiecare utilizator. Atributele colectate permit definirea și rafinarea profilului utilizatorului, precum și cunoștințele tehnice ale acestuia în acest domeniu. Contextul și conștientizarea utilizatorilor sunt caracteristici care au fost identificate ca fiind obligatorii într-un SSD care abordează riscurile cibernetice în infrastructurile critice [91].

Un SSD ar putea învăța pe baza acțiunilor utilizatorului și poate trimite date de telemetrie prin sistemul limbaj pentru a rafina caracteristicile profilului utilizatorului. Ulterior, aceste date pot fi utilizate de sistemul de prezentare sau interfață cu utilizatorul, astfel încât datele afișate să fie prezentate utilizatorului pe baza profilului său. Acesta reprezintă un aspect care face ca un sistem să fie calificat drept inteligent. Un exemplu tipic ar fi modul în care anumite date de risc sunt percepute de către un utilizator și în ce mod sunt înțelese datele tehnice. Pe de altă parte, acest lucru s-ar putea referi și la aspectele de înțelegere a gravității reale a riscului, precum și la atenuări și controale adecvate.

Un factor de decizie, bazat pe profilul acestui loc de muncă, s-ar concentra mai mult pe aspectele strategice ale datelor de risc, care ar fi așteptate de la un SSD. Aspecte precum impactul securității sau siguranței, reputația, procentul industriei care se confruntă cu acest risc, costurile, dependența de alte IC sau chiar o potențială conexiune cu IC de stat național ar fi de interes pentru acest tip de utilizator.

Pe de altă parte, un operator care se ocupă de inginerie sau operațiuni, poate solicita detalii tehnice și caracteristici pentru fiecare risc și metode de atenuare. Date suplimentare pot îmbunătăți capacitatea de a reduce riscurile, cum ar fi starea viitoare prognozată a sistemului după ce au fost aplicate anumite modificări.

Prin urmare, pe baza profilului utilizatorului, SSD poate prezenta cunoștințele așteptate și necesare și oferi suport în procesul de management al riscurilor cibernetice. În orice soluție tehnică dezvoltată pentru acest domeniu, factorul uman joacă un rol critic.

2.3.1.2. Date de risc

Un alt tip de date care vor servi ca intrare în SSD sunt datele despre riscuri. Acestea se referă la domeniul principal al SSD și, prin urmare, reprezentă cel mai mare volum de date. Pe baza cadrelor actuale de securitate cibernetică, a standardelor și a celor mai bune practici, precum și a metodologiilor de gestionare a riscurilor, au fost clasificate datele despre riscuri pe baza anumitor criterii. Mai jos sunt descrise criteriile propuse și oferite exemple de tipuri de date despre risc și cum pot fi utilizate.

Etapa procesului de management al riscului. Procesul de management al riscului este o aplicare sistematică a politicilor, procedurilor și practicilor de management la activitățile de comunicare, consultare, stabilire a contextului și identificarea, analizarea, evaluarea, tratarea, monitorizarea și evaluarea riscului [39]. Prin urmare, datele se pot referi la anumite faze ale managementului riscului, care ar putea fi rezumate astfel:

- *identificare* – identificarea și definirea unui risc cibernetic în termeni generali;
- *evaluare* – date care ar ajuta un utilizator al sistemului să confirme dacă un risc cibernetic este aplicabil unui anumit sistem în IC, precum și severitatea riscului;
- *atenuare* - propunerea unui control pentru eliminarea sau reducerea riscului la un nivel acceptabil.

Datele despre riscuri se pot referi la faze simple sau multiple ale procesului de management al riscului. În plus, pot conține și informații generale despre riscurile identificate de comunitate sau companii similare, sau riscurile care au fost identificate în cadrul organizației țintă. Acesta este

un aspect legat de introducerea datelor care trebuie luat în considerare atunci când se dezvoltă prototipuri și modele care să analizeze, înțeleagă, stocheze și crea cunoștințe din aceste date.

Surse de date pentru construirea cunoștințelor. Acest tip de intrare este legat de clasificarea anterioară a datelor. Pe de o parte, datele despre riscuri pot descrie faza de management al riscului, dar pot fi, de asemenea, clasificate în funcție de formatul și sursele de proveniență. Mai jos sunt menționate principalele surse de date identificate privind riscurile cibernetice din IC. Datele despre riscuri cu privire la sistemele TI tradiționale ar putea fi aplicabile și în domeniul IC. Un sistem de control industrial ar putea fi monitorizat sau integrat cu PC-uri tradiționale care conțin software standard. Acest tip de interconectare duce la preluarea unor riscuri din sistemele TI tradiționale în sistemele specializate din IC. Cu toate acestea, este acordată prioritate surselor de date privind riscurile IC, deoarece acestea includ adesea sau menționează riscurile legate de TI.

Cadrul MITRE ICS ATT&CK. Acest cadru a fost dezvoltat de Corporația MITRE și conține date care descriu acțiunile pe care un adversar le-ar putea întreprinde împotriva ICS [102]. Datele conținute variază de la modul în care o rețea este compromisă, tacticile utilizate, modul de atingere a obiectivelor și procedurile utilizate. Acest cadru descrie tipuri de acțiuni care sunt utilizate în mod obișnuit de adversari în timpul fiecărei etape a unui atac cibernetic. Acest obiectiv al cadrului a fost creat pentru a înțelege mai bine cum funcționează un adversar atunci când compromite un ICS, pe baza incidentelor de securitate cibernetică descoperite [103]. Aceasta este o derivație a cadrului inițial MITRE ATT&CK, conceput pentru sisteme TI corporative sau tradiționale. O remarcă interesantă este că MITRE ICS ATT&CK menționează că anumite atacuri împotriva sistemelor de control industrial din IC sunt lansate prin intermediul sistemelor tradiționale TI [104]. Datorită specificului IC, compromiterea datelor pot avea particularități aplicabile în cadrul rețelelor ICS. Acest tip de informații este esențial pentru îmbogățirea datelor despre riscurile identificate, precum și pentru a prezenta utilizatorului soluții adecvate și măsuri de atenuare. Prin corelarea tacticilor cunoscute, a TTP-urilor cu anumite riscuri identificate, SSD poate oferi utilizatorilor sfaturi și recomandări cu privire la modul de reducere sau atenuare a acestora. Un cadru similar care există pentru rețelele tradiționale TI ar putea conține date care se suprapun. Acesta ar putea fi, de asemenea, integrat în sistemul lingvistic al SSD propus, pe baza necesităților și cerințelor. De exemplu, un IC care deține o mare parte din infrastructura TI tradițională ar putea lua în considerare riscurile TI atunci când evaluează riscurile pentru întreaga organizație.

Date legate de CVE. Common Vulnerability Enumeration, cunoscut sub numele de CVE, este un standard internațional în atribuirea unui identificator unic unei anumite vulnerabilități [105]. Aceasta este o inițiativă condusă de comunitate, în timp ce atribuirea elementelor de identificare este gestionată de organisme de securitate a informațiilor, cum ar fi Agenția de

securitate cibernetică și infrastructură din SUA. Furnizorii din domeniul ICS participă la această inițiativă, ceea ce înseamnă că CVE-urile ar putea fi o sursă bună de date structurate în ceea ce privește riscurile cibernetice pentru domeniul IC. CVE este cel mai frecvent standard utilizat în urmărirea unei vulnerabilități, precum și în identificarea informațiilor necesare pentru atenuarea acestei vulnerabilități. Fiecare vulnerabilitate din IC ar putea fi considerată un risc cibernetic, prin urmare acest tip de date ar îmbunătăți eficiența SSD. Formatul CVE este standardizat și are formatul CVE și ID-ul vulnerabilității. Prin urmare, aceste date pot fi extrase cu ușurință de modelele SSD și importate în baza de cunoștințe relevantă. Cu toate acestea, extragerea datelor în termeni de recomandări pentru soluții alternative sau potențiale dependențe, ar putea necesita asistența disciplinelor emergente, cum ar fi inteligența artificială.

Acțiuni anterioare de identificare/atenuare a riscurilor. Datele privind riscurile nu sunt neapărat partajate într-un format structurat, dar ar putea fi diseminate prin alte tipuri de media, cum ar fi note, rapoarte și chiar lucrări de cercetare. Accesul la astfel de informații este esențial în reducerea potențialelor limite de cunoștințe pe care le-ar putea avea SSD, atunci când abordează subiectele ca riscuri cibernetice.

Tipul sursei care identifică un risc cibernetic. O altă clasificare a datelor despre risc poate după criteriul de unde provin riscurile identificate. Se propun două tipuri de surse principale: externe și interne.

Externe. Datele privind riscurile care provin din surse externe sunt, în general, de încredere pentru a construi cunoștințe și pentru a oferi sfaturi atunci când este vorba de atenuarea riscurilor. Ca surse externe pot fi furnizori de date de risc, în acest caz - entități externe organizației în care este utilizat SSD, alte IC, organisme naționale, sau furnizori.

Interne. Principala sursă internă de date despre risc este organizația sau IC în sine. Organizația oferă cele mai corecte informații cu privire la riscurile cibernetice care au fost identificate prin observare, evaluarea vulnerabilităților interne, deciziile luate în cadrul IC și altele.

Direcția de solicitare a datelor. O ultimă clasificare a datelor de risc este fluxul de informații. De exemplu, cererea pentru categoriile de date descrise mai sus ar putea fi inițiată fie prin procese obișnuite, fie prin procese *ad-hoc,* care dintr-o perspectivă la nivel înalt ar putea fi clasificate ca: din interior sau din exterior.

Din sistemele externe spre cele interne. Ca parte a datelor de intrare despre riscurile cibernetice, s-au identificat sursele de date care furnizează informații către SSD, atunci când acestea vor fi publicate. Chiar dacă procesul tehnic va colecta informațiile din exterior, iar conceptual poate fi considerat ca ieșire, se consideră acest lucru ca un flux de intrare datorită

faptului că datele sunt solicitate în mod regulat și sunt utilizate pentru a construi cunoștințe. Prin urmare, aceasta este direct legată de sursa și de programul cu care sunt livrate datele.

Din sistemele interne spre cele externe. Solicitările de date de ieșire provin din anumite module SSD, ori de câte ori anumite informații despre date de risc lipsesc și se încearcă să fie colectate și asimilate. Aceasta se realizează pentru a minimiza, sau a preveni, situațiile în care SSD nu are cunoștințe cu privire la un anumit risc. Acest lucru poate apărea într-o situație ipotetică când un risc este identificat în organizație și pe baza lucrărilor cheie, ID-uri CVE sau alți indicatori, SSD acționează ca un sistem inteligent și încearcă să colecteze în timp real informații privind atenuarea riscurilor și controale care ar putea fi sugerate utilizatorului.

2.3.1.3. Date despre IC

Ultima categorie de date de intrare necesară prototipului de SSD sunt datele legate de IC. Aceasta categorie se referă la toate elementele și activele din sistemul și IC care ar putea prezenta riscuri cibernetice. În plus, datorită naturii IC și în principal a interconexiunilor, acest tip de date ar putea conține informații referitoare la interdependențe cu alte IC sau riscuri în entități externe care afectează în cele din urmă IC.

În procesul de management al riscurilor cibernetice, o potențială vulnerabilitate ar putea avea un efect în cascadă asupra altor sisteme. Prin urmare, datele IC sunt utile atunci când se relatează și conectează datele despre riscuri la sistemele digitale utilizate în organizație, pentru a putea identifica, evalua, nota și monitoriza riscurile cibernetice existente.

Alte date referitoare la IC care au, de asemenea, o importanță critică sunt interconectarea cu alte IC. În zilele noastre este aproape imposibil ca o IC să existe și să funcționeze independent. Majoritatea, dacă nu toate IC, sunt interconectate atât la nivel național, cât și internațional. O defecțiune a rețelei energetice ar putea avea un impact asupra IC la nivel local, regional sau chiar internațional. Același lucru este valabil și pentru efectele și daunele potențiale ale unui incident cibernetic.

2.3.1.4. Alte date

Categoria auxiliară de date de intrare poate fi ajustată și multiplicată după cum este necesar, în funcție de necesitățile și contextul fiecărui domeniu IC. Similar dezvoltării software, SSD-ul propus pentru gestionarea riscurilor cibernetice în IC trebuie adaptat în funcție de context. În faza de proiectare este necesar să se țină cont de factori precum, orientarea și scopul sistemului, cadrul organizațional, standardele și reglementările, factorul uman, precum și nivelul de maturitate al organizației (adaptat după [48]).

2.3.2. Sistemul de prezentare

Acest sistem are funcția de a descrie și afișa interfața principală utilizatorului și descrie soluțiile pentru întrebarea dată, sau răspunsul la solicitarea individuală făcută de utilizator. Datorită importanței factorului uman, precum și a contextului, rolul interfeței cu utilizatorul este direct proporțională cu capacitatea de utilizare a unui sistem. Cu cât este mai ușor de utilizat un sistem și cu cât interfața este mai intuitivă, cu atât este mai probabil ca sistemul să fie acceptat și adoptat rapid de către utilizatorul final. Acest lucru are un impact direct asupra eficienței SSD. Drept rezultat, datele reprezentate într-un format clar, adaptat necesităților și profilului utilizatorului, vor crește impactul pozitiv al SSD în procesul de management al riscurilor cibernetice.

Ca parte a acestui sistem, datele returnate de sistem vor depinde în mare măsură de profilul utilizatorului, cum ar fi conducerea superioară sau operatorul, precum și de datele despre riscuri cibernetic care sunt asociate cu cererea. Printre acțiunile și formatele de date care sunt returnate de sistemul de prezentare, sistemul ar trebui să fie capabil să proceseze tipuri standard de solicitări, precum și să se adapteze și să învețe noile tipuri de solicitări. Printre tipurile standard de solicitări, interfața ar trebui să fie capabilă în orice moment să furnizeze informații cu privire la riscurile cibernetice identificate în IC, inclusiv impactul sau pierderea potențială, atenuarea și costurile propuse. Acestea sunt informațiile care sunt cel mai des percepute ca soluție pentru gestionarea riscurilor cibernetice. În plus, sistemul ar putea să furnizeze date despre orice tip de risc cibernetic care este aplicabil în domeniul dat, incluzând, dar fără a se limita la, descrierea riscului, pașii de identificare, evaluare, precum și atenuare. Sistemul se referă la caracteristica inteligentă a sistemului, deoarece trebuie să înțeleagă și să se adapteze în funcție de tipul de căutare.

Ținând cont de capacitatea modulară a acestui SSD, sistemul de prezentare poate conține și o interfață REST (*Representational State Transfer*), care este o metodologie cunoscută pentru introducerea și extragerea datelor prin intermediul API-urilor. Acest lucru va permite SSD să fie ușor integrat și conectat la alte sisteme, cum ar fi cadrele generale de gestionare a riscurilor care ar putea fi utilizate în cadrul organizației. API-ul REST poate fi utilizat și în cazul în care SSD este independent. Comenzile pot fi integrate cu ușurință și utilizate de sistemul de prezentare pentru a efectua analize în vederea evaluării abilităților tehnice ale utilizatorului. În cazul în care utilizatorii vor recunoaște că datele sunt clare și controlul a fost implementat, sistemul poate învăța și înțelege că rezultatul a fost selectat și afișat în mod adecvat. Alternativ, sistemul poate înregistra alegerea utilizatorului de a afișa mai puține informații tehnice sau soluții alternative pentru un anumit risc cibernetic, pentru ca mai apoi aceste informații sa fie utilizate pentru îmbunătățiri si ameliorări.

Prin urmare, acest tip de interfață este dependent de calitatea datelor consumate de sistemul limbaj, cum ar fi datele profilului utilizatorului sau datele despre riscuri și demonstrează un rol important în eficiența SSD, precum confirmarea sau perfecționarea cunoștințelor privind anumite riscuri cibernetice.

2.4. Rolul dimensiunii umane

Dimensiunea umană are un rol critic în dezvoltarea și utilizarea oricăror sisteme de sprijinire a deciziei. Pentru a asigura că performanța și calitatea deciziilor recomandate de computer sunt performante, dimensiunea umană trebuie evaluată în toate fazele dezvoltării sistemului. În plus, domeniul și contextul în care vor fi utilizate sistemele pot impune cerințe suplimentare. De exemplu, domeniile în care siguranța și securitatea reprezintă o preocupare principală induce necesitatea privind o instruire continuă a utilizatorilor și sisteme avansate care sunt ajustate la cerințe. În această secțiune, este evaluată implicarea dimensiunii umane în cadrul unui sistem de suport decizional pentru managementul riscurilor cibernetice în IC. A fost analizat impactul pe care această dimensiune îl are asupra sistemelor de suport decizional și se propun soluții pentru a depăși sau gestiona mai bine limitările cunoscute cauzate de elementele factorului uman. De asemenea, este discutat despre modul în care soluțiile și recomandările propuse pot crește eficiența SSD utilizate în IC.

Nu există o definiție universală pentru dimensiunea umană. În cadrul acestei teze, dimensiunea umană este definită ca multitudinea de aspecte care descriu activitățile umane, de la etică la cunoaștere. Termenul „elementele factorului uman” este similar cu „dimensiune umană” și se referă la noțiuni ca înțelegere, interpretare, percepție, abilități de a îndeplini o sarcină sau chiar de a descrie starea fizică.

Tot din jur se bazează pe decizii, decidem asupra meniului, traseului pentru a ajunge la serviciu sau îmbrăcămintei în funcție de prognoza meteo sau de agenda zilnică. Pe lângă contextul și factorii care influențează rezultatul decizional, factorul uman are un rol cheie în interpretarea și perceperea contextului, identificarea deciziei dorite și în cele din urmă luarea deciziei. Oricare dintre acțiunile enumerate mai sus ar putea avea rezultate similare sau diferite pentru oricare, în același context.

Evaluarea și integrarea dimensiunii umane în timpul dezvoltării unui SSD devine o sarcină complexă, deoarece trebuie analizat un spectru larg de variabile legate de acest factor. În contextul sistemelor utilizate în medii cu cerințe sporite de siguranță sau securitate [106], precum IC, elementele factorului uman au o prioritate și importanță și mai mare.

Rolul dimensiunii umane proliferează puternic în toate aspectele domeniului IC. În acest capitol, sunt explorate particularitățile elementelor factorului uman și impactul acestora asupra eficienței unui sistem informațional. Anterior s-a identificat deja că acest element nu este abordat în mod adecvat în faza de proiectare [107]. De asemenea, sunt evaluate aceste aspecte în raport cu un SSD propus ca soluție viabilă de sprijinire a procesului decizional în gestionarea riscurilor cibernetice în domeniul IC.

Necesitatea intervenției umane sau a supravegherii sistemelor dintr-un domeniu IC este aplicabilă și SSD-ului. Acestea sunt mai mult decât o tehnologie și reflectă dimensiunea socială, tehnică și culturală. Aceasta implică faptul că un SSD trebuie evaluat în funcție de criteriile create de dimensiunea umană, deoarece acest tip de sistem informațional este puternic conectat cu utilizatorii săi și reprezintă un sistem socio-tehnic. Evaluarea SSD trebuie să includă și impactul pe care l-ar avea sistemul asupra performanței utilizatorilor [108]. În plus, este necesară evaluarea calității vieții utilizatorului după ce are la dispoziție un astfel de sistem, precum și efectul general asupra organizației, costurilor sau strategiilor de implementare [108].

Pe baza criteriilor de mai sus, fiecare sistem trebuie proiectat și adaptat domeniului de utilizare [109], necesităților utilizatorilor și rolurilor din organizație, precum și contextului. Această abordare trebuie analizată din perspectiva dimensiunii umane, întrucât elementele factorului uman pot reprezenta un impact major, sau un beneficiu, asupra dezvoltării, utilizării și eficienței SSD. În plus, contextul domeniului poate indica, chiar și indirect, anumite cerințe funcționale pentru SSD, precum și asupra proceselor organizaționale. Factori precum domeniul de aplicare, tipul de acțiuni și impactul acestora, precum și obiectivul general al SSD, contribuie la modelarea și definirea cerințelor sistemului.

Când vine vorba de categorii de utilizatori, următoarea listă neexhaustivă descrie utilizatorii principali ai SSD în domeniul de aplicare:

- *utilizatori* (decidenți sau operatori),
- *sponsori și beneficiari* (conducere superioară și proprietari ai sistemului),
- *dezvoltatori* (responsabili cu dezvoltarea tehnică și implementarea SSD),

Pentru ca SSD să fie adoptat și utilizat activ în cadrul organizației, precum și proiectat eficient, este necesar ca toate rolurile sa fie implicate din faza proiectării unui sistem [49]. Această lista poate fi extinsă, în funcție de cerințele și necesitățile organizației față de SSD.

Interfața SSD are unul dintre cele mai importante roluri în asigurarea faptului că sistemul este utilizabil și bine adoptat în organizație. Un produs TI greu de utilizat are mai puține șanse să aibă succes, chiar dacă oferă toate funcționalitățile necesare. Contextul și elementele factorului

uman sunt printre factorii principali care modelează interfața SSD, care are o influență directă asupra eficienței SSD. Prin urmare, dimensiunea umană poate avea un impact asupra securității unui sistem, atât pozitiv, cât și negativ [110]. Interfața, de exemplu, poate sprijini și ajuta utilizatorii să ia decizii mai bune. Mai mult, contextul specific al SSD dictează evaluarea comportamentului uman atunci când vine vorba de protejarea unui sistem [111]. Luând în considerare acest lucru, se va evalua atât impactul pozitiv, cât și negativ al dimensiunii umane asupra sistemelor informaționale.

2.4.1. Dimensiunea umană în sistemele informaționale

Dimensiunea umană are un rol critic în dezvoltarea și utilizarea sistemelor de sprijinire a deciziei [91, 107]. Elementul de *cultură profesională,* care presupune cunoștințe despre domeniul specific, abilitățile necesare pentru a utiliza eficient SSD, precum și *formatul și conținutul* afișat de sistemul de prezentare, joacă roluri continue și majore în atingerea sferei și eficienței propunerii. SSD. Pentru a gestiona riscurile cibernetice, sunt necesare cunoștințe specializate și actualizate despre riscuri și atenuări pentru a controla mai eficient aceste riscuri. Integrarea acestui proces în domeniul IC stabilește cerințe specifice pentru rezultatele furnizate de SSD. Mai jos este explorat impactul elementelor factorului uman asupra sistemelor limbaj și de prezentare.

Un SSD pentru managementul riscurilor cibernetice în domeniul IC poate fi caracterizat ca un sistem informațional inteligent, de colaborare, centrat pe utilizator, care se adaptează la profilul utilizatorului. O soluție pentru a depăși limitările cunoscute ale factorului uman este ajustarea rezultatelor în funcție de rolul utilizatorului. Aceasta reprezintă una dintre capabilitățile propuse ale interfeței cu utilizatorul, care poate fi văzută ca o extensie a capacității de adaptare. Datele profilului utilizatorului reprezintă o sursă critică de date care poate fi extrem de utilă în depășirea constrângerilor cunoscute create de dimensiunea umană. Aceste date, și cunoștințele construite în jurul lor, ar putea fi stocate ca parte a tipului de date de profil de utilizator pentru a face parte din sistemul lingvistic [107]. capacitatea de a oferi rezultate adaptate unui anumit rol se referă direct la formatul și conținutul datelor prezentate de SSD. Mai jos sunt câteva exemple.

- *dezvoltatorii* trebuie să vadă datele tehnice și modul în care sistemul funcționează în timp real, pentru a verifica și ajusta codul ca parte a sarcinilor sale;
- *factorii de decizie* necesită informații strategice cu privire la riscurile cibernetice identificate, impactul potențial, reputația, costurile estimate pentru atenuare și alte tipuri de date la nivel înalt. Pe baza domeniului de aplicare al SSD propus, acest rol supraveghează procesul de management al riscului, este informat despre rezultatul și

progresul atenuării sau poate solicita orice alte informație de la alte roluri, cum ar fi de la operatori;

- *operatorii* necesită date tehnice privind riscurile cibernetice, sistemele digitale afectate, dependențele cu alte sisteme și îndrumări pentru a atenua sau limita acest risc și, de asemenea, capacitatea de a colabora cu alții. Acesta ar fi profilul care necesită rezultate tehnice complexe și intuitive care pot include, printre altele, - starea proiectată a sistemului, progresul implementării pentru atenuări, ghiduri sau proceduri de la furnizori, precum și capacitatea de a coopera cu orice alte roluri în timpul acestor procese. Un sistem clar și intuitiv ar sprijini enorm sarcinile îndeplinite de rolul operatorului și ar minimiza și potențialele incidente de siguranță.

Orice abateri majore în sistemul de prezentare în ceea ce privește formatul, conținutul și relevanța rolurilor ar putea reprezenta un risc pentru acceptarea SSD. Acest lucru poate avea implicații semnificative asupra operațiunilor, securității și siguranței IC. În literatură acest risc a fost definit ca opacitatea sistemului în care output-ul nu este adaptat rolului: fie există prea multe, fie nu sunt suficiente informații, fie sunt suficiente, dar sunt prezentate într-o manieră confuză [49].

O altă soluție care ar îmbunătăți eficiența percepută a SSD este simplitatea interfeței cu utilizatorul. Prin răspunsuri clare și o interfață intuitivă, sistemele informaționale beneficiază de o rată mai mare de succes și de utilizare. Cu cât este mai ușor de găsit și citit informațiile referitoare la un risc cibernetic, cum ar fi descrierea, dependențele, impactul, costul și atenuările - cu atât este mai probabil ca acest risc să fie înțeles rapid și corect de către utilizator și, eventual, controlat eficient. Această caracteristică a interfeței cu utilizatorul poate avea un impact direct asupra eficienței reale, percepute, a SSD.

De asemenea, este argumentată necesitatea de a construi SSD ca un *modul* pentru interoperabilitate și pentru a facilita integrarea în alte metodologii de management al riscului [91]. Standardele comune și taxonomia pentru schimbul de date pot fi utilizate pentru a realiza acest lucru, precum și pentru a reduce costurile și pentru a oferi funcționalități de interoperabilitate. În mod similar, standardele pot fi utilizate în procesul de proiectare și dezvoltare a interfețelor utilizator, respectând în același timp cele mai bune practici și recomandări în ceea ce privește designul ușor de utilizat.

Conform lui F. G. Filip, standardul ISO 9241 poate fi văzut ca o soluție utilă, utilizabilă și utilizată pentru interfețele SSD [108]. Această serie de standarde se referă la aspectele hardware și software-ergonomie pentru interacțiunea umană cu sistemul [112]. Diferite module ale

standardului se referă la cerințele privind modul de utilizare a tastaturii, meniurilor, dialogurilor de comandă, precum și aprofundează în domenii mai specializate, cum ar fi proiectarea centrată pe om, accesibilitatea, afișajele vizuale electronice, interacțiunea tactilă și chiar designul pentru dispozitivele fizice de intrare [112]. Utilizarea unor astfel de standarde este o soluție de perspectivă. Acest lucru ar asigura că un SSD modern beneficiază de aceeași interfață prietenoasă și utilizabilă, chiar dacă utilizează tehnologii emergente. Unele dintre aceste tehnologii sau concepte pot fi biometria (recunoașterea vocii/vorbirii/feței), realitate virtuală sau realitate augmentată. În cazul unor cerințe specifice, orice interfață cu utilizatorul poate fi ajustată sau îmbunătățită în continuare în funcție de necesitățile sau reglementările fiecărei întreprinderi.

Percepția este un alt element legat de factorul uman. În contextul dat aceasta se referă la evaluarea rezultatelor furnizate de SSD, precum și la înțelegerea datelor reale. Procesul de percepție este direct legat de calitatea înțelegerii, estimării și evaluării riscurilor cibernetice real sau a atenuărilor. Unele studii arată că utilizatorii sunt mai conștienți de vulnerabilitățile pentru care atacurile sunt raportate mai frecvent [93], posibil datorită familiarității și cunoștințelor specifice acestui sistem pe baza rapoartelor de incident. Din altă parte, studiile arată că percepția competențelor și resurselor necesare pentru a efectua un atac cibernetic este direct legată de estimarea unei maturități tehnologice ridicate a unui sistem sau de lipsa cunoștințelor despre nivelul de maturitate [93]. Percepția este un factor care poate avea un impact negativ asupra eficienței sistemului informațional, bazat pe mediul, cultura sau cunoștințele utilizatorului final.

Acest lucru demonstrează încă o dată că dimensiunea umană este complexă, iar la dezvoltarea SSD sau a interfețelor sale trebuie luate în considerare diferite tipuri de cerințe. Cerințele pot fi utilizate și în timpul evaluării regulate a eficienței sistemului. *Percepția* este unul dintre cele mai critice elemente ale factorului uman, cu repercusiuni directe asupra eficacității și calității procesului de identificare și evaluare a riscurilor.

Un cadru care poate susține estimarea percepției este *Modelul de Acceptare Tehnologică* (TAM), care poate prognoza integrarea unei anumite tehnologii [144]. Acest model a fost utilizat inițial în context industrial și a câștigat ulterior popularitate în evaluarea acceptării sistemelor informaționale [113]. TAM a fost utilizat în evaluarea schimbării comportamentului și a adoptării noilor tehnologii, cum ar fi computerele personale [114], tehnologiile care permit senzorii [115] sau serviciile electronice [116]. TAM constă din două variabile:

- *utilitatea percepută* (PU) a tehnologiei de către utilizator;
- *ușurința de utilizare percepută* (PEU), care reflectă evaluarea utilizatorului cu privire la cât de ușor este de utilizat tehnologia pentru o anumită sarcină.

Un exemplu de aplicație TAM se referă la parole: o parolă puternică are un PU mare, dar un PEU redus, deoarece parolele ar putea fi uitate [117]. Dacă se adaugă autentificarea cu doi factori, atunci PEU ar crește, în timp ce PU ar putea crește sau scădea, în funcție de percepția utilizatorului. Prin urmare, evaluarea și măsurile corective necesită luarea în considerare a altor factori. TAM nu este neapărat o soluție universală și se recomandă să fie integrată ca parte a altor modele [118]. Acest model poate fi utilizat și pentru a descrie parțial percepția umană în contextul sistemelor informaționale, mai ales că este propus un SSD care să fie utilizat în domeniul IC, care este adesea asociat industriei. Acest factor poate fi inclus în procesele de evaluare a eficienței. De asemenea, contextul este trivial pentru a estima mai bine PU și PEU. În cazul dat, acesta s-ar referi la cultura de securitate (organizațională sau individuală), conștientizarea utilizatorilor în ceea ce privește amenințările și impacturile generate de riscurile cibernetice, instruirea utilizatorilor pentru a putea descuraja sau atenua aceste amenințări, precum și sistemul în sine (de exemplu, interfață cu utilizatorul, controale de securitate, performanță). În plus, cunoștințele deținute de utilizatorii finali în TI pot facilita îmbunătățirea experienței utilizatorului, precum și susținerea unui proces mai rapid de învățare și adaptare la interfețe mai complexe [72]. Cooperarea interdisciplinară între experți în TI și TO ar putea îmbunătăți percepția de ansamblu prin dezvoltarea de interfețe informative potrivite pentru mediile operaționale, precum și prin implementarea proceselor utilizabile în cadrul sistemului informațional.

Impactul, autoeficacitatea și *costul* sunt alte concepte care se referă la dimensiunea umană. Motivația de a preveni sau descuraja amenințările cibernetice este legată de amenințarea percepută, cunoștințele despre impactul potențial, capacitatea de a preveni precum și costul necesar [119]. Dacă privim SSD ca un sistem socio-tehnic, factorii externi față de utilizatori pot influența evaluarea percepției, impactului și costului chiar și a capacității de a descuraja amenințarea. Exemple de astfel de cazuri pot fi factori care au influență asupra abilităților psihologice sau fizice. Se recomandă o instruire regulată și cuprinzătoare pentru utilizatorii SSD, pentru a acoperi toate tipurile de scenarii. Deoarece domeniul IC are cerințe operaționale ridicate, o astfel de instruire nu ar fi o suprasolicitare și ar putea fi inclusă în programele obișnuite de instruire și evaluări care există deja în domeniul IC din cauza cerințelor operaționale. Mai mult, există oportunitatea de a utiliza SSD-ul propus pentru a facilita acest proces. De exemplu, acesta poate fi utilizat în modul demonstrativ pentru a susține exerciții sau programe de formare. Acest lucru poate îmbunătăți cultura profesională și poate sprijini dezvoltarea capacității interne, precum și menținerea abilităților TI necesare pentru a utiliza eficient acest sistem.

Prin urmare, SSD poate sprijini activități precum simularea sau formarea prin includerea procesului de joc în scenariile de management al riscurilor cibernetice. Acest lucru poate fi, de

asemenea, util în timpul prezentărilor de dovadă a conceptului, pentru a convinge managementul superior cu privire la investițiile necesare în securitatea cibernetică (adaptat din [99]).

Dimensiunea umană trebuie evaluată complex. Este important să recunoaștem că elementele factorului uman pot influența eficiența sistemului într-o direcție pozitivă sau negativă, în funcție de diverși factori.

2.4.2. Sistem suport decizional pentru organizații cu risc sporit

În secțiunea anterioară s-au evaluat aspecte generale ale dimensiunii umane în raport cu sistemele informaționale. Cele mai multe dintre aceste sisteme au controale de securitate adecvate pentru tipul de amenințări cibernetice. Cu toate acestea, IC reprezintă o țintă pentru grupurile teroriste sau actorilor statali, deoarece războiul hibrid a devenit destul de răspândit în ultima vreme. Prin urmare, este necesar să fie dezvoltat un număr de sisteme informaționale care consideră amenințări avansate și care sunt protejate împotriva acestora. În astfel de cazuri, cerințele de securitate și siguranță prevalează asupra costurilor și riscurilor de reputație. Când vine vorba de sistemele critice specializate, implicația dimensiunii umane este mult mai complexă și crucială. Respectiv este analizat impactul factorului uman în contextul unui SSD axat pe securitate și siguranță. IC reprezintă un domeniu în care deciziile ar putea avea un impact asupra societății, oamenilor sau chiar statelor naționale. Managementul riscurilor cibernetice în IC reprezintă un proces critic, deoarece deciziile ar putea avea un impact asupra TO utilizat în astfel de organizații.

Întrucât SSD este un sistem antropocentric, impactul dimensiunii umane ar trebui evaluat în fazele de concept și proiectare, dar și pe parcursul evaluărilor regulate. Acest lucru poate avea un impact pozitiv asupra sistemului, deoarece este proiectat într-un mod mai sigur (adaptat din [110]). Conceptele de securitate implementate precum și controalele trebuie să fie adecvate scopului sistemului și înțelese de majoritatea utilizatorilor. De asemenea, este necesar un echilibru între securitate și utilizare, pentru a avea cea mai bună eficiență. Sistemele slab utilizabile sau sistemele în care utilizatorii nu sunt capabili să facă față controalelor de securitate și respectiv sistemele vor crea o eficiență mai mică pentru organizație. Pe de altă parte, un SSD complet securizat, cuprinzător și precis, utilizat pentru managementul riscurilor cibernetice în IC nu garantează că vor fi luate cele mai bune decizii. Este la atitudinea utilizatorilor, cum ar fi operatorii sau factorii de decizie, să efectueze evaluarea finală a rezultatelor propuse și să ia decizia. O posibilitate de a depăși acest lucru poate fi automatizarea procesului decizional, care nu numai că ar sprijini, identifica sau propune o decizie, dar va lua și cea mai bună decizie [108, 120].

În general, factorii legați de comportamentul uman pot fie să îmbunătățească, fie să scadă calitatea deciziilor. Sistemele care sunt percepute ca fiind foarte avansate ar putea duce la faptul

că utilizatorul are încredere mai mult decât este necesar în rezultatele prezentate de sistem. Acest lucru ar putea reduce abilitățile analitice și profesionale ale utilizatorului în timp [108]. Pe de altă parte, sistemele mai puțin eficiente ar putea obosi utilizatorii, deoarece multe informații lipsesc sau trebuie încă procesate. Prin urmare, o abordare bine ajustată este obligatorie atunci când vine vorba de decizii care pot afecta siguranța sau securitatea.

Un model care poate fi utilizat pentru evaluarea impactului dimensiunii umane și ajustarea în funcție de sistemele informaționale pentru astfel de medii este cadrul de integrare a factorilor umani (HFI) [110]. HFI este un cadru utilizat în Regatul Unit pentru a integra factorul uman în sistemele de apărare. HFI analizează identificarea, urmărirea și rezolvarea limitărilor umane în dezvoltarea capacității. Criteriile HFI sunt atât bazate pe obiective, cât și pe risc. Un concept similar este prezent în cadrul de integrare a sistemelor umane (HSI) din Statele Unite [121]. Spre deosebire de HFI, HSI se bazează pe nouă domenii, dintre care șase coincid cu cele ale HFI. O comparație între domeniile celor două cadre poate fi văzută în Figura 2.3. Al șaptelea domeniu al HFI (social și organizațional) este, văzut mai complex în HSI (ca supraviețuire, locuință și mediu).

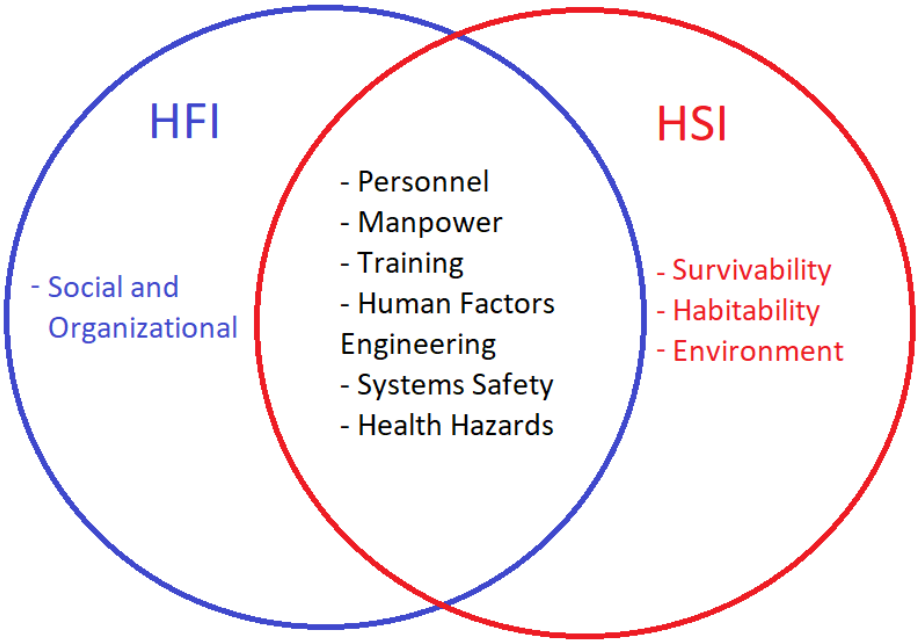

Fig. 2.3. Elemente comune și distincte între HFI și HSI

Ambele cadre se concentrează pe eliminarea riscurilor legate de dimensiunea umană și ar putea fi utilizate pentru a evalua vectorii care afectează securitatea cibernetică a sistemelor extrem de critice. Au fost efectuate anumite analize asupra modului în care sistemele informaționale pot fi dezvoltate și utilizate în organizațiile de apărare, pe baza criteriilor HFI [110]. În baza rezultatele existente vor fi propuse recomandări pentru SSD în domeniul de aplicare.

HFI are șapte domenii, însă analiza a fost efectuată doar pe șase dintre ele care sunt aplicabile securității cibernetice. Totuși al șaptelea domeniu, care acoperă pericolele pentru sănătate, poate reprezenta o amenințare externă la adresa utilizatorului final și, prin urmare, avea un impact indirect asupra securității cibernetice. Datorită complexității dimensiunii umane, aceste domenii ar trebui considerate complexe datorită interdependenței. Mai jos sunt enumerate categoriile și constatările respective, și evaluarea acestor în raport cu SSD.

Factori sociali si organizatorici. Sistemele informaționale sunt sisteme socio-tehnice care duc la faptul că utilizatorii pot reprezenta o vulnerabilitate față de sistem [110]. Acest risc este adesea influențat de politicile de management, cultura de securitate cibernetică sau chiar eficiența sistemelor informaționale. Motivația utilizatorilor, echilibrul dintre viața profesională și cea privată, pregătirea adecvată, precum și conducerea organizațională, sunt exemple care influențează pozitiv angajații și creează o cultură organizațională armonică. Lipsa includerii acestor factori în evaluările riscurilor de securitate cibernetică [122] ar putea duce la faptul că amenințările interne sunt mai mari decât cele externe [123]. Această întrebare devine și mai complexă atunci când sunt analizate abilitățile, conștientizarea, formarea și cultura utilizatorilor finali. Factorii sociali și organizaționali sunt multidimensionali și necesită o abordare complexă pentru a reduce riscurile asociate. Combinând elementele HFI cu conceptul de proces, oameni și tehnologie (PPT), poate fi corelat rolul și impactul dimensiunii umane asupra organizației (Figura 2.4).

Este important de remarcat faptul că, deși nu este posibilă eliminarea completă a riscurilor asociate cu dimensiunea umană a organizației, acestea pot fi reduse până la un nivel acceptabil printr-un proces adecvat de formare și prin consolidarea capacităților.

Ingineria factorului uman și siguranța sistemelor. În contextul SSD, aceste elemente oferă o perspectivă asupra modului în care dimensiunea umană este evaluată și integrată în proiectarea, dezvoltarea, utilizarea și evaluarea sistemelor utilizate în mediile operaționale. Această analiză ajută la optimizarea interfeței dintre utilizatori și calculatoare, precum și la asigurarea siguranței sistemului în timpul funcționării. Cea mai eficientă metodă de reducere a amenințărilor prezentate de acest element este includerea acestor preocupări începând cu faza de proiectare.

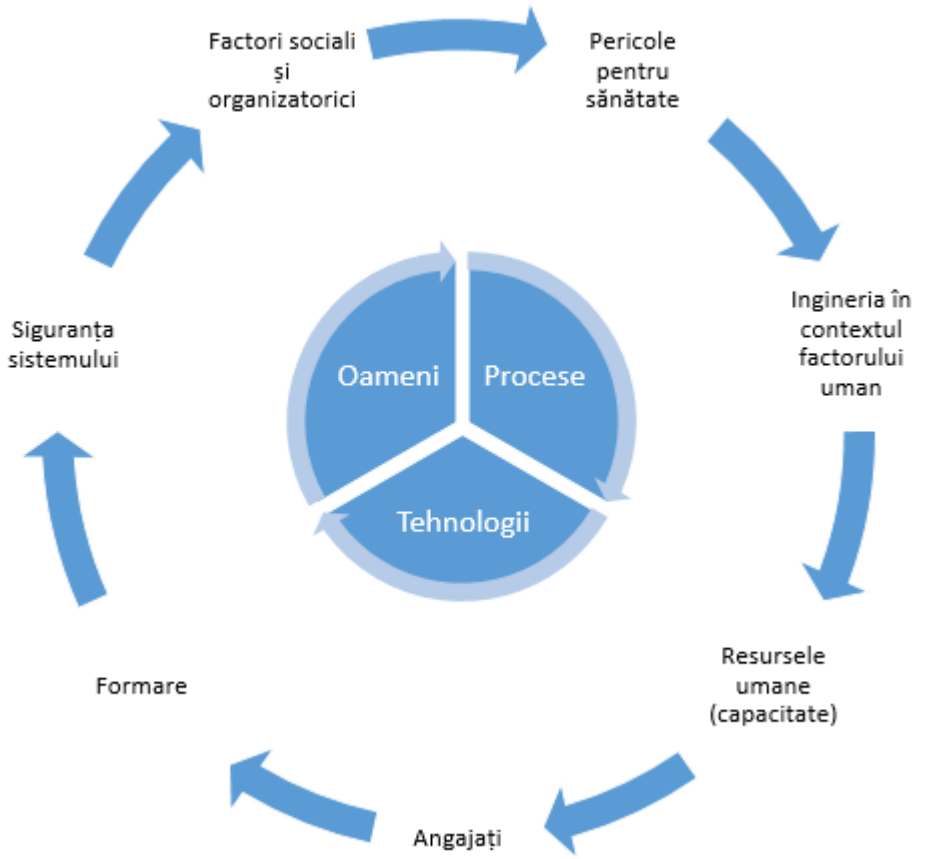

Fig. 2.4. Relația dintre factorii HFI și PPT (Adaptat după [124])

Deoarece cuantificarea și măsurarea amenințărilor reprezentate de dimensiunea umană este dificilă, tehnologiile emergente, cum ar fi biometria, pot fi utilizate pentru a evalua starea utilizatorului în timpul îndeplinirii sarcinilor critice [110]. Stresul și presiunea ar putea determina utilizatorii să ia decizii suboptime [125], ca percepție este factorul principal atunci când vine vorba de identificarea și prevenirea evenimentelor sau riscurilor de siguranță. Biometria este aplicabilă pentru domeniul SSD, deoarece această tehnologie a devenit accesibilă și destul de răspândită (de exemplu, scanarea feței, irisului sau gesturilor). Acest lucru poate fi utilizat de către SSD pentru a identifica trăsăturile care se referă la un stres sau anxietate mai mare al unui utilizator și ar putea fi o cauză pentru comportamente riscante. Un alt element care ar putea reduce riscurile prezentate de factorul uman este reziliența SSD. Aceasta ar putea fi o soluție suplimentară la nivel de aplicație în reducerea oricărui tip de sabotaj sau eroare, fie aceasta intenționată sau nu.

Forța de muncă și personalul. Forța de muncă definește nivelul resurselor umane disponibile pentru îndeplinirea unei sarcini specifice [110]. Adesea, resursele umane și financiare limitate impun organizațiile în externalizarea funcțiilor critice, inclusiv a securității cibernetice. Aceasta poate fi cauza unor noi riscuri, cum ar fi creșterea volumului de muncă pentru utilizatori și scăderea atenției și investițiilor pentru o anumită sarcină critică. Automatizarea SSD pentru

anumite sarcini simple și cu risc scăzut ar putea ajuta la reducerea acestui risc. Totuși, acest lucru poate avea și alte implicații, despre care se va discuta în capitolul următor.

Pe de altă parte, sistemele informaționale pot produce sentimentul de anonimat sau că rezultatele nu au impact în viața reală, ceea ce poate declanșa un comportament care nu este adecvat în viața reală. Acest fapt poate genera riscuri majore de siguranță din punctul de vedere al personalului. Organizațiile trebuie să ajusteze pregătirea existentă pentru a acoperi domeniul TI și riscurile inerente. În plus, posibilitatea ca un atac cibernetic să conducă la incidente de siguranță este încă subestimată, iar conștientizarea poate fi crescută prin exerciții relevante la locul de muncă.

Formarea. Programele de instruire continuă reprezintă cea mai eficientă metodă de reducere a riscurilor a factorului uman față de organizație. Instruirea trebuie să fie cuprinzătoare în ceea ce privește materialele și studiile de caz utilizate, iar pentru cele mai bune rezultate, instruirea nu trebuie să fie efectuată doar de angajator [126]. Se recomandă includerea utilizatorilor în procesul general de management al riscurilor cibernetice, pentru a crește gradul de conștientizare și cunoștințe despre aceste riscuri [110]. Instruirea este, de asemenea, recunoscută ca o soluție eficientă pentru identificarea și prevenirea amenințărilor interne [110].

O strategie de sprijin pentru instruire și conștientizare este utilizarea standardelor în identificarea și evaluarea procesului dintr-o organizație, cum ar fi standardul ISO 27001 [36]. În plus, cadrele de competență pentru îndeplinirea anumitor funcții, cum ar fi competențele esențiale ale operatorului, pot, de asemenea, diminua probabilitatea erorii umane sau riscurile create de acest factor [127]. Probabilitatea ca utilizatorii începători, neinstruiți, să se angajeze într-un comportament riscant este mai mare în comparație cu utilizatorii care au pregătire și cunoștințe adecvate despre amenințările cibernetice [117]. Pe baza acestor constatări, pot fi stabilite cerințe privind abilitățile și cunoștințele pentru îndeplinirea sarcinilor operaționale.

Cultura securității cibernetice poate fi dezvoltată eficient pe baza experienței și instruirii, precum și pe cursuri de perfecționare periodice pentru a asimila bunele practici care au fost dezvoltate între timp. Schimbul de experiență, precum și familiarizarea cu realizările inovatoare în domeniu reprezintă una dintre cele mai eficiente metode de prevenire sau minimizare a riscurilor. Cerințele funcționale în ceea ce privește instruirea utilizatorilor finali pot fi implementate în SSD. De asemenea, este important de subliniat că instruirea în domeniul securității cibernetice este un proces, datorită caracteristicii dinamice a spațiului cibernetic și a procesului de digitalizare care afectează domeniul IC [128].

2.4.3. Automatizarea procesului de luare a deciziilor

Automatizarea aplicată în luarea deciziilor prin intermediul sistemelor decizionale autonome reprezintă o soluție potențială de reducere a apariției sau impactului erorilor umane cunoscute. Deoarece această întrebare vine adesea în contextul unui SSD, se explorează stadiul actual al automatizării în SSD. Cerințele privind automatizarea și impactul au fost deja studiate [108] și au fost propuse diferite clasificări ale sarcinilor care ar putea fi automatizate [120, 129, 130]. În plus, automatizarea este văzută ca o practică bună și o recomandare în cadrele TI moderne, cum ar fi ITILv4 pentru TI Service Management [131] sau DevOps pentru dezvoltarea de software [132].

Cerințele pentru a permite automatizarea și a atribui luarea deciziilor unui sistem pot fi clasificate în funcție de tipul problemei de rezolvat [108]:

- *problemele complet structurate* pot fi rezolvate în mod adecvat prin automatizare completă;
- *problemele semi structurate* se rezolvă cel mai bine cu intervenția sau supravegherea umană, totuși SSD ar putea îndeplini anumite sarcini preliminare și sprijină utilizatorii în acest sens prin recomandarea sau propunerea unei soluții;
- *problemele nestructurate* pot fi rezolvate doar utilizând inspirația umană, cu toate acestea, SSD care utilizează concepte emergente, cum ar fi inteligența artificială sau data mining, ar putea sprijini, de asemenea, acest proces pentru mai multe aspecte.

Această clasificare trebuie desigur aplicată și în baza contextului, cerințelor impuse de mediul de lucru și caracteristica problemei. În contextul dat, domeniul IC dictează cerințe mai stricte ca un mediu operațional.

O altă strategie recomandă automatizarea sarcinilor care necesită *un comportament bazat pe abilități,* în timp ce sarcinile care necesită *un comportament bazat pe cunoștințe* să fie efectuate de utilizatori [133].

Aceste definiții pot sprijini identificarea sarcinilor care pot fi automatizate într-un mod sigur și eficient pentru domeniul SSD. Automatizarea activităților care necesită o decizie bazată pe abilități ar putea facilita munca factorilor de decizie și ar permite ca aceștia să se concentreze asupra riscurilor severe, care necesită un comportament bazat pe cunoștințe. Este de menționat că avansarea către un rol de supraveghere nu exclude cerința de a avea cunoștințe în operațiuni sau inginerie, dimpotrivă, aceasta ar fi un avantaj în IC, ca domeniu trans disciplinar, în identificarea domeniilor care pot fi automatizate.

Cu toate acestea, din progresele înregistrate în automatizare, intervenția umană nu poate fi total eliminată din SSD și ar trebui să rămână pentru sarcini în care este necesară creativitatea, utilizarea cunoștințelor și instinctul de autoconservare (adaptat din [108]). Acest fapt este impus de domeniul IC, deoarece managementul riscurilor cibernetice este un proces care necesită creativitate și analiză amănunțită, mai ales în contexte legate de IC. Comparând automatizările existente în alte medii similare, precum NASA, se observă că se adoptă aceeași abordare [134]. Automatizarea nu exclude pe deplin dimensiunea umană. Întrucât automatizarea este implementată și dezvoltată de utilizatori, există riscul ca acest proces să creeze noi riscuri banale întrucât dezvoltatorii pot sa nu dețină suficientă experiență în automatizarea unei sarcini specifice [108]. Cu toate acestea, astfel de riscuri ar putea fi reduse prin asigurarea faptului că echipele de dezvoltatori au suficientă experiență, precum și că sunt create grupuri de lucru comune pentru a evalua produsele finale create.

Managementul riscurilor cibernetice constituie un proces complex care analizează un număr mare de variabile. Deoarece numărul riscurilor cibernetice este în continuă creștere, este necesară o cooperare mai bună între factorii de decizie și operatori în identificarea sarcinilor care pot fi automatizate. În plus, cooperarea între toate părțile interesate poate duce la decizii mai bine informate, ce va conduce nemijlocit la scenariul în care investițiile în automatizare ar duce la câștiguri de eficiență și la economii. Un alt beneficiu pentru menținerea intervenției umane în SSD este păstrarea calității vieții profesionale a utilizatorului final. Asemenea sisteme trebuie să fie utile și utilizabile, dar să continue să stimuleze utilizatorii finali să gândească analitic și critic pentru a îmbunătăți deciziile luate [135, 136]. Implicarea utilizatorilor, continuă sau ad-hoc, ar asigura îmbunătățirea continuă a calității automatizării. De asemenea, utilizarea unor concepte precum AI, *data mining* și *machine learning* ar putea schimba cerințele pentru automatizare în timp. Cu toate acestea, acest lucru ar putea crea noi tipuri de riscuri și preocupări.

2.5. Concluzii la capitolul II

Aplicată la 93 de publicații relevante metoda analizei sistematice a literaturii de specialitate în domeniul utilizării SSD pentru managementul riscurilor cibernetice în domeniul IC a determinat, că riscurile cibernetice identificate, clasificarea și atenuarea ulterioară a lor reprezintă domenii insuficient explorate. Se constată, că procesul de management al riscurilor devine din ce în ce mai complex și adaptat necesităților tipului de IC. Riscurile cibernetice incluse în procesul general de management al riscului sunt mai eficient gestionate atunci când există cunoștințe de specialitate a IC.

Foarte puține metodologii evaluează impactul pe care TI și securitatea cibernetică îl au asupra IC. Astfel, un management eficient al riscurilor cibernetice în IC este realizat când se perfecționează acuratețea și capacitatea de luare a deciziilor. De asemenea s-a constatat că nu există un SSD care să ia în considerare toate tipurile de riscuri de securitate cibernetică menționate.

Din aceste considerente se propune a fi dezvoltat un concept de SSD, care ar îmbunătăți procesul de evaluare și clasificare a riscurilor. Complexitatea studiilor relevante identificate și numărul redus de studii în acest domeniu, denotă că proiectarea unui întreg SSD pentru toate tipurile de riscuri solicită timp și resurse mari. Astfel s-a reliefat necesitatea construirii și dezvoltării unui SSD modular, ușor integrabil în alte SSD sau procese de management al riscurilor. Conducându-ne de teoremele de incompletitudine ale lui Gödel se poate de concluzionat, că proiectarea unui SSD universal care să asiste combaterea tuturor tipurilor de riscuri cibernetice este imposibilă. De aceea, proiectarea SSD pentru asistența riscurilor cibernetice este posibilă realizând inițial un SSD generic, capabil să asiste combaterea noilor tipuri de riscuri prin extinderea acestuia cu module, care să realizeze cunoștințele referitoare la noile tipuri de risc apărute. Astfel, SSD pentru gestionarea riscurilor cibernetice reprezintă un sistem inteligent evolutiv, capabil să fie extins cu funcții și module care să realizeze noile tipuri de riscuri cibernetice. Această metodologie se referă la toate subsistemele SSD, inclusiv la interfețe. Un SSD dezvoltat ca un modul cu diverse interfețe standarde pentru conectare și consumare a datelor ar permite să fie gestionat eficient și utilizat în diverse tipuri de domenii.

A fost prezentat un concept de SSD pentru managementul riscurilor cibernetice în domeniul IC și s-au identificat elementele necesare la elaborarea unui SSD cum ar fi: factorul uman, publicul țintă, reziliența, modelarea și simularea, complexitatea și interdependența. Aceste elemente sunt la baza rezultatelor obținute și a cercetărilor ulterioare prezentate în capitolul următor. Au fost elaborate aspecte ale elementelor cheie identificate, precum și asupra considerentelor de proiectare pentru sistemul limbaj și de prezentare al unui SSD.

Ținând cont de importanța de analiza necesitățile și cerințele fiecărei organizații în faza de proiectare, s-au identificat și propus soluții optime pentru SSD-uri de a fi utilizate în CI pentru cele două sisteme, precum și recomandări privind evaluarea factorului uman din fază de proiectare.

Sistemul de limbaj este unul dintre primele elemente care trebuie luate în considerare atunci când se identifică tipurile de date necesare și sursele potențiale care pot fi utilizate. Ținând cont de faptul, că SSD urmează să fie adaptat pentru IC, s-au selectat și propus sursele de date relevante. În timp ce anumite abordări ce țin de riscurile cibernetice pot fi adaptate din TI, domeniul IC conține sisteme specifice, cum ar fi ICS, care trebuie luate în considerare. Structura propusă pentru sistemul limbaj ar putea fi utilizată ca punct de plecare în faza de proiectare. În cazul în care datele

de intrare nu sunt structurate, deoarece sunt analizate sisteme complexe pentru domenii specifice, categoriile ar putea fi utilizate oricum pentru a reduce costurile și resursele necesare pentru prelucrarea ulterioară a acestor date.

Interfața cu utilizatorul are unul dintre cele mai importante roluri în asigurarea eficienței și a integrării sistemului. Un sistem informațional greu de utilizat are mai puține șanse de a reuși atât pe piață, cât și în îndeplinirea scopului său. Prin urmare, evaluarea contextului și a dimensiunii umane 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. Mai mult, evaluarea comportamentului uman trebuie luată în considerare atunci când vine vorba de asigurarea siguranței [111]. Acest lucru trebuie aplicat și protecției cibernetice a unui sistem IC.

În plus, dacă privim SSD ca pe o aplicație, atunci capacitatea de adaptare ar asigura timpul și costul redus pentru rezolvarea unei întrebări, dar și îmbunătățirea calității aplicației software [137]. Un sistem care poate învăța, valida și clasifica automat tipul de date de intrare, va asigura adaptabilitatea acestuia și intervenție manuală minimă. Astfel conceptul de SSD propus să corespundă designului modular, astfel încât să poată fi adaptat la diferite tipuri de IC, precum și la necesități sau cerințe specifice în ceea ce privește managementul riscurilor cibernetice. Prin aplicarea celor mai bune practici din TI în domeniul TO, s-a observat tendința utilizării tehnologiilor web sau mobile moderne pentru a susține aspectul multi-utilizator, pentru a asigura colaborarea live ca parte a procesului de rezolvare a deciziilor [138]. În cazul gestionării riscurilor cibernetice în cadrul infrastructurii critice, acest scenariu nu este exclus și este foarte probabil ca pentru gestionarea riscurilor cibernetice la nivel național acest lucru să constituie un avantaj.

O altă condiție importantă care trebuie luată în considerare la proiectarea arhitecturii SSD este contextul. Având în vedere că SSD-ul propus are un rol și un scop specific, trebuie să fie luate în considerare aspectele care ar asigura că SSD este adecvat scopului pentru oricare dintre domeniile IC. Contextul are implicații mari asupra tuturor cerințelor sistemului, începând de la hardware și software utilizat, conectivitate la rețea, până la tipurile de date care pot fi consumate în cadrul unui sistem.

Dimensiunea umană proliferează brusc în contextul unui SSD utilizat în IC, mai ales datorită caracteristicilor operaționale ale domeniului țintă. Întrucât SSD reprezintă un sistem socio-tehnic, acesta trebuie să fie proiectat și adaptat continuu necesităților utilizatorilor și rolurilor acestora în organizație. Această afirmație poate fi corelată și cu teorema lui Gödel. Elementele factorului uman, cum ar fi percepția, abilitățile, capacitatea de a lua decizii corecte atunci când

utilizatorul este sub presiune morală sau cultura profesională joacă un rol critic în contextul SSD propus.

În plus, costul, timpii de livrare, precum și cultura organizațională pot influența, de asemenea, calitatea SSD-ului. Prin urmare, se recomandă utilizarea unor standarde, precum ISO 9241, sau ISO 27001, pentru a reduce costul și timpii de livrare dat fiind faptul că majoritatea cerințelor funcționale pot fi acoperite de standard. Mai mult, tehnologiile computerizate moderne, precum cele care citesc parametrii biometriei, reprezintă o oportunitate de a minimiza riscurile prezentate de dimensiunea umană. Un SSD poate sprijini și activități organizaționale, cum ar fi exerciții regulate sau formări. 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.

Automatizarea are de asemenea beneficii în ceea ce privește reducerea costurilor, optimizarea personalului, precum și câștiguri de eficiență. Cu toate acestea, prin definiție, un IC nu îndeplinește cerințele pentru utilizarea automată a procesului decizional atunci când gestionează riscurile cibernetice. Credem că un anumit procent de sarcini pot fi automatizate complet, chiar și în domeniul IC. Activitățile de supraveghere ale operatorilor rămân esențiale pentru o automatizare sigură și securizată, dar și pentru reducerea erorilor sau limitărilor umane cunoscute.

Rezultatele și recomandările din acest capitol pot fi utile pentru cercetătorii sau dezvoltatorii ce vor proiecta un SSD utilizat în medii critice. Elementele de factor uman descrise, precum și soluțiile propuse, ar putea fi utilizate pentru a descrie cultura utilizatorului final, cunoștințele pentru a modela utilizarea percepută și eficiența SSD-ului propus.

3. MODELUL DE EVALUARE A NIVELULUI DE MATURITATE A SECURITĂȚII CIBERNETICE

Managementul riscurilor cibernetice este un proces complex și reprezintă adesea o provocare pentru organizațiile de orice tip. În contextul domeniului IC, orice risc este critic în momentul în care poate reprezenta și o amenințare pentru TO, societate sau economie.

În acest capitol s-au utilizat rezultatele din analiza expusă anterior cu scopul de a identifica tipurile și impactul amenințărilor cibernetice asupra IC, precum și în cadrul studiilor de caz efectuate pe tema integrării securității computerelor în domeniul medicinei sau domeniului nuclear și radiologic din Republica Moldova. Aceste arii prezintă și un interes personal, datorită recomandărilor organizațiilor și organismelor internaționale acordate securității cibernetice în domenii de interes. Aceste domenii sunt considerate parte a IC și se numără printre țintele de top ale criminalilor cibernetici. Cercetarea include și o analiză comparativă a securității cibernetice între cadrul legislativ, tehnici existente și bunele practici, standarde sau ghiduri internaționale.

Ulterior, rezultatele obținute precum și teoria existentă au fost utilizate în dezvoltarea unui model de evaluare a nivelului de maturitate a securității cibernetice pentru organizațiile din IC. Acest model este complementar conceptului de SSD propus în capitolul II și conține elementele și aspectele critice identificate mai devreme. Modelul va sprijini implementarea SSD și evaluarea aspectelor organizaționale în legătură cu riscurile cibernetice pentru a asigura că SSD este adecvat scopului, este eficient și îndeplinește obiectivele.

Acest model poate fi văzut ca o metodă inovatoare pentru îmbunătățirea nivelului de securitate cibernetică a IC. Modelul oferă capabilitate de a identifica direct și indirect zonele și acțiunile necesare pentru minimizarea riscurilor cibernetice și creșterea rezilienței IC. Modelul propus a fost evaluat pozitiv de către experți externi din acest domeniu și a fost recunoscut aplicativ și util (Anexa 2, Anexa 3, Anexa 4). Modelul a fost de asemenea premiat cu Medalia de Bronz în cadrul Salonului Cadet INOVA 2021 (Anexa 5), Medalia de Bronz în cadrul Salonului internațional de Invenții și Inovații „Traian Vuia” 2022 [191], iar elementele modelului au fost publicate într-un capitol aparte în lucrările conferinței IE21 desfășurate în mai 2021 la București (România) [139].

Acest tip de activitate asigură că produsele dezvoltate sunt potrivite scopului într-un scenariu real. Având în vedere circumstanțele și contextul domeniului IC, obținerea de referințe și avize de la entități externe confirmă actualitatea și necesitățile conceptelor și modelelor propuse în această teză.

Mai mult, pentru a valida și a prezenta modelul a fost dezvoltat un prototip ce servește ca un concept care imita procesul de evaluare (Anexa 7). Activitatea experimentală a oferit perspective asupra arhitecturii SSD, performanței acestuia, precum și impactului și integrării unui astfel de sistem într-o organizație. Această aplicație a fost, de asemenea, comparată conceptual cu cercetările anterioare din acest domeniu, pentru a evalua aplicabilitatea și acuratețea. Rezultatele obținute au fost integrate în recomandările și considerațiile finale pentru utilizarea SSD în managementul riscurilor cibernetice.

În plus, modelul propus a fost demonstrat ca fiind aplicabil în cadrul evaluării retroactive a nivelului de securitate cibernetică pe baza studiilor de caz anterioare. Aceste rezultate au validat repetat eficiența modelului, cât și au ajutat la identificare tendințelor în dezvoltarea unui program de securitate cibernetică. Toate rezultatele obținute, dezvoltate, prototipurile și conceptele au fost publicate în reviste sau lucrări ale conferințelor, astfel fiind supuse expertizelor experților.

3.1. Un model de evaluare pentru maturitatea securității cibernetice

Managementul riscurilor cibernetice poate reprezenta o provocare pentru decidenți sau operatori, datorită faptului că riscurile cibernetice pot afecta oricare dintre procesele organizaționale. Legătura percepută dintre riscurile cibernetice și tehnologie a stabilit mentalitatea că îmbunătățirile tehnologice sunt soluții pentru minimizarea riscurilor cibernetice. Pe de altă parte, dimensiunea umană este un domeniu foarte complex și rolul său este adesea subestimat atunci când vine vorba de tehnologie sau de gestionare a riscurilor cibernetice. Este necesar să fie identificate prioritățile și domeniile care necesită atenție, pentru a se asigura că informațiile și tehnologiile operaționale sunt sigure. În această secțiune este prezentat modelul de evaluare a maturității securității cibernetice. Pornind de la premisele că elementele factorului uman sunt adesea identificate drept cauze ale incidentelor cibernetice și au un impact semnificativ asupra eficienței percepute a unui SSD [140, 141]. O privire de ansamblu la nivel înalt care ia în considerare dimensiunea umană este esențială pentru a se asigura că SSD este acceptat și va îndeplini obiectivele predefinite în organizație. În procesul de ameliorare a managementului riscurilor cibernetice în domeniul IC, unele dintre soluții se pot concentra pe interfața de utilizator SSD, formatul rezultat și conținutul [142, 107]. Cu toate acestea, elementele factorului uman, cum ar fi pregătirea, percepția, capacitatea de a îndeplini sarcini critice, precum și politicile organizaționale joacă un rol important în asigurarea securității cibernetice. Acestea pot spori sau reduce eficiența operatorilor, având un impact asupra elementelor factorului uman. Ținând cont de acest lucru - eficiența SSD este direct dependentă de nivelul de maturitate al securității cibernetice din organizație.

Pe de altă parte, soluțiile care reduc impactul negativ al factorului uman au un rol major în eficiența SSD, dar și în procesul de management al riscurilor cibernetice în organizație. O recomandare de a utiliza taxonomii sau standarde poate ajuta la îmbunătățirea unui sistem din diferite puncte de vedere și la reducerea costurilor. Cu toate acestea, multitudinea de elemente și soluții necesare de analizat poate crea confuzie. Prin urmare, metodologia care poate ameliora stabilirea priorităților pentru îmbunătățirea managementului riscurilor cibernetice ar facilita acest proces și ar îmbunătăți poziția de securitate generală a IC. Pentru acest domeniu, s-a construit modelul de evaluare care poate ajuta și la identificarea limitărilor majore care împiedică dezvoltarea culturii de securitate cibernetică. Procesul de dezvoltare a modelului dat s-a raportat la constatările și recomandările privind analiza impactului dimensiunii umane asupra SSD propus [143], precum și la extinderea asupra cadrelor existente, astfel, la integrarea factorului uman [144].

3.1.1. Stadiul cercetărilor în acest domeniu

În această secțiune este evaluat stadiul actual al evaluării dimensiunii umane în raport cu sistemele informaționale. Acest lucru ajută la identificarea atributelor semnificative pentru modelul propus. Pentru a evalua stadiul actual al cercetărilor din domeniu, s-a efectuat un scurt studiu asupra impactului dimensiunii umane asupra tuturor sistemelor informaționale, cu atenție asupra domeniului IC . S-a ales ca metodologie analiza selectivă a literaturii – o metodă de cercetare care permite rezumarea rezultatelor obținute anterior.

A fost efectuată o căutare utilizând termeni în limba engleză care definesc întrebarea de cercetare: „*factor uman*” ȘI „*rol*” ȘI „*sisteme informaționale*” ȘI „*infrastructură critică*”.

Portalul selectat pentru căutare a fost *SpringerLink* (disponibil la https://www.springer.com). Acesta reprezintă o colecție online de reviste sau cărți științifice și tehnologice. Pe baza căutării inițiale, au fost returnate un total de 165 de rezultate. Ulterior, a fost efectuată o altă căutare cu termenii (în engleză) „*factor uman*” și „*dimensiune umană*”, deoarece acești termeni sunt utilizați cel mai frecvent. Astfel, au fost identificate alte 18 lucrări și cărți, dintre care 4 au fost similare cu cele de la căutarea inițială. Prin urmare, termenul de „*factor uman*” este utilizat mai des și este menționat în majoritatea studiilor relevante. În continuare, s-au examinat rezultatele examinând titlul, cuvintele cheie și rezumatele. În final, au fost selectate 25 de studii care se potrivesc cel mai bine cu întrebarea de cercetare. Ulterior principalele constatări și relevanța lor față de întrebarea principală de cercetare au fost rezumate. Prima impresie creată de studii ar putea fi părtinitoare, deoarece a fost utilizată o singură platformă pentru căutare. Cu toate acestea, majoritatea cercetărilor se concentrează pe soluții tehnologice. Aceeași observație

este menționată într-unul dintre studii, care menționează că scopul inițial al tehnologiei ca soluție de îmbunătățire a soluției umane, este ignorat la scurt timp după implementarea sistemului [145].

Implicația dimensiunii umane în sistemele informaționale a fost analizată de câteva decenii [145, 146] și studiată din diferite puncte de vedere. Pe de o parte, accentul managementului superior este să investească în soluții tehnice [140], deoarece poate fi un impact semnificativ dacă sistemele sunt inutilizabile și nu îndeplinesc domeniul de aplicare [145]. Cu toate acestea, factorul uman este identificat și ca sursă a multor incidente [140, 141], și duce la consecințe care derivă din eroarea umană [147], care ulterior sunt utilizate ca tehnici de atac, cum ar fi ca inginerie socială pentru a compromite rețeaua unei IC [148].

Mai mult, indiferent de impactul și rolul pe care dimensiunea umană îl are în raport cu sistemele informaționale, majoritatea studiilor au identificat soluții care se concentrează pe tehnologie [149, 150]. Au fost identificate și alte elemente ale factorului uman ce pot fi potențiale cauze, precum reacțiile cognitive și afective în relație cu sistemele informaționale [142] sau reacția comportamentală în momentele critice [151]. Dintre soluțiile discutate pentru îmbunătățirea poziției dimensiunii umane, cea mai comună recomandare este îmbunătățirea formării și creșterea gradului de conștientizare [149]. Există, de asemenea, soluții pentru îmbunătățirea politicilor organizaționale, precum și naționale [141], sau îmbunătățirea sistemelor din punct de vedere tehnic pe baza cerințelor derivate din perspectiva dimensiunii umane, cum ar fi analiza domeniului de lucru, conceptul de inginerie a factorului uman [152], sau ergonomie pentru asigurarea siguranței utilizatorilor finali [153].

Faza de proiectare este, de asemenea, abordată în mai multe lucrări în legătură cu implementarea necesităților utilizatorilor finali [146]. Printre efectele care pot proveni din faza de proiectare se numără: costul ignorării dimensiunii umane, influența proiectanților [145] și influența dezvoltatorilor asupra sistemului [154]. Un alt aspect critic reprezintă limbajul confuz și înțelegerea cerințelor către sistem [145], care pot avea un impact asupra produsului final. Mai mult, importanța formatului de prezentare și a conținutului în momentul testării finale a sistemului [145], calitatea deciziilor [155] sau tipul de informații legate de securitate [156], au fost, de asemenea, printre subiectele abordate în literatura. Există o convergență a cercetării conform căreia eficiența și productivitatea depind în mare măsură de dimensiunea umană, care este adesea percepută ca veriga cea mai slabă [141], dar și ca soluție [149].

În studii mai recente, subiectele ce țin de etică pentru un proces responsabil de cercetare [157], precum și îndrumările privind utilizarea în siguranță a inteligenței artificiale devin tot mai actuale [158]. Se observă, de asemenea, o schimbare în perceperea rezilienței ca o combinație de factori sociali și organizaționali și nu numai din perspectiva aplicației sau hardware [141, 150].

În general, vedem că dimensiunea umană este parțial luată în considerare atunci când vine vorba de utilizabilitate, eficiență sau beneficii ale unui sistem informațional. Cu toate acestea, analiza factorilor și soluțiilor este fracționată, deoarece nu există o viziune sau o abordare complexă. În timp ce unele soluții se concentrează pe reducerea impactului negativ al anumitor elemente ale factorului uman, găsim că există spațiu de interpretare pentru a înțelege care ar fi abordarea și rezultatele finale dorite. Pe de altă parte, îmbunătățirile tehnologice sunt cel mai adesea identificate ca soluții, chiar și pentru erorile cunoscute ale factorului uman.

3.1.2. Modelul de maturitate a securității cibernetice

Pe baza rezultatelor analizei selective a literaturii de specialitate, precum și a studiilor anterioare [143], se poate afirma că un model care ar permite decidenților să efectueze o evaluare complexă asupra stării securității cibernetice, ar fi o inovație. Acest lucru ar putea fi și complementar modelelor existente în evaluarea maturității securității. Modelul propus va conține criterii pentru fiecare dintre principalele categorii care fac parte dintr-un program de securitate cibernetică: administrare și management, educație și evaluare, mediu de lucru și managementul riscurilor de securitate cibernetică. Față de cadrele existente, precum HFI care se concentrează pe achiziții în sectorul apărării și este specific datorită domeniului și cerințelor, s-a dorit construirea un model ușor de citit și aplicat de decidenți, sau chiar operatori. În plus, se propun diferite niveluri de maturitate care includ bariere de securitate cibernetică bine cunoscute, atunci când vine vorba de tehnologiile operaționale utilizate în IC. Acest model poate servi și ca mijloc de evaluare a culturii actuale de securitate cibernetică, care este un subiect comun de cercetare. Deoarece acest model este multidimensional, el poate servi și ca metodă de evaluare a performanței și a caracteristicilor oferite de soluția dată, sau de sistemul de bază de cunoștințe, care sunt componente ale SSD. În cele din urmă, poate servi și pentru a descrie cazuri de utilizare care urmează să fie implementate în sistemul de rezolvare a chestiunilor date.

Acest model are ca scop oferirea de suport pentru decidenți să înțeleagă dacă managementul riscurilor cibernetice ar trebui îmbunătățit prin îmbunătățiri tehnologice sau prin reducerea impactului negativ al elementelor factorului uman. Premisa pentru aceasta abordare constă în faptul că managementul riscurilor cibernetice este un proces socio-tehnic, datorită impactului pe care dimensiunea umană îl are asupra securității sistemului. Din punct de vedere organizațional, asigurarea că securitatea cibernetică este abordată în mod adecvat poate contribui la alte obiective de dezvoltare, cum ar fi competitivitatea economică [159]. Cercetarea se bazează pe datele din anumite studii selectate care evidențiază dificultățile de realizare a evaluării riscurilor pentru sisteme complexe și interconectate [160], pe care le reprezintă IC. Mai mult, unele studii

recomandă, de asemenea, construirea de noi sisteme de management pentru a aborda riscurile din diferite domenii ale sistemelor cibernetice, din perspective diferite, cum ar fi fizică, cognitivă sau socială [161, 162].

Pentru a asigura integrarea modelului în mediul actual al IC, precum și în scopuri de optimizare, s-a făcut referire la cadrele existente utilizate pentru evaluarea culturii de securitate în domenii cu cerințe stricte de siguranță și securitate. De exemplu, operatorii nucleari sau radiologici, care sunt considerați parte a IC, au cerințe de siguranță și securitate stabilite pe termen lung, care au adăugat securitatea cibernetică de-a lungul timpului [163, 164]. Acest lucru va evita orice dublare a eforturilor, precum și va promova integrarea modelului propus.

În plus, modelul a fost dezvoltat analizând necesitățile privind conformitatea sau auditul ISO27000. Acest standard analizează sistemul de management al securității informației al unei organizații și conține politici, proceduri care definesc nivelul de acceptare a riscurilor al organizației, domeniul general și direcția în ceea ce privește managementul securității informațiilor și procedurile aferente care implementează sistemul propriu-zis. Un sistem de management al securității informațiilor se bazează pe următoarele principii și concepte [36]:

a) Conștientizarea necesității securității informațiilor.
b) Atribuirea răspunderii pentru securitatea informațiilor.
c) Asigurarea unei abordări cuprinzătoare a managementului securității informațiilor.
d) Încorporarea angajamentul managementului și interesul părților interesate.
e) Creșterea valorilor societale.
f) Evaluări de risc care determină controale adecvate pentru a atinge un nivel acceptabil de risc.
g) Prevenirea și detectarea activă a incidentelor de securitate a informațiilor.
h) Reevaluarea continuă a securității informațiilor și efectuarea de modificări, după caz.

Pe parcursul dezvoltării modelului, s-a efectuat o comparație și s-a constatat că dimensiunile propuse reflectă în principiu conceptele și principiile generale de securitate a informațiilor descrise mai sus. O corelare între dimensiunile propuse a modelului propriu și principiile și conceptele ISO 27001 este redată mai jos:

- Administrare și management (a, b, c).
- Educație și evaluare (a, b).
- Mediu de lucru (d, e).
- Managementul riscului de securitate cibernetică (d, f, g, h).

Corelarea nu este definitivă, întrucât unele principii și concepte se pot reflecta în general la orice dimensiune, datorită rolului și importanței pe care acestea îl au în cadrul unui program de securitate cibernetică. Pe baza acestor constatări, putem reda importanța fiecărei dimensiuni în Figura 3.1.

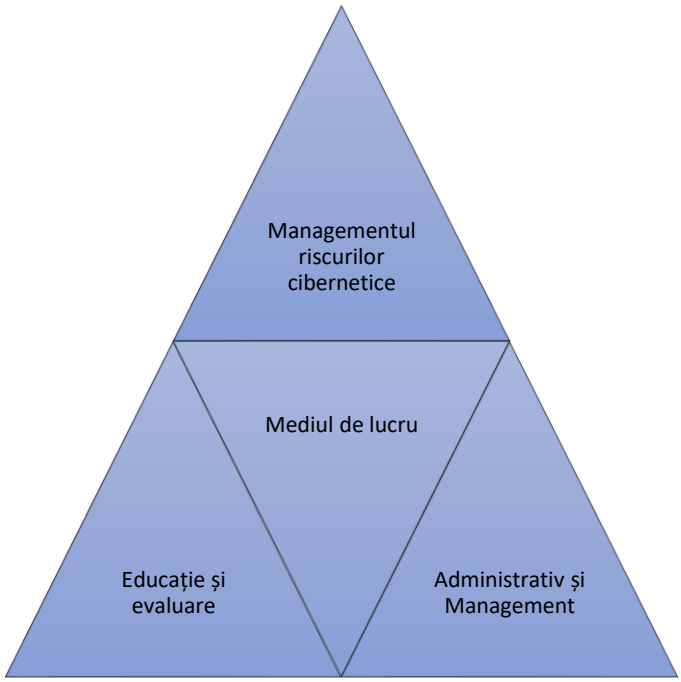

Fig. 3.1. Conexiunea și importanța dimensiunilor modelului

Cerințele pentru educație și evaluare, precum și dimensiunea administrativă și de management stau la baza asigurării unui mediu adecvat dezvoltării culturii de securitate cibernetică. Aceste două dimensiuni asigură un mediu adecvat de lucru, care este trivial pentru un management eficient al riscurilor cibernetice. În baza analizei se observă că asigurarea securității cibernetice este un proces continuu într-o muncă în echipă. Aceasta reiterează importanța pe care dimensiunea umană o are în toate etapele securității cibernetice în toate domeniile, în special în cel al IC.

În plus, analiza comparativă cu seria de standarde ISO 27000 [36] arată că atributele selectate pot fi utilizate și în sprijinul evaluărilor de guvernanță, deoarece acestea pot caracteriza managementul general al securității cibernetice în organizație. Acest lucru crește rata de eficiență și potențialele cazuri de utilizare în care acest model poate fi aplicat. Indirect, aceasta înseamnă și că modelul este aliniat cu seria NIST 800-53, precum și cu alte recomandări privind subiectele de securitate informatică din domeniul nuclear, cum ar fi cele de la AIEA [32, 33, 34].

Modelul propus este personalizat pentru domeniul IC, totuși poate fi utilizat ca referință pentru alte tipuri de sisteme informatice sau domenii. Modelul complet cu toate dimensiunile și atributele poate fi vizualizat în Tabelul 3.1. Modelul include atributele referitoare elementelor

factorului uman, care au fost identificate în Capitolul 2 [91, 143]. A fost inclus de asemenea ca atribut și Modelul de Acceptare Tehnologică, care este util pentru scopul acestui model și este recomandat de a fi inclus ca parte a altor modele sau sisteme de evaluare [144, 113, 118].

Modelul conține cinci niveluri de maturitate pentru a evalua procesul de management al riscurilor cibernetice, care cuprinde atât criterii de dimensiune tehnologică, cât și de dimensiune umană. Nivelurile variază de la „*Foarte înalt*" la „*Foarte scăzut*". Nivelul „*Foarte înalt*" corespunde celor mai mari valori pentru toate criteriile, începând cu nivelul administrativ și management, până la conștientizarea securității cibernetice și utilizarea sistemelor informaționale. Adițional, este propus un sistem de punctare care va ajuta utilizatorii acestui model să evalueze maturitatea securității cibernetice, în conformitate cu procesele operaționale dintr-o organizație IC.

Tabelul 3.1. Modelul de maturitate a securității cibernetice

Definirea categoriei și a atributelor pentru fiecare dintre nivelurile de maturitate de securitate cibernetică	**Sistemul de notare propus**
Foarte înalt	
Criterii administrative si de management:	
Cerințele pentru securitatea cibernetică și reziliență sunt luate în considerare încă din faza de proiectare și evaluare a sistemului și sunt recunoscute ca o combinație de tehnologie și dimensiune umană.	5
În procesul decizional, securitatea cibernetică și factorul de reziliență au o pondere mai mare în comparație cu costurile.	5
Responsabilitățile pentru securitatea cibernetică sunt clare și bine definite în funcție de structura și funcțiile respective. Procesul de schimb de informații este bine stabilit pe verticală și pe orizontală, inclusiv pe plan extern.	5
Funcțiile de management și monitorizare sunt stabilite și au un rol major în procesul decizional.	5
Criterii de educație și de evaluare:	
Sunt stabilite și revizuite programe regulate de formare pe baza bunelor practici existente în domeniu. Formarea se bazează pe performanță și conține evaluări.	5
Programul de formare ia în considerare dimensiunea umană. Instruirea utilizatorilor finali ai sistemului informatic este obligatorie.	5
Procedurile și cerințele se aplică tuturor rolurilor din cadrul organizației. Evaluarea ia în considerare impactul real și riscul acestui factor.	5
Respectarea indicatorilor bazați pe performanță este obligatorie pentru îndeplinirea sarcinilor operaționale.	5
Criterii de mediu de lucru :	
Mediul de lucru și politicile sunt prietenoase cu personalul; feedback-ul este pozitiv.	5
Tot personalul înțelege impactul amenințărilor cibernetice, al vectorilor de atac și al vulnerabilităților sistemului și este capabil să implementeze atenuarea și prevenirea necesare în funcție de rol.	5
Gradul de confort social al lucrătorilor este considerat un factor important.	5
Criterii de management al riscurilor cibernetice:	
Managementul riscurilor cibernetice este bine definit pe cele mai bune practici și integrat cu managementul riscurilor organizațional. Riscurile cibernetice sunt gestionate atât din perspectiva dimensiunii tehnologice, cât și a dimensiunii umane.	5

Riscurile cibernetice sunt înțelese și recunoscute de la conducerea superioară / factorii de decizie / indivizi.	5
Formările și exercițiile sunt activități comune și acoperă scenarii din viața reală.	5
Sistemele informatice sunt utilizate pentru sarcini operaționale, acolo unde este posibil. Personalul este proactiv în furnizarea de *feedback* și îmbunătățirea funcționalității utilizării sistemelor informaționale.	5
SSD este utilizat pentru sarcini critice; automatizarea sarcinilor este implementată pe cât posibil; rolurile de supraveghere sunt repartizate corespunzător funcției ocupate.	5
Modelul de evaluare a tehnologiei (TAM) are indicatori foarte înalți	5
Scorul total mediu:	**5,0p (100%)**
Înalt	
Criterii administrative si de management:	
Cerințele pentru securitatea cibernetică și reziliența sunt moștenite din politicile sau reglementările organizaționale/naționale și sunt recunoscute ca o combinație de tehnologie și dimensiune umană.	5
Factorul de cost are o influență minoră asupra luării deciziilor, uneori poate avea aceeași pondere față de cerințele funcționale.	4
Există o funcție responsabilă de securitatea cibernetică. Schimbul de informații poate avea loc atât pe verticală, cât și pe orizontală, dar și cu părți externe.	5
Funcțiile de management și monitorizare sunt stabilite, însă nu au un rol în procesul decizional. Această responsabilitate revine personalului administrativ superior.	4
Criterii de educație și de evaluare:	
Sunt stabilite programe regulate de instruire și acoperă majoritatea proceselor organizației. Antrenamentul se bazează pe performanță și conține evaluări.	5
Programul de formare ia în considerare dimensiunea umană. Instruirea utilizatorilor finali ai sistemului informatic este obligatorie	5
Procedurile și cerințele se aplică majorității organizației numai obligatorii pentru rolurile cu risc ridicat. Evaluarea ia în considerare impactul real și riscul acestui factor.	4
Indicatorii minimi bazați pe performanță sunt definiți pentru a îndeplini sarcinile operaționale.	4
Criterii de mediu de lucru:	
Mediul de lucru și politicile sunt orientate spre minimizarea majorității impactului negativ al potențialilor factori umani.	4
Impactul potențial al amenințărilor cibernetice asupra tehnologiilor operaționale este înțeles de către întreaga organizație, totuși există un decalaj în recunoașterea autoeficacității în descurajarea și prevenirea acestora.	4
Gradul de confort social al lucrătorilor este luat în considerare în timpul dezvoltării politicii	4
Criterii de management al riscurilor cibernetice:	
Managementul riscurilor cibernetice este bine definit și integrat cu managementul riscurilor organizațional. Riscurile cibernetice sunt gestionate atât din perspectiva dimensiunii tehnologice, cât și a dimensiunii umane.	5
Riscurile cibernetice sunt înțelese și recunoscute de managementul superior / factorii de decizie și de majoritatea operatorilor. Riscurile identificate cu impact sporit, sunt gestionate în mod adecvat și în timp util.	4
Sunt definite și instituționalizate programe de formare și exerciții.	4
SSD sunt utilizate în sarcini critice acolo unde este posibil. Automatizarea este parțial utilizată. Există o mare dependență de sistemele informaționale pentru procesele operaționale.	4
Modelul de evaluare a tehnologiei are indicatori înalți.	4
Scorul total mediu:	**4,31p (86%)**
Mediu	
Criterii administrative si de management :	

Cerințele pentru securitatea cibernetică și reziliența sunt considerate de conducerea superioară ca fiind legate de tehnologie.	3
Factorul cost poate avea o pondere mai mare în comparație cu cerințele funcționale	3
Procesul de schimb de informații este stabilit oficial pe verticală și pe orizontală, totuși nefiind utilizat la maxim. Comunicarea externă este formalizată, dar nu este pe deplin valorificată.	3
Criterii de educație și de evaluare:	
Sunt stabilite programe regulate de formare pentru toți utilizatorii. Acestea includ aspecte formale și generale legate de procesele organizaționale.	3
Programul de formare ia în considerare doar anumite elemente ale factorului uman. Instruirea pentru utilizatorii finali ai sistemului informatic este opțională.	3
Procedurile și cerințele se aplică în mod selectiv rolurilor bazate pe profilul de risc. Evaluarea este în corespondență cu rolurile selective.	3
Indicatorii minimi pentru îndeplinirea sarcinilor operaționale sunt legați de finalizarea programelor de formare sau dezvoltare, cu toate acestea programele de formare sunt percepute de toți ca o povară.	3
Criterii de mediu de lucru :	
Mediul de lucru și politicile minimizează singurul impact negativ major al potențialilor factori umani.	3
Impactul potențial al amenințărilor cibernetice asupra tehnologiilor operaționale este parțial recunoscut.	3
Gradul de confort social al lucrătorilor este considerat un factor parțial important, astfel feedback-ul este satisfăcător.	3
Criterii de management al riscurilor cibernetice:	
Managementul incidentelor, monitorizarea și instrumentarea sunt orientate spre respectarea bunelor practici și standard.	3
Tratamentul riscului se concentrează în principal pe riscuri mari și este adesea văzut ca o îmbunătățire tehnologică. Impactul potențial al riscurilor cibernetice este parțial recunoscut în organizație.	3
Programele de formare și exercițiile sunt periodic definite și instituționalizate.	3
SSD sunt utilizate numai de anumiți utilizatori și pentru majoritatea sarcinilor critice; majoritatea necesităților sunt acoperite de SSD, dar performanța și beneficiile sale sunt considerate medii.	3
Modelul de evaluare a tehnologiei are indicatori medii	3
Scorul total mediu:	**3,0p (60%)**
Scăzut	
Criterii administrative si de management:	
Cerințele de securitate cibernetică și rezistență sunt moștenite din reglementări din afara organizației, dar nu sunt luate în considerare în întregime în tehnologie și nici în organizație. Principalii factori de rezistență sunt legați doar de siguranța IC. Nu există nimeni responsabil pentru securitatea cibernetică	2
Costurile reprezintă factori conducători în luarea deciziilor, adesea în dezavantajul cerințelor funcționale.	3
Criterii de educație și de evaluare:	
Formarea pentru utilizatorii finali ai sistemului informatic este considerată necesară doar pentru roluri tehnice limitate.	2
Sunt definite strategii generice și programe generale de instruire, care conțin și un aspect de securitate cibernetică.	2
Procedurile și cerințele se aplică în mod selectiv rolurilor bazate pe profilul de risc, cu toate acestea, importanța și impactul benefic al formării nu sunt recunoscute. Evaluarea este formală și nu ia în considerare impactul și riscul real.	2
Criterii de mediu de lucru:	
Mediul de lucru și politicile sunt în vigoare în mod oficial și sunt considerate selective ca rezultat al incidentului în rândul personalului.	2

Impactul potențial al amenințărilor cibernetice asupra tehnologiilor operaționale nu este recunoscut. Cultura securității cibernetice este evaluată limitat în termeni de necesități operaționale.	2
Gradul de confort social al lucrătorilor nu este considerat un factor important. Feedback-ul este sub medie.	2
Criterii de management al riscurilor cibernetice:	
Incidentele sunt identificate de operatori și gestionate prin proceduri ad-hoc.	2
Riscurile cibernetice sunt recunoscute, cu toate acestea, suportul necesar este oferit doar sub presiunea circumstanțelor.	2
Programe de formare și exerciții sunt organizate ocazional. Nu există acțiuni sau strategii planificate pentru a minimiza riscurile potențiale.	2
SSD sunt utilizate pentru sarcini de bază; în timp ce anumite cazuri de utilizare sunt implementate – doar unele sunt utilizate; beneficiile IS sunt văzute ca fiind reduse.	2
Modelul de evaluare a tehnologiei are indicatori scăzuți.	2
Scorul total mediu:	**2,08p (41,6%)**
Foarte scăzut	
Criterii administrative si de management :	
Factorii de decizie nu recunosc importanța securității cibernetice și a rezistenței sistemelor informaționale. Aceste cerințe sunt percepute din toate punctele de vedere ca o povară asupra procesului tehnologic de bază. Importanța acestor criterii este de obicei acordată temporar, după ce a avut loc deja un incident. Nu există nimeni responsabil pentru securitatea cibernetică.	1
Criterii de educație și de evaluare:	
Programul de formare este formalizat la maximum, adesea exclusiv prin rapoarte și înregistrări fără sesiuni live.	2
Valoarea antrenamentului și a exercițiilor nu este recunoscută și este considerată o povară. Formarea este văzută în principal ca o cerință de conformitate. Formarea nu acoperă evaluări.	1
Criterii de mediu de lucru:	
Mediul de lucru și politicile nu sunt nici măcar luate în considerare și adoptate oficial.	1
Importanța securității cibernetice pentru sistemele operaționale este înțeleasă doar de unii indivizi. Acest fapt nu este raportat, nici escaladat.	1
Evaluarea feedback-ului este fie lipsă, fie neconcludentă, deoarece se bazează pe evaluări care nu sunt adaptate contextului.	1
Criterii de management al riscurilor cibernetice:	
Incidentele sunt elucidate cel mai adesea de către entități externe, urmate de o gestionare a procedurilor operaționale ocazionale.	1
Nu există programe de antrenament, exerciții sau proceduri aprobate pentru a minimiza riscurile potențiale.	1
Beneficiile utilizării unui SSD nu sunt recunoscute.	1
Modelul de evaluare a tehnologiei are indicatori foarte scăzuți.	1
Scorul mediu total:	**1,11p (22,2 %)**

Nivelurile de maturitate a securității cibernetice pot fi măsurate într-o manieră mai subiectivă sau obiectivă. De exemplu, dacă scorul este de cel puțin 80%, atunci maturitatea securității cibernetice este considerată foarte mare. Organizația trebuie fie să mențină și să ajusteze controalele existente în toate dimensiunile, fie să avanseze evaluarea prin introducerea unor atribute noi specifice domeniului. Scopul acțiunilor, în conformitate cu modelul, sunt fie de a ameliora tehnologiile sau elementele factorului uman.

Pentru scoruri între 60-80% se poate presupune că controalele interne generale sunt eficiente, însă acestea necesită îmbunătățiri. De asemenea, pe baza riscurilor, necesităților și cerințelor, organizațiile pot încerca să avanseze maturitatea într-un interval de timp specific.

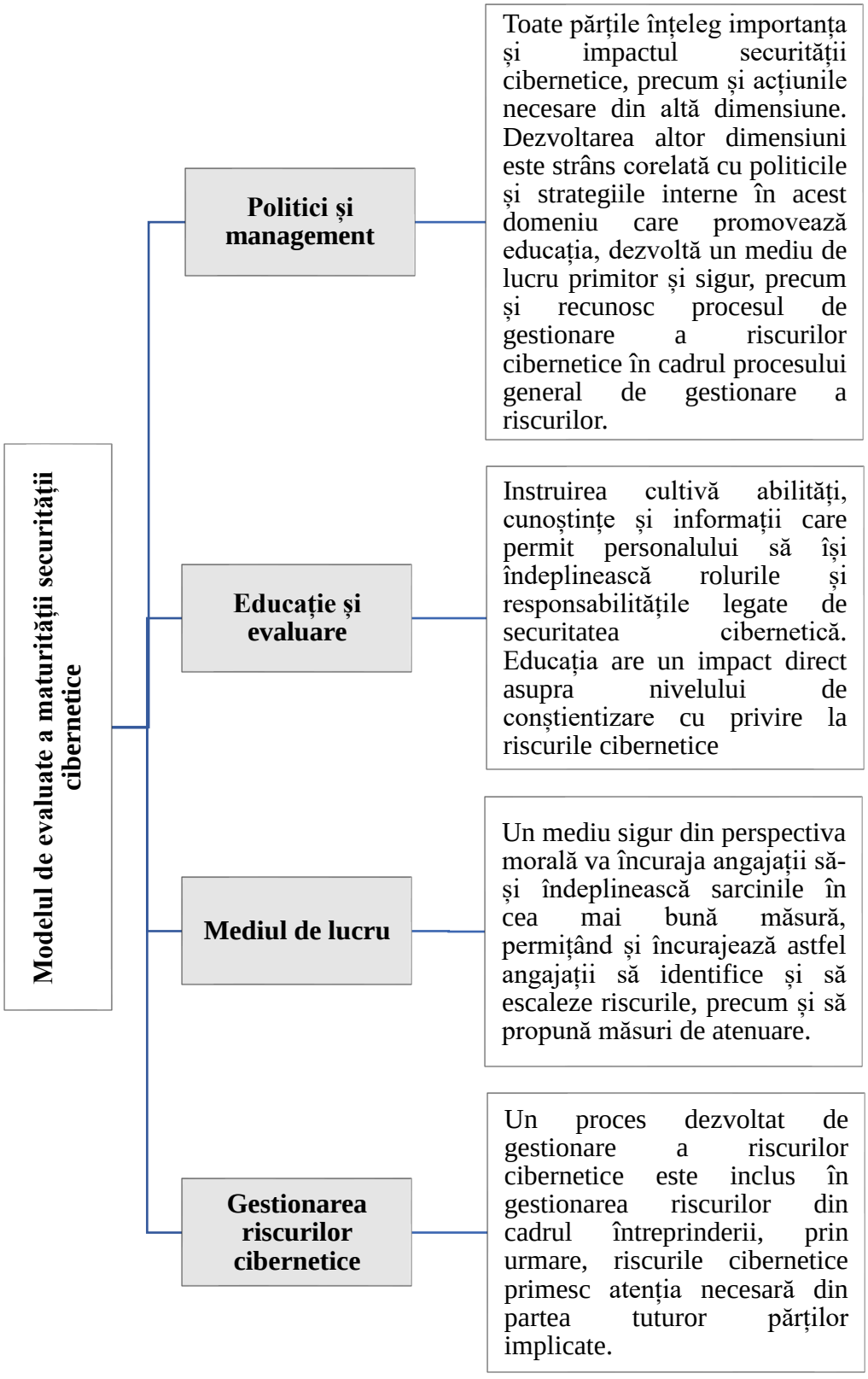

Fig. 3.2. Interdependența dimensiunilor securității cibernetice

Dacă o organizație obține un scor între 40-60% atunci este necesar de evaluat fiece dimensiune conform cerințelor privind nivelul de maturitate cerut. În domeniul IC, cerințele de siguranță și securitate sunt mai stricte decât în alte domenii, iar fiecare organizație trebuie să își adapteze obiectivele de securitate în funcție de apetitul pentru risc, resursele financiare și peisajul general al amenințărilor. Pentru scoruri sub 40% organizațiile din domeniul IC trebuie să implementeze un plan de remediere pentru dimensiunile care au un scor critic scăzut. Acest lucru va asigura că există toate premisele pentru a crește maturitatea securității. În plus, pot fi urmate recomandări din subcapitolul 3.4 pentru a înțelege mai bine dinamica dimensiunilor modelului în procesul de dezvoltare a programului de securitate cibernetică. Figura 3.2 descrie impactul dimensiunilor asupra maturității securității cibernetice a unei organizații.

Acțiunile și efectele aferente sunt reflectate din perspectivă organizațională. Aceste dimensiuni au un rol direct asupra maturității securității cibernetice. Totuși, în contextul evaluării eficienței unui SSD pentru managementul riscurilor cibernetice, rezultatele pot fi corelate sau comparate cu potențialele acțiuni în creșterea maturității securității cibernetice din perspectivă organizațională, pentru a beneficia de un rezultat maxim.

3.1.3. Sistemul formal metric inteligent ce implementează modelul

În această secțiune este propus un sistem formal metric inteligent de evaluare a maturității securității cibernetice a infrastructurilor critice, ce reprezintă o premieră în acest domeniu. Sistemul formal metric inteligent reprezintă un instrument efectiv care poate asista beneficiarii la obținerea soluțiilor la întrebările respective. Acest sistem transpune elementele din modelul propus în domeniile conexe infrastructurilor critice ce utilizează sisteme informaționale. Sistemul propus permite evaluarea impactului pozitiv al utilizării sistemelor informatice în diverse domenii, cât și aspectele ce pot genera riscuri. Mai jos este propusă o logică a modelelor de evaluare a maturității securității cibernetice a infrastructurilor critice.

Dumitrescu D. definește conceptele *sistem formal*, *deducție*, *teoremă* și *demonstrație* în felul următor [165]:

Definiția 1: Un **sistem formal** S este o structură $S = (\Sigma, F_s, A_s, R_s)$, ale cărei elemente au următoarea semnificație:

(i) Σ este un alfabet (finit sau nu);

(ii) F_s este mulțimea *formulelor bine formate* din S;

(iii) F_s este o submulțime a mulțimii șirurilor finite formate cu elementele alfabetului și se defineşte recursiv;

(iv) A_s reprezintă mulțimea *axiomelor* sistemului;

(v) A_s este o submulțime a lui F_s;

(vi) R_s este o mulțime de predicate decidabile definite peste F_s. R_s formează *regulile de inferență*.

Observație: Fie $r \in R_s$. În locul notației $r(f_1, f_2, ..., f_n, g)$ se utilizează notația $f_1, f_2, ..., f_n \vdash g$, care se citește „formula g se poate deduce din formulele $f_1, f_2, ..., f_n$ și regula r”.

Definiția 2: Fie $A_1, A_2,..., A_p$ și $B_1, B_2, ..., B_n$ două mulțimi de formule. Spunem că $B_1, B_2, ..., B_n$ este o *deducție* B_n plecând de la ipotezele $A_1, A_2, ..., A_p$ și se notează $A_1, A_2, ..., A_p, ..., B_n$ dacă și numai dacă pentru orice $i \in \{1, 2, ..., n\}$ avem una din următoarele situații:

(i) B_i este o axiomă a sistemului S.

(ii) B_i este una din formulele $A_1, A_2, ..., A_p$.

(iii) B_i este obținută prin aplicarea unei reguli $r_k \in R_s$ unor formule $B_{i(1)}, ..., B_{i(e)}$, ce preced pe B_i, adică $i(1), ..., i(e) < 1$.

Observație: $B_1, B_2, ..., B_n$ se mai numește *o deducție* pornind de la $A_1, A_2, ..., A_p$.

Definiția 3: Se numește *teoremă* a lui $\boldsymbol{S}$ orice formulă $\boldsymbol{A}$ pentru care există o deducție pornind de la o mulțime vidă de formule. O astfel de deducție se numește o *demonstrație* a lui $\boldsymbol{A}$.

Următoarele definiții se referă la contextul tezei. Noțiunea de *infrastructură critică* nu beneficiază de o definiție precisă și unică. Prin urmare, poate diferi în funcție de țară. Termenii asociați cel mai frecvent cu această noțiune acoperă (adaptat după [13, 14, 15]):

- Producția, transportul și distribuția de energie electrică;
- Producția, transportul și distribuția gazelor;
- Producția de petrol și produse petroliere, transport și distribuție;
- Telecomunicațiile;
- Alimentarea cu apă (apă potabilă, apă uzată, apă de suprafață);
- Agricultura, producția și distribuția de alimente;
- Încălzirea (de exemplu, gaze naturale, păcură, încălzire urbană);
- Sănătatea publică (spitale, ambulanțe);
- Sistemele de transport (alimentarea cu combustibil, rețeaua feroviară, aeroporturi, porturi, navigație interioară);
- Serviciile financiare (servicii bancare, compensare);
- Serviciile de securitate (poliție, armată).
- Servicii din sectorul de urgențe (medicale, materiale periculoase, centru de apel de urgențe e.g. 9-1-1, echipe tactice e.g. SWAT, etc.);

- Sectorul nuclear, materiale și deșeuri (CAE, Reactoare nucleare de cercetare, materiale nucleare în medii medicale, industriale, academice, transportare, depozitare, procesare și eliminare deșeuri NR).

Definiție 4. *Securitatea cibernetică* reprezintă un proces continuu ce implică diferite procedee cu scopul final de a proteja activele valoroase din spațiul cibernetic. Între acestea se pot număra datele cu caracter personal personale, date confidențiale, sisteme critice financiare și altele.

Definiție 5. *Maturitatea securității cibernetice a infrastructurilor critice* reprezintă un indicator important care demonstrează gradul de imunitate la riscurile cibernetice. Cu cât gradul maturității este mai mare, vulnerabilitatea infrastructurii critice este mai mică.

Determinarea *Nivelului de maturitate al securității cibernetice* și a *nivelului riscurilor cibernetice în infrastructurile critice* se face cu ajutorul chestionarului de evaluare corespunzător, prezentat în Anexa 1.

Chestionarul sub formă de tabel reprezintă totodată și:

a) Interfața aplicației inteligente.
b) Baza de cunoștințe a Sistemului formal metric inteligent „Securitatea cibernetică în infrastructurile critice" și a aplicației inteligente corespunzătoare.

Construirea *sistemului formal pentru Evaluarea Maturității Securității Cibernetice a infrastructurilor critice* (în continuare S_{EMSC}) se poate face adaptând definiția conceptului *sistem formal* la domeniul de cercetare.

Conform **Definiției 1.** *S* reprezintă o structură $S = (\Sigma, F_s, A_s, R_s)$, ale cărei elemente au următoarea semnificație:

(i) Σ - alfabetul $\boldsymbol{S_{EMSC}}$,

$\Sigma =$ ***Input*** U ***Internal*** U ***Output***, unde:

- ***Input*** - mulțimea elementelor de intrare ale sistemului S_{EMSC}

$\boldsymbol{Input} = \{\boldsymbol{O}, \boldsymbol{E_{1,1}}, \boldsymbol{E_{1,2}}, \boldsymbol{E_{1,3}}, \boldsymbol{E_{1,4}}, \boldsymbol{E_1}, \boldsymbol{E_{2,1}}, \boldsymbol{E_{2,2}}, \boldsymbol{E_{2,3}}, \boldsymbol{E_{2,4}}, \boldsymbol{E_2}, \boldsymbol{E_{3,1}}, \boldsymbol{E_{3,2}}, \boldsymbol{E_{3,3}}, \boldsymbol{E_3}, \boldsymbol{E_{4,1}}, \boldsymbol{E_{4,2}}, \boldsymbol{E_{4,3}}, \boldsymbol{E_{4,4}}, \boldsymbol{E_{4,5}}, \boldsymbol{E_4}, \boldsymbol{E}\}$;

- ***Internal*** $= \{\boldsymbol{e_{1,1}}, \boldsymbol{e_{1,2}}, \boldsymbol{e_{1,3}}, \boldsymbol{e_{1,4}}, \boldsymbol{e_1}, \boldsymbol{e_{2,1}}, \boldsymbol{e_{2,2}}, \boldsymbol{e_{2,3}}, \boldsymbol{e_{2,4}}, \boldsymbol{e_2}, \boldsymbol{e_{3,1}}, \boldsymbol{e_{3,2}}, \boldsymbol{e_{3,3}}, \boldsymbol{e_3}, \boldsymbol{e_{4,1}}, \boldsymbol{e_{4,2}}, \boldsymbol{e_{4,3}}, \boldsymbol{e_{4,4}}, \boldsymbol{e_{4,5}}, \boldsymbol{e_4}, \boldsymbol{e}\}$;
- ***Output*** - mulțimea elementelor de ieșire ale sistemului $S_{EMSC,}$

$\boldsymbol{Output} \in \{$**„Nivelul de maturitate „*Foarte înalt*""**,
„Nivelul de maturitate „*Înalt*"",

„Nivelul de maturitate „*Mediu*””,

„Nivelul de maturitate „*Scăzut*””,

„Nivelul de maturitate „*Foarte scăzut*””,

„Nivelul riscurilor cibernetice „*Foarte jos*””,

„Nivelul riscurilor cibernetice „*Scăzut*””,

„Nivelul riscurilor cibernetice „*În mediu*””,

„Nivelul riscurilor cibernetice „*Înalt*””,

„Nivelul riscurilor cibernetice „*Foarte înalt*””};

(ii) F_s este mulțimea *formulelor bine formate* din *S*.

$\boldsymbol{N_{MA}(o)} \in$ {**„Nivelul de maturitate „*Foarte înalt*””,**

„Nivelul de maturitate „*Înalt*””,

„Nivelul de maturitate „*Mediu*””,

„Nivelul de maturitate „*Scăzut*””,

„Nivelul de maturitate „*Foarte scăzut*””};

$\boldsymbol{N_{RC}(o)} \in$ {**„Nivelul riscurilor cibernetice „*Foarte jos*””,**

„Nivelul riscurilor cibernetice „*Scăzut*””,

„Nivelul riscurilor cibernetice „*În mediu*””,

„Nivelul riscurilor cibernetice „*Înalt*””,

„Nivelul riscurilor cibernetice „*Foarte înalt*””};

$\boldsymbol{E_{i,j}(o)} = \boldsymbol{e_{i,j}}$; $\boldsymbol{e_{i,j}} \in \{0, 1, 2, 3, 4, 5\}$;

$\boldsymbol{E_i(o)} = \sum \boldsymbol{E_{i,j}(o)}$; $\boldsymbol{E_i(o)} = \boldsymbol{e_i}$;

$\boldsymbol{E(o)} = \sum \boldsymbol{E_i(o)}$; $\boldsymbol{E} = \boldsymbol{(o)} = \boldsymbol{e}$ unde: $i = 1, ..., 4$; $j = 1, ..., j_i$; $j_1 = 4$; $j_2 = 4$; $j_3 = 3$; $j_4 = 5$.

(iii) A_s reprezintă mulţimea *axiomelor* sistemului:

$$A_s = \{\boldsymbol{O}, \boldsymbol{E_{i,j}(o)} = \boldsymbol{e_{i,j}}; \boldsymbol{E_i(o)} = \boldsymbol{e_i}; \boldsymbol{E(o)} = \boldsymbol{e}\},$$

(iv) A_s este o submulțime a lui F_s;

R_s este o mulțime de predicate decidabile definite peste F_s.

R_s integrează *regulile de inferență*:

a) $\mathbf{R_1}$**:** $\mathbf{E}_{i,j}(\boldsymbol{o}) = \boldsymbol{e_{i,j}}$;

b) $\mathbf{R_2}$**:** $\boldsymbol{e_i} = \sum \boldsymbol{E_{i,j}(o)}$; $\boldsymbol{E_i(o)} = \boldsymbol{e_i}$;

c) $\mathbf{R_3}$**:** $\boldsymbol{e} = \sum \boldsymbol{E_i(o)}$; $\boldsymbol{E(o)} = \boldsymbol{e}$;

unde:

$\boldsymbol{o} \in \boldsymbol{O}$;

$\boldsymbol{O}$ – mulțimea universală a infrastructurilor critice;

$e_{i,j} \in \{0, 1, 2, 3, 4, 5\}$; $i = 1, ..., 4$; $j = 1, ..., j_i$; $j_1 = 4$; $j_2 = 4$; $j_3 = 3$; $j_4 = 5$.

R4: If $E(o) = 80$ **THEN**

$N_{MA}(o)$ = „**Nivelul de maturitate „*Foarte înalt*”**”;

$N_{RC}(o)$ = „**Nivelul riscurilor cibernetice „*Foarte jos*”**”.

R5: IF $(E(o) \geq 69)$ & $(E_{1,2}(o) \geq 4)$ & $(E_{1,4}(o) \geq 4)$ & $(E_{2,3}(o) \geq 4)$ & $(E_{2,4}(o) \geq 4)$ & $(E_{3,1}(o) \geq 4)$ & $(E_{3,2}(o) \geq 4)$ & $(E_{3,3}(o) \geq 4)$ & $(E_{4,2}(o) \geq 4)$ & $(E_{4,3}(o) \geq 4)$ & $(E_{4,4}(o) \geq 4)$ & $(E_{4,5}(o) \geq 4)$

THEN DO

$N_{MA}(o)$ = „**Nivelul de maturitate „*Înalt*”**”;

$N_{RC}(o)$ = „**Nivelul riscurilor cibernetice „*Scăzut*”**”

END.

R6: IF $(E(o) \geq 48)$ & $(E_{1,1}(o) \geq 3)$ & $(E_{1,2}(o) \geq 3)$ & $(E_{1,3}(o) \geq 3)$ & $(E_{1,4}(o) \geq 3)$ & $(E_{2,1}(o) \geq 3)$ & $(E_{2,2}(o) \geq 3)$ & $(E_{2,3}(o) \geq 3)$ & $(E_{2,4}(o) \geq 3)$ & $(E_{3,1}(o) \geq 3)$ & $(E_{3,2}(o) \geq 3)$ & $(E_{3,3}(o) \geq 3)$ & $(E_{4,1}(o) \geq 3)$ & $(E_{4,2}(o) \geq 3)$ & $(E_{4,3}(o) \geq 4)$ & $(E_{4,4}(o) \geq 3)$ & $(E_{4,5}(o) \geq 3)$

THEN DO

$N_{MA}(o)$ = **„Nivelul de maturitate „*Mediu*””**;

$N_{RC}(o)$ = **„Nivelul riscurilor cibernetice „*În mediu*””**

END.

R7: IF $(E(o) \geq 27)$ & $(E_{1,1}(o) \geq 2)$ & $(E_{1,2}(o) \geq 3)$ & $(E_{1,3}(o) \geq 0)$ & $(E_{1,4}(o) \geq 0)$ & $(E_{2,1}(o) \geq 2)$ & $(E_{2,2}(o) \geq 2)$ & $(E_{2,3}(o) \geq 2)$ & $(E_{2,4}(o) \geq 0)$ & $(E_{3,1}(o) \geq 2)$ & $(E_{3,2}(o) \geq 2)$ & $(E_{3,3}(o) \geq 2)$ & $(E_{4,1}(o) \geq 2)$ & $(E_{4,2}(o) \geq 2)$ & $(E_{4,3}(o) \geq 2)$ & $(E_{4,4}(o) \geq 2)$ & $(E_{4,5}(o) \geq 2)$

THEN DO

$N_{MA}(o)$ = **„Nivelul de maturitate „*Scăzut*””**;

$N_{RC}(o)$ = **„Nivelul riscurilor cibernetice „*Înalt*””**

END.

R8: ELSE DO

$N_{MA}(o)$ = **„Nivelul de maturitate „*Foarte scăzut*””**;

$N_{RC}(o)$ = **„Nivelul riscurilor cibernetice „*Foarte înalt*””**

END.

Definiție (a vedea [166]). **Spațiu metric** este un cuplu (***X,*** *d*). unde ***X*** este o mulțime nevidă. ale cărei elemente se numesc puncte ale spațiului. Iar

$$d: X \times X \to R_+$$

o aplicație numită *funcție-distanță* sau *metrică a spațiului* cu proprietățile:

$d(x, y) \geq 0$, $\forall x, y \in X$, numai și numai dacă, $x = y$

$d(x, y) = d(y, x)$, $\forall x, y \in X$ (simetrie)

$d(x, y) \leq d(x, z) + d(z, y)$, $\forall x, y \in X$ (inegalitatea triunghiulară)

Fie $\boldsymbol{O_1}$ și $\boldsymbol{O_2}$ - două infrastructuri critice.

Construim spațiile metrice:

R9: $\boldsymbol{D_{1,1}, D_{1,2}, D_{1,3}, D_{1,4}, D_1, D_{2,1}, D_{2,2}, D_{2,3}, D_{2,4}, D_2, D_{3,1}, D_{3,2}, D_{3,3}, D_3, D_{4,1}, D_{4,2}, D_{4,3}, D_{4,4}, D_{4,5}, D_4, D}$.

Metricile spațiilor le definim în modul următor:

a) Pentru spațiile $\boldsymbol{D_{i,j}}$: $d_{i,j}(\boldsymbol{o_1}, \boldsymbol{o_2}) = abs(\boldsymbol{E_{i,j}}(\boldsymbol{o_1}) - \boldsymbol{E_{i,j}}(\boldsymbol{o_2}))$, $\boldsymbol{o_1}, \boldsymbol{o_2} \in \boldsymbol{O}$,

$i = 1, ..., 4$; $j = 1, ..., j_i$; $j_1 = 4$; $j_2 = 4$; $j_3 = 3$; $j_4 = 5$.

b) Pentru spațiile $\boldsymbol{D_i}$: $d_i(\boldsymbol{o_1}, \boldsymbol{o_2}) = abs(\boldsymbol{E_i}(\boldsymbol{o_1}) - \boldsymbol{E_i}(\boldsymbol{o_2}))$, $i = 1, ..., 4$, $\boldsymbol{o_1}, \boldsymbol{o_2} \in \boldsymbol{O}$.

c) Pentru spațiul $\boldsymbol{D}$: $d(\boldsymbol{o_1}, \boldsymbol{o_2}) = abs(\boldsymbol{E}(\boldsymbol{o_1}) - \boldsymbol{E}(\boldsymbol{o_2}))$, unde $\boldsymbol{o_1}, \boldsymbol{o_2} \in \boldsymbol{O}$.

Spațiile metrice elaborate pot fi utilizate pentru evaluarea gradului maturității securității cibernetice și a nivelului riscurilor cibernetice a infrastructurilor critice pentru:

- măsurarea maturității securității cibernetice și a nivelului riscurilor cibernetice a infrastructurilor critice a unei infrastructuri;
- compararea maturității securității cibernetice și a nivelului riscurilor cibernetice a infrastructurilor critice a două infrastructuri;
- elaborarea clasamentelor maturității securității cibernetice și a nivelului riscurilor cibernetice a infrastructurilor critice a două infrastructuri, a unei liste de infrastructuri, a infrastructurilor critice dintr-o țară, regiune sau de pe întreg mapamondul;
- unul sau mai mulți indicatori de evaluare a maturității securității cibernetice și a nivelului riscurilor cibernetice a infrastructurilor critice sau toți 16 indicatorii;
- o grupă sau mai multe de indicatori de evaluare a maturității securității cibernetice și a nivelului riscurilor cibernetice a infrastructurilor critice.

De asemenea, un drept de autor a fost înregistrat la AGEPI privind sistemul formal metric inteligent „Securitatea cibernetică în infrastructuri critice” (Seria 0, Nr. 7305 din 04.08.2022) [189].

3.1.4. Conceptul de aplicație TI ce implementează modelul

În această secțiune este prezentat un prototip (programul sursă) pentru operaționalizarea sistemului formal inteligent de evaluarea a maturității securității cibernetice (Anexa 7). Programul implementează funcționalitatea de bază pentru procesul de evaluare prin modelul propus și a bazei de cunoștințe dezvoltate [190]. Aplicația este extensibilă și poate fi integrată și ajustată la necesitățile oricărei organizații. Pe lângă concept, aceasta aplicație poate ajuta la integrarea modelului sau sistemului formal în orice tip de organizație, deoarece automatizează procesul de evaluare și facilitează revizuirea rezultatelor finale.

Limbajul de programare utilizat este *Python*, datorită versatilității precum și bibliotecilor disponibile. Acest lucru îmbunătățește evaluarea și adaptarea codului, precum și utilizarea unui limbaj bine cunoscut în TI. Programul conține o clasă numită *Model*, care acoperă implementarea modelului, și o clasă numită UserInterface, responsabilă pentru interfața generală și interacțiunea cu utilizatorul final, cum ar fi crearea de meniuri, vizualizarea și introducerea datelor. În *Python*, clasele oferă o modalitate ușoară de a combina datele, funcționalitățile și metodele, prin urmare această soluție poate fi ușor înțeleasă și adaptată după cum este necesar. După instanțiere, clasele pot fi utilizate pe tot parcursul programului. Deoarece cercetarea s-a axat pe modularitate și interoperabilitate, s-a decis că această abordare este cea mai bună soluție pentru acest obiectiv.

Programul utilizează ca bază de cunoștințe un fișier cu valori separate prin virgulă, care conține date despre atributele modelului. Un extras al fișierului și al conținutului acestuia este reprezentat în Tabelul 3.2.

Tabelul 3.2. Conținutul bazei de cunoștințe - exemplu

Nivel	**Criterii**	**Element**	**Atribut**
Foarte înalt	*pol_adm*	1	Cerințele de securitate cibernetică și reziliență sunt luate în considerare în faza de proiectare și evaluare a sistemului și sunt recunoscute ca o combinație între tehnologie și dimensiunea umană.
Foarte înalt	*pol_adm*	2	În procesul decizional, securitatea cibernetică și factorul de reziliență au o pondere mai mare în comparație cu costurile.
Foarte înalt	*pol_adm*	3	Responsabilitățile pentru securitatea cibernetică sunt clare și bine definite în funcție de structura și funcțiile respective. Procesul de schimb de informații este bine stabilit pe verticală și pe orizontală, inclusiv pe plan extern. Există o funcție responsabilă de securitatea cibernetică.
Foarte înalt	*pol_adm*	4	Funcțiile de management și supraveghere a riscurilor cibernetice sunt stabilite și joacă un rol major în procesul decizional.

A fost creată și o funcție dedicată care citește întregul fișier și extrage cunoștințele necesare pentru a fi utilizate de program prin filtrarea nivelului de maturitate, dimensiunea și atributele securității cibernetice în sine.

Pentru stocarea rezultatelor evaluării, a fost utilizat modulul Pickle care este inclus în distribuțiile Python. Aceasta oferă o metodă ușoară de a stoca și citi o structură de obiect Python și a fost utilizată pentru stocarea rezultatelor evaluării, precum și pentru citirea rezultatelor evaluării anterioare. Aceasta conceptualizează stocarea datelor pentru această aplicație. Având în vedere că scopul aplicației este prototipizarea, nu au fost utilizate structuri complexe pentru bazele de date, cum ar fi SQL.

Ca și în cazul funcției de modul, datele sunt stocate în format octet. Următoarele fragmente de cod sunt utilizate pentru a salva și, respectiv, a încărca datele din fișier:

pickle.dump (indicatori, fp)

indicatori = pickle.load (fp)

Programul utilizează o structură de meniu principal ca metodă de îmbunătățire a gradului de utilizare și de a îndeplini scopul prezentării acestui program. Un format existent pentru un astfel de meniu a fost utilizat, adaptat și extins necesităților noastre, pe baza codului open-source disponibil [167]. La instanțierea clasei, următorul fragment de cod prezintă opțiunile pentru selectarea organiza principal.

...

```
MAIN_MENU = {

        1: {
                "label": "General Information",
                "func": self.f1
        },

        2: {
                "label": "Assessment: Policies and administration",
                "func": self.assess1
        },
        3: {
```

...

Conceptul utilizat aici este dicționar în dicționar, care permite citirea cu ușurință și construirea unui meniu principal. La inițializare este necesar de a selecta organizația care va fi supusă evaluării. Ulterior, meniul principal afișează operațiunile posibile, iar după selectarea opțiunii din meniul principal, se apelează funcțiile respective.

Meniul principal complet are următorul format la lansarea programului:

Organizațiile găsite în baza de date sunt următoarele

1. Control_Trafic_Aerian

2. Institutie_Medicala

3. Operator_Energie

4. Operator_Nuclear

Alegeți cifra care corespunde organizației

2

Organizatie: Institutie_Medicala

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

Alegeți o opțiune de meniu:

Titlurile meniului sunt ușor de înțeles și se refera la acțiunile pe care acestea le efectuează. Acest fapt este în corelare cu sugestiile și recomandările din secțiunile 2.2, 2.3 și 2.4.

Opțiunea *Informații generale* prezintă scorul general de maturitate al securității cibernetice pentru fiecare dimensiune, precum și o prezintă nivelul de maturitate în raport cu un prag stabilit. Această amplificare a rezultatelor a fost introdusă pentru a demonstra capacitatea de a extinde prototipul în baza necesităților. De exemplu, tehnologii precum *machine learning* sau inteligența artificială ar putea fi utilizate în aceste implementări. De exemplu, în prototipul dat în cazul în care nivelul de maturitate este sub medie, ceea ce reprezintă un risc ridicat, modelul avertizează utilizatorul despre acest fapt și încurajează luarea de măsuri. Rezultatul alegerii acestei opțiuni de meniu este următoarea:

Alegeți o opțiune de meniu

> 1

****** Informații generale despre nivelul de maturitate al securității cibernetice ******

Ultima evaluare efectuată pe: 2022-05-19

Cel mai recent punctaj mediu: 2,9

****AVERTIZARE****

Maturitatea generală a securității cibernetice este sub medie. Sunt necesare acțiuni pentru îmbunătățirea poziției de securitate. Pentru a vizualiza rezultatele pe dimensiune, selectați IMPRIMAȚI CELE MAI RECENTE REZULTATE.

Următoarele patru opțiuni de meniu declanșează procesul de evaluare pentru fiecare dimensiune a modelului. Funcțiile evaluează mai întâi maturitatea pentru dimensiunea selectată, parcurgând toate atributele, apoi calculează scorul mediu pentru dimensiune și salvează rezultatele în baza de date a programului. Prototipul implementează această funcționalitate, iar adițional, în conformitate cu bunele practici, orice intrare în program este filtrată pentru a ne asigura ca date corecte din punct de vedere semantic sunt introduse. Rezultatul acestei funcții este prezentat mai jos:

Alegeți o opțiune de meniu

> 3

Foarte înalt: programe de formare cuprinzătoare și regulate sunt stabilite și revizuite pe baza celor mai bune practici existente în acest domeniu. Formarea se bazează pe performanță și conține evaluări.

Înalt: sunt stabilite programe regulate de formare și acoperă majoritatea proceselor organizaționale. Instruirea se bazează pe performanță și conține evaluări.

Medie: sunt stabilite programe regulate de instruire pentru toți utilizatorii. Acestea includ aspecte formale și generale legate de procesele organizaționale.

Scăzut: Instruirea utilizatorilor finali ai sistemelor informatice este considerată necesară doar pentru anumite roluri tehnice.

Foarte scăzut: Programul de antrenament este formalizat la maximum, adesea exclusiv prin rapoarte și înregistrări fără sesiuni live.

Alegeți cifra care corespunde nivelului de maturitate de securitate cibernetică al organizației dvs.:

(*5-Foarte mare, 4-Ridicat, 3-Medie, 2-Scăzut, 1-Foarte scăzut*)

După cum se poate observa, programul utilizează cunoștințele de la nivelul de maturitate de securitate cibernetică propus anterior. Conținutul este ușor de citit și înțeles și poate fi ajustat prin modificarea bazei de cunoștințe.

Meniul permite de asemenea schimbarea organizației evaluate, cât și compararea nivelului de maturitate a organizației curente cu cel al altei organizații care a fost evaluată anterior:

Own organization is - Control_Trafic_Aerian

****

1. Control_Trafic_Aerian

2. Institutie_Medicala

3. Operator_Energie

4. Operator_Nuclear

Choose the organization to compare with (enter digit)

4

Comparing with organization: Operator_Nuclear

Comparison results:

	Control_Trafic_Aerian	*Operator_Nuclear*
Policy and administration:	*5*	*5*
Training and Education:	*3*	*2*
Work Environment:	*3*	*4*
Cyber Risk Management:	*3.2*	*5*
Average Score:	*3.55*	*4.0*

Press Enter to continue...

Una dintre ultimele funcții din meniul principal prezintă scorul mediu pe fiecare dimensiune, precum și calculează și salvează un scor general de maturitate de securitate cibernetică pentru organizație. Ieșirea acestui meniu implementează în opinia capacitatea de a identifica dimensiunea care are cel mai redus nivel de maturitate. Rezultatul programului, bazat pe datele de testare date pentru o organizație, este următorul:

The latest assessment results per each dimension are:

- Policies and Administration, last assessment performed on: 2022-06-16, latest average score: 5

- Education and Evaluation, last assessment performed on: 2022-06-16, latest average score: 3

- Work Environment, last assessment performed on: 2022-06-16, latest average score: 3

- Cyber Risk Management, last assessment performed on: 2022-06-16, latest average score: 3.2

**** Overall cyber security score is 3.5****

Prototipul dezvoltat pentru implementarea acestui sistem formal metric inteligent evidențiază versatilitatea și opțiunile de aplicare și integrare a modelului și respectiv a sistemului formal în orice sistem de management al riscului. În plus, arată capacitatea acestui sistem formal

metric inteligent de a fi implementat sub forma unei aplicații simple autonome, care poate fi utilizată de factorii de decizie în procesul de verificare a nivelului de maturitate a securității cibernetice sau de a efectua o nouă evaluare [190]. Formatul și elementele utilizate de acest program au fost selectate pentru a facilita integrarea și adaptarea modelului de către organizații. În timpul dezvoltării prototipului s-au identificat și evidențiat opțiuni de îmbunătățire a modelului, cum ar fi combinarea rezultatelor evaluării cu diverse tehnici de analiză, prin emiterea de avertismente atunci când nu a fost atins un prag minim de maturitate. Acest lucru, combinat cu datele istorice de la alte organizații, ar putea fi util în selectarea dimensiunilor care necesită în mod logic acțiuni de îmbunătățire. În plus, aplicația poate reprezenta componenta de baza pentru un sistemul de suport decizional pentru managementul riscurilor cibernetice. În acest caz, aplicația servește drept cod principal al sistemului, iar atunci când trebuie făcute evaluări de risc sau planuri de tratament, SSD poate fi apelat printr-o funcție de meniu. Interdependența și interoperabilitatea modelului de evaluare a maturității securității cibernetice cu sistemele de suport decizional demonstrează necesitatea evaluării dimensiunii umane pe parcursul ciclului de viață al sistemului informațional.

3.1.5. Postura securității cibernetice

În acest subcapitol a fost prezentat Modelul dezvoltat pentru a facilita evaluarea maturității securității cibernetice, baza de cunoștințe pentru securitatea cibernetică în infrastructuri critice, sistemul formal metric inteligent și aplicația prototip. Au fost identificate și propuse cele patru domenii cheie și a fost creat tabelul care corespunde diferitelor niveluri de maturitate a securității cibernetice. Clasificarea și definirea privind securitatea cibernetică nu pot fi universale, prin urmare modelul propus poate fi extins sau redus în funcție de cerințele și necesitățile organizației. Modelul a fost adaptat domeniului IC și au fost incluse ca atribute cele mai frecvente bariere în promovarea securității cibernetice în astfel de organizații. Criteriile sunt formulate transparent, în limbaj clar, pentru a se asigura că modelul poate fi adaptat de către orice organizații.

Printre cele mai importante atribute se remarcă responsabilitatea individuală pentru securitatea cibernetică, care reprezintă o provocare pentru toate domeniile. Indiferent de cât de avansat este procesul de digitalizare, securitatea cibernetică este adesea privită ca o responsabilitate străina sau chiar ca o chestiune tehnologică. Pentru a asigura că riscurile sunt identificate și atenuate în timp util, este trivială susținerea întregii organizații și sprijinul din partea managementului.

Integrarea TI în tehnologiile operaționale este un alt atribut, puternic interconectat cu altele. Prin înțelegerea impactului amenințărilor cibernetice asupra proceselor dintr-un IC, precum și a

factorului de autoeficacitate, managementul riscurilor cibernetice va deveni mult mai eficient. Trecerea de la raportarea incidentelor sau vulnerabilităților de la entități externe, la identificarea lor printru procedeu intern organizației, este un atribut care poate defini nivelul de securitate cibernetică într-o organizație. Mai mult, în cazul în care dimensiunea umană este printre principalele cauze ale incidentelor de securitate cibernetică, un program de securitate cibernetică bine dezvoltat și cuprinzător poate asigura că organizațiile IC își îndeplinesc misiunea în siguranță și în siguranță.

Dimensiunea umană trece, de asemenea, printr-un proces continuu de schimbare. Adaptarea rutinelor, procedurilor și evaluărilor pentru a acoperi noile tipuri de amenințări trebuie să înceapă de la nivel individual. Tehnologiile nu sunt singura soluție pentru îmbunătățirea culturii securității cibernetice. În timp ce percepția este ca atare, rezultatele analizei selective a literaturii arată că există un consens că elementele factorului uman joacă un rol important în relația cu sistemele informaționale. Prin urmare, un program de formare continuu și complex poate minimiza riscurile cauzate de impactul negativ al dimensiunii umane.

În plus, a fost dezvoltată o aplicație pentru implementarea în formă de cod a conceptului pentru model, care ar putea fi utilizată de părțile interesate pentru a testa și implementa modelul, precum și pentru a sprijini validări la scară largă și programe pilot pentru evaluarea maturității securității cibernetice. Codul urmează același concept ca și în cazul modelului și poate fi rafinat și ajustat, în funcție de contextul, necesitățile și cerințele organizației de implementare.

Un SSD pentru managementul riscurilor cibernetice în IC este o soluție puternică și promițătoare pentru a optimiza resursele utilizate pentru a atenua eficient riscurile cibernetice, precum și pentru a crește poziția de securitate cibernetică a organizației. Cu toate acestea, asigurarea securității cibernetice este o sarcină continuă și complexă și necesită acțiuni complexe în toate domeniile. În timp ce organizațiile pot beneficia de utilizarea unui SSD pentru managementul riscurilor cibernetice, tehnologia nu este întotdeauna soluția. În multe cazuri, elementele factorului uman, precum și alte dimensiuni, cum ar fi politicile, sunt cheia securității cibernetice. În acest capitol este prezentat un model de evaluare a maturității securității cibernetice în infrastructurile critice care este complementar SSD-ului propus. Descriem dimensiunile și atributele corelate cu cele cinci niveluri de maturitate propuse. Modelul a fost prezentat și discutat la Conferința Internațională IE 2021 desfășurată la București, România, precum și la Conferința Națională a Doctoranzilor de la Universitatea de Stat din Moldova (2021).

Modelul a fost prezentat spre evaluare într-un format diferit care permite o evaluare mai ușoară (Anexa 1). Modelul a fost evaluat cu rezultate pozitive de Institutul de Metrologie din Moldova (Anexa 2), Administrația Slovenă de Securitate Nucleară (Anexa 3) și a fost acordată

medalia de bronz la Salonul Internațional de Inovare și Cercetare Științifică „Cadet INOVA'21” (Anexa 4), și medalia de bronz la Salonul Internațional de Invenții și Inovații 2022 [191]. În plus, elemente din model au fost incluse în curriculumul de „Securitate nucleară și radiologică”, parte a Programului de Master la Universitatea Tehnică din Moldova (Anexa 5)

Datorită succesului și *feedback*-ului pozitiv asupra acestui model, a fost dezvoltat, de asemenea, un sistem formal metric inteligent și un prototip în Python care implementează și augmentează conceptele descrise în model. Acest lucru ajută organizația să evalueze mai ușor maturitatea securității cibernetice, precum și să adapteze modelul la diverse necesități.

În următoarele subcapitole sunt prezentate unele studii de caz privind evaluarea cerințelor de securitate cibernetică pentru asistența medicală, precum și domeniul nuclear și radiologic din Republica Moldova, precum și corelarea rezultatelor și recomandărilor privind modelul propus.

3.2. Integrarea securității cibernetice în dispozitivele și serviciile din medicină

Domeniul de asistență medicală a fost și este întotdeauna centrat pe om: de la simplul scop al tratamentului de care o persoană are necesitate până la proiectarea de unități și sisteme care să ajute la identificarea și prevenirea problemelor de sănătate. În contextul digitalizării, noile tehnologii și concepte pot depăși adesea granița tradițională a acestui domeniu.

Echipamentele din medicină utilizate au un scop și o funcție clară, care variază de la cele utilizate în tratament sau diagnostic, până la cele necesare monitorizării. Similar cu alte domenii IC, aceste dispozitive au fost inițial gândite și proiectate cu cerința operării în siguranță. Odată cu dezvoltarea tehnologiilor TI, echipamentele din medicină au evoluat pentru a utiliza noile oportunități oferite de calculatoare. Astfel, aceste echipamente trebuie sa aibă un nivel de securitate adecvat pentru a asigura că funcționalitatea și funcționarea nu sunt afectate, ci, dimpotrivă, sunt protejate de orice riscuri cibernetice și sunt rezistente la încercările de atac cibernetic. Acest lucru se aplică atât dispozitivelor individuale, cât și ecosistemelor întregi, cu scopul principal de a asigura siguranța individului și a societății în ansamblu. Un exemplu recent din decembrie 2021 arată că dispozitivele din medicină sunt vulnerabile și necesită cooperare orizontală pentru a asigura funcționarea sigură [168].

Alte tehnologii emergente, cum ar fi imprimarea 3D sau tele-medicina, operarea și detectarea de la distanță, pot fi, de asemenea, utilizate în domeniul sănătății. Prin urmare, cerința privind securitatea cibernetică se aplică dincolo de domeniul medicinii ca IC, și afectează și orice dispozitive terțe sau chiar cele din lanțul de aprovizionare. Orice tehnologie trebuie să fie robustă din punctul de vedere al securității, pe lângă cea de siguranță, pentru a minimiza orice potențiale riscuri cibernetice. Numărul de procese și servicii care sunt fie complet digitale, fie care utilizează

servicii digitale este foarte mare și include: *e*-Rețetă, aplicații mobile de sănătate, sisteme de implicare a pacienților, telemedicină, hardware sau aplicații de diagnostic. O prezentare neexhaustivă a serviciilor sau sistemelor digitale actuale de asistență medicală poate fi văzută în Figura 3.3.

Healthcare Information and Management Systems Society, o organizație care este adesea menționată și urmărită atunci când se vorbește despre digitalizarea asistenței medicale, oferă diverse modele de maturitate pentru a măsura următoarele procese [169]:

- *Modelul de adoptare pentru Analytics* - analizează rezultatele pe care organizația le-a obținut prin utilizarea analizei.
- *Continuitatea îngrijirii* – analizează amploarea și implementarea comunicării electronice între operatori și pacienți.
- *Rezultatele aprovizionării integrate* - procese și produse utilizate în îngrijire.
- *Adoptarea imaginilor digitale* - utilizarea imaginilor digitale.
- *Adoptarea infrastructurii* - recomandă tehnologii de utilizat pentru a atinge anumite obiective sau standarde.
- *Adoptarea Fișei Medicale electronice în ambulatoriu* – așa-numitul dosar electronic al unui pacient.

Modelul de adoptare a infrastructurii ia în considerare și aspectele de securitate cibernetică. Acest lucru arată că există deja o cerere și necesitatea de a evalua aspecte din acest domeniu. Acest lucru face ca asistența medicală, un domeniu IC, să fie interdisciplinară: pe de o parte, se concentrează pe tratamentul indivizilor, utilizând diverse tehnologii și metode. Pe de altă parte, schimbul de cunoștințe și expertiză trebuie să aibă loc pentru a sprijini domeniul asistenței medicale în ansamblu pentru a-și furniza serviciile într-o manieră sigură din perspectiva securității cibernetice.

În următoarea secțiune sunt reflectate implicațiile securității cibernetice în sectorul medicinii. Discuțiile vor fi corelate, acolo unde este posibil, de cele patru dimensiuni prezentate în modelul de evaluare a maturității securității cibernetice în infrastructurile critice. Acest proces ajută la confirmarea modelului la cercetările anterioare efectuate în acest domeniu.

Fig. 3.3. O privire de ansamblu asupra serviciilor digitale actuale centrate pe om în domeniul sănătății

3.2.1. Securitatea și siguranța în domeniul medicinii

Societatea mereu apreciază beneficiile oferite de serviciile digitale, cum ar fi fișa electronică a pacientului, astfel încât la fiecare vizită la o clinică medicii au acces la toate datele medicale necesare. Multe dintre dispozitivele medicale, cele pentru investigații cu raze X sau RMN stochează rezultatul într-un format digital și ar putea fi salvat automat în dosarul medical electronic. Cele mai multe dintre aceste sisteme au fost proiectate și implementate pentru a utiliza computere pentru gestionarea activităților de zi cu zi în domeniul sănătății, deoarece acestea au fost și sunt considerate inovații.

În cadrul instituțiilor medicale obișnuite se observă că acestea au ca prioritate disponibilitatea datelor, din punct de vedere tehnic rețeaua TI este relativ mare cu un număr mare

de dispozitive conectate iar personalul specializat în TI este deseori insuficient. Din păcate, această afirmație poate fi adevărată pentru un număr mare de instituții de asistență medicală, în special pentru țările în care nu există un cadru clar de securitate cibernetică care să definească responsabilitățile pentru asigurarea securității cibernetice. Cazul TI din domeniul sănătății devine și mai complex odată cu introducerea *rețelelor wireless*, a *site-urilor web* destinate publicului sau a interconectivității cu alte instituții și baze de date. Comparând acest lucru cu o organizație tradițională cu o infrastructură TI, se poate afirma cu ușurință că amprenta tuturor acestor tehnologii este mare și necesită o mulțime de resurse pentru a se asigura că aceste sisteme sunt menținute la zi și configurate corespunzător. În plus, sistemele TI tradiționale utilizate în majoritatea organizațiilor care au recunoscut deja riscurile de securitate cibernetică, cum ar fi în sectorul financiar, încă nu au un management adecvat al vulnerabilităților sau un control al activelor. Domeniul financiar este unul dintre liderii în utilizarea și implementarea tehnologiilor și politicilor pentru a asigura securitatea datelor, datorită valorii ridicate a acestor date. Cu toate acestea, datele generate și utilizate în domeniul asistenței medicale, cum ar fi fișele electronice ale pacienților, sunt, de asemenea, valoroase, deoarece ar putea fi utilizate pentru un număr mare de scenarii. Din păcate, majoritatea acestor date medicale au aplicate controale de securitate insuficiente. Procesele de bază de autentificare sau de autorizare nu sunt implementate corespunzător.

În plus, cultura de securitate din acest domeniu poate fi evaluată ca fiind scăzută, prin urmare tipurile comune de atacuri, cum ar fi trimiterea de e-mailuri de tip spear phishing, ar putea oferi acces unui atacator să găsească și să utilizeze cu scop malițios datele de la instituțiile medicale. Ca exemplu elocvent, atacul *ransomware WannaCry* din 2017, care a criptat datele utilizatorului și a cerut o răscumpărare pentru codul de decriptare, a afectat și sectorul asistenței medicale [170]. Impactul datelor inutilizabile în domeniul medicinii poate avea consecințe dezastruoase. Orice abatere a dozei de radiații utilizate în investigații sau tratament, funcționarea defectuoasă a sistemelor de monitorizare a semnelor vitale sau lipsa antecedentelor medicale ar putea avea un impact iminent asupra vieții oamenilor.

Implicațiile și impactul incidentelor de securitate cibernetică în IC depășesc impactul incidentelor TI tradiționale. Acestea ar putea duce, de asemenea, la incidente de siguranță. Un atac cibernetic este asociat în primul rând cu o alterare a proprietății datelor, indiferent dacă este afectată confidențialitatea, integritatea sau disponibilitatea datelor. Cu toate acestea, în IC precum cel nuclear și în cazul dat - asistența medicală, un atac cibernetic poate fi utilizat pentru a compromite datele, ceea ce ar putea duce și la un eveniment de siguranță. De exemplu, un dispozitiv medical care utilizează surse nucleare sau radiologice pentru tratament și este controlat

de un computer compromis, ar putea duce, din păcate, la un incident de siguranță cu consecințe nefaste pentru pacient și/sau personal.

Un exemplu de incident de securitate cibernetică a fost și modificarea rezultatelor imaginilor medicale 3D [171]. Acest atac poate fi utilizat în scopuri rău intenționate, cum ar fi adăugarea de elemente care ar face ca scanarea să prezinte un diagnostic mai rău sau, pe de altă parte, pentru a ascunde părți ale scanării care arată o anomalie. Astfel de atacuri pot fi utilizate și cu scopul de a perturba cercetările în curs, pentru câștiguri financiare chiar și un act de terorism prin impact asupra societății [171]. Aceasta este una dintre primele dovezi de concepte care arată realitatea unui astfel de scenariu de atac cibernetic. Un potențial atacator ar putea, teoretic, să conducă cu ușurință un astfel de atac, având anumite cunoștințe despre modul în care funcționează aceste sisteme. Astfel, dispozitivele din medicina ce utilizează materiale nucleare, radiologice, chimice și alte tipuri de materiale potențial periculoase, au o importanță critică pentru sănătatea populației si a societății, în momentul în care aceste dispozitive susceptibile la un atac cibernetic pot duce la compromiterea siguranței. Consecințele ar putea fi foarte dezastruoase în astfel de evenimente.

Potrivit Alemzadeh, majoritatea incidentelor (84%) legate de dispozitivele de asistență medicală raportate organismului de reglementare au fost legate de probleme hardware, iar doar 16% au fost legate de probleme de software [172]. În timp ce tehnologia s-a schimbat în ultimii ani, precum și înțelegerea riscurilor de securitate a crescut considerabil, se poate considera în continuare că anumite defecțiuni hardware ar putea fi declanșate sau îmbunătățite de un atac de securitate cibernetică prin utilizarea funcțiilor operațiunilor care nu au fost luate în considerare în faza de proiectare a dispozitivului.

Numărul de perturbări ale datelor este în creștere în zilele noastre. Numărul de sisteme și aplicații interconectate este un factor care face ca atacurile cibernetice să reprezinte un risc sporit pentru aceste tipuri de sisteme. Comunitatea TI lucrează împreună cu furnizorii pentru a identifica și integra potențiale controale de securitate. Cu toate acestea, de multe ori aceste controale sunt adaptate la sisteme, care nu corespund conceptului de securitate prin proiectare, unde astfel de riscuri sunt identificate și luate în considerare încă din faza de proiectare a unui sistem. Rezultatul este că aceste controale pot fi eficiente, însă nu în toate situațiile. Există cazuri în care multe sisteme trebuie să fie închise, de exemplu, fără nicio conexiune la internet, ori orice flux de intrare și ieșire de date să fie monitorizat în afara sistemului propriu zis.

Datele din medicină pot conține diverse informații personale, cum ar fi data nașterii pacientului, actul de identitate, numărul de asigurare, precum și date medicale. Publicarea acestor date confidențiale ar putea duce la situația la o creștere a tentativelor de fraudă, determinate de

dorințe de câștig financiar ilicit (de exemplu, clauze false pentru asigurare, accesarea conturilor instituțiilor financiare utilizând datele personale ca pas intermediar etc.). Cu toate acestea, în acest domeniu, nivelul culturii de securitate este încă relativ scăzut, riscurile cibernetice nefiind identificate sau evaluate în mod corespunzător. Acest lucru se datorează în principal unui nivel scăzut de conștientizare a securității și potențialelor implicații și consecințe ale unei încălcări a datelor.

Calculele efectuate de computere care fac parte din dispozitivele medicale sunt programate utilizând algoritmi logici de bază. De exemplu, o scanare ar avea ca rezultat un set de date care este salvat într-o bază de date și se aplică diverși algoritmi și verificări. În plus, învățarea automată și inteligența artificială pot fi, de asemenea, utilizate pentru a evalua aceste date și a scoate un format care poate fi citit de om, care poate fi și un diagnostic. Astfel, potențialii vectori de atac pot fi deduși teoretic. La fel ca în orice alt proces de testare de securitate, inițial modulul de introducere a datelor este testat dacă acceptă alt tip de intrare, cum ar fi un format diferit, precum și dacă a igienizat corespunzător aceste date înainte de a le transmite modulului de procesare. Similar industriilor tradiționale, sistemele operaționale din domeniul sănătății au fost proiectate și programate cu convingerea și presupunerea că datele introduse sunt standard și vor fi întotdeauna într-un anumit format și dimensiune. Scopul și cerința principală au fost să asigure funcționalitatea dispozitivului, fără a lua în considerare alte cerințe sau preocupări, cum ar fi securitatea cibernetică. Următorul pas logic în analiza vectorului de atac este fluxul de date. Analizarea sistemului și înțelegerea modului în care datele sunt transferate de la un modul la altul ar arăta potențiale puncte de defecțiune sau, în acest caz, potențiali vectori de atac. Acesta a fost și vectorul de atac cel mai probabil utilizat în timpul cercetării efectuate de Mirsky [171].

Exemplul abordat în această secțiune arată încă o dată impactul și actualitatea necesității asigurării securității cibernetice în medicină. Este necesar un plan de acțiune pragmatic și coordonat pentru a asigura că industria și instituțiile relevante recunosc riscul amenințărilor cibernetice și înțeleg soluțiile necesare pentru a asigura securitatea în acest domeniu.

3.2.2. Politica și cultura de securitate

În această secțiune este discutată necesitatea standardizării cerințelor de securitate cibernetică între domeniile dintr-o țară și a unei cooperări orizontale puternice la nivel național.

Politica și reglementările în domeniul securității cibernetice sunt o prioritate pentru multe instituții internaționale [173]. Din punct de vedere juridic, țările și-au dezvoltat deja și își îmbunătățesc mereu strategia de securitate cibernetică și cadrul legal respectiv. Recunoașterea riscurilor din spațiul cibernetic și a impactului potențial pentru IC, inclusiv în medicină, este unul

dintre primii factori de motivare pentru stabilirea și menținerea unui program de securitate cibernetică. Aceste măsuri pot fi luate la diferite niveluri – cum ar fi la nivel administrativ, printr-o politică sau un ghid până la nivel de operator prin implementarea tehnică, cum ar fi sistemele sau controalele implementate. În plus, cele mai bune practici și cerințe care s-ar aplica în mod normal domeniului TI sau software-ului trebuie să fie luate în considerare și de alte domenii din momentul în care sistemele informatice devin parte din acel domeniu. Dar acest lucru nu a fost întotdeauna cazul și o parte din evoluția legată de securitatea cibernetică a avut loc după anumite evenimente. De exemplu, incidentele legate de sectorul sănătății sunt deja o realitate comună și ar trebui luate în considerare de toate statele în dezvoltarea capacității de a identifica și de a răspunde la astfel de incidente [7, 9, 10]. Dacă ne întoarcem cu un deceniu în urmă, probabil că nu mulți s-ar gândi la astfel de riscuri atunci când dezvoltau sau utilizau aceste noi sisteme computerizate.

În paralel cu domeniul nuclear și radiologic, în care aspectele de securitate cibernetică au fost incluse ca parte a asigurării unui regim de securitate nucleară, precum și cerințele tehnice pentru operatorii în manipularea datelor sensibile sau implementarea sistemelor de securitate fizică, se poate observa că unele aspectele de securitate ar putea fi efectuate de organismul de reglementare din domeniul TI. Cooperarea orizontală este necesară între domeniile care utilizează TI și specialiști în securitate cibernetică pentru a defini și evalua corect astfel de controale tehnice, datorită cunoștințelor specifice necesare. Aceasta este o recomandare pentru cazul specific al domeniului nuclear/radiologic și al securității cibernetice, care ar putea fi aplicată și pentru domeniul medical [62]. Multe dintre riscurile cibernetice ar putea fi minimizate dacă securitatea cibernetică ar fi inclusă ca o cerință la proiectarea unor astfel de sisteme. Mai mult, astfel de cerințe pot fi stabilite și la eliberarea unei licențe sau autorizații, la procesul de acreditare pentru instituțiile medicale. O soluție ar fi o reglementare hibridă de autorizare, licențiere sau acreditare care s-ar face de către organismul de reglementare respectiv, de exemplu din domeniul sănătății, susținută de instituția care poate oferi expertiză în materie și reglementare din domeniul securității cibernetice.

Dacă se analizează tipul de date care sunt colectate, partajate și utilizate, atunci în multe țări un astfel de tip de date este deja calificat drept date cu caracter personal și protejat de lege. Astfel, riscurile sunt identificate în anumite regiuni și există o serie de controale de securitate care sunt aplicate prin reglementări. Majoritatea reglementărilor privind datele personale, cum ar fi GDPR, acoperă aspectul raportării către autoritatea națională ori de câte ori a fost descoperită o încălcare. Reglementările reprezintă un bun început și pot servi drept ghid pentru furnizori, precum și pentru operatori, în stabilirea unui program de securitate a informațiilor și acoperă elemente precum protecția datelor, răspunsul la incidente, mecanismele de raportare. În multe cazuri

realitatea este diferită și scopul de a fi conform lasă adesea lacune de securitate care nu sunt acoperite de reglementări.

Un rol important în dezvoltarea și implementarea securității cibernetice în alte ramuri, cum ar fi medicină, trebuie să fie preluat și de instituțiile de învățământ superior. De exemplu, Universitatea de Stat din Moldova, Facultatea de Calculatoare, Informatică și Microelectronică din Universitatea Tehnică a Moldovei să ofere cursuri de specialitate în securitate cibernetică pentru alte facultăți, datorită legăturilor pe care această temă le are cu alte domenii. Paralel, permiterea organizațiilor naționale și internaționale să dezvolte cerințe și bune practici legate de cibernetică este o acțiune cheie care trebuie văzută în toate domeniile. Complexitatea infrastructurii TI din zilele noastre este atât de mare, încât conectează majoritatea dispozitivelor din diverse domenii, dintre care multe nu au fost dezvoltate și concepute pentru a rezista atacurilor cibernetice. Prin urmare, cooperarea și acțiunile întreprinse la nivel național și internațional sunt cheia pentru includerea aspectelor de securitate cibernetică în alte cadre de reglementare.

Cooperarea orizontală este necesară și pentru evaluarea poziției de securitate a dispozitivelor medicale, datorită cunoștințelor specifice necesare pentru a înțelege funcționalitatea dispozitivelor, precum și impactul pe care o modificare a fluxurilor de date l-ar putea avea asupra dispozitivului și asupra pacientului însuși. Aceasta a fost și una dintre concluziile cercetărilor efectuate pentru dispozitivele medicale utilizate în domeniul cardiologiei și necesitatea informării utilizatorilor cu privire la riscurile de securitate cibernetică [174]. Acest lucru este valabil și pentru orice dispozitive medicale, inclusiv dispozitivele mobile sau cele situate în incinta unui operator de asistență medicală [175]. Chestiunea culturii securității intră din nou în joc pentru a informa în consecință utilizatorii, precum și operatorii despre care sunt riscurile de securitate cibernetică și cât de tangibile sunt acestea pentru siguranța lor. O cooperare interdisciplinară este trivială atunci când vine vorba de securitatea cibernetică datorită integrării componentelor TI în TO, transmiterii riscurilor de securitate cibernetică de către orice domeniu care face uz de TI, precum și acțiunilor comune în creșterea culturii generale de securitate.

De asemenea, comunitatea internațională ar trebui să preia inițiativa de a evalua riscurile de securitate cibernetică din alte domenii și să dezvolte recomandări și directive pentru domeniul medicinii. Preluarea bunelor practici ar sprijini țările să le adopte și să le adapteze în cadrul lor legislativ. Acest lucru ar asigura că, indiferent de resursele de care dispune o anumită țară, aceasta va putea accesa cele mai bune practici și recomandări actualizate în securizarea dispozitivelor de îngrijire a sănătății, ceea ce s-ar reflecta în cele din urmă în mod pozitiv pentru societate și siguranța acesteia. Considerarea acestora ar satisface cerințele în materie de procese la nivel național și ar declanșa schimbări directe atât pentru operatori, cât și pentru furnizorii de astfel de

echipamente. Subiectul devine și mai important atunci când vorbim de dispozitive care utilizează radiații ionizante și ar putea avea un impact asupra siguranței societății. Industria nucleară este un exemplu în care amenințările la siguranță au convins statele membre să sprijine elaborarea de reglementări și orientări pentru securitatea cibernetică în instalațiile nucleare sau pentru operatorul de materiale nucleare și radiologice, și să le monitorizeze sub egida AIEA.

3.2.3. Viitorul securității cibernetice în domeniul medicinii

Dintr-o perspectivă globală, evoluțiile ulterioare și inovarea în sectorul sănătății ar trebui să includă securitatea cibernetică ca o condiție obligatorie și să includă și o cooperare interdisciplinară. Motivul pentru care sectorul medical constituie o țintă se datorează lacunelor politicilor, controalelor tehnice slabe, precum și subestimării valorii datelor care sunt procesate sau stocate. Similar altor sectoare, este necesar să se schimbe mentalitatea și să se educe utilizatorii cu privire la beneficiile controalelor de securitate. Aici se impune cooperarea interdisciplinară sau orizontală.

Se recomandă ca riscurile cibernetice să fie abordate din punct de vedere al politicilor preferință la nivel național, cu scopul de a asigura că furnizorii de echipamente medicale îndeplinesc anumite cerințe de securitate care sunt deja obligatorii. În plus, este necesară implementarea reglementărilor naționale pentru asigurarea cerințelor de securitate. Acest lucru ar trebui să fie aplicabil atât sistemelor TI tipice atât corporative, cât și computerelor utilizate în domeniul IC. Cooperarea orizontală între instituțiile cheie la nivel național ar trebui consolidată [176].

Totuși, acest lucru poate duce la anumite diferențe între țări în ceea ce privește nivelul de maturitate al unor astfel de reglementări, precum și în funcție de nivelul culturii de securitate. Prin existența unor scheme de certificare naționale, regionale și chiar internaționale, s-ar asigura că astfel de sisteme de asistență medicală au fost proiectate și dezvoltate conform celor mai bune practici de securitate. În cele din urmă, acest lucru este aplicabil și altor domenii din industrie. Acest lucru este, de asemenea, implicit în contextul cooperării regionale, în care dosarele medicale sunt schimbate între țări, cu scopul de a oferi mobilitate și acces la servicii, indiferent de locația unei persoane [171].

Se poate considera că tehnologiile actuale sunt suficiente pentru a începe acest proces, totuși va necesita actualizări în viitor atât pentru design, cât și pentru funcționalitate, pentru a ne asigura că dispozitivele de asistență medicală au un nivel adecvat de securitate care minimizează orice potențiale amenințări pentru siguranța exploatării. Deși există anumite modele de maturitate și ajută la măsurarea digitalizării în domeniul sănătății, analizând și anumite controale tehnice în

securitatea cibernetică, se constată că nu toate aspectele au fost acoperite. Prin urmare, modelul propus în subcapitolul 3.1 este aplicabil și în alte domenii IC, cum ar fi medicină, deoarece oferă o imagine de ansamblu solidă și generală a întregului program de securitate cibernetică din organizație.

Ca recomandare, bunele practici în domeniul securității TI sunt aplicabile în alte domenii, și pot fi adaptate în funcție de sfera și cerințele sistemului. Este și cazul dispozitivelor medicale. Exemplul de atac cibernetic prezentat în această secțiune ar fi putut fi detectat și prevenit prin implementarea anumitor controale elementare de securitate și proiectare, cum ar fi criptarea datelor și verificările de integritate. Prin urmare, cerințele minime de securitate ar trebui să fie aplicabile în măsura posibilului în toate domeniile industriei, inclusiv în domeniul sănătății, pentru a asigura că vânzătorii, precum și operatorii respectă o anumită linie de bază de securitate. Scopul general este de a preveni un atac cibernetic și, cel mai important, de a reduce și de a preveni orice incident de siguranță de care ar putea suferi o persoană sau o țară.

O altă recomandare și o practică bună este securitatea prin proiectare, care prevede necesitatea identificării și stabilirii cerințelor de securitate ale unui sistem încă din faza de proiectare. Acest lucru poate duce adesea la alegerea diferitelor arhitecturi și configurații pentru a îndeplini aceste cerințe - acțiuni care sunt imposibil sau foarte costisitoare de realizat după ce un dispozitiv a fost deja proiectat și este utilizat activ.

3.3. Aplicabilitatea modelului pentru evaluarea dezvoltării programelor de securitate cibernetică

În acest subcapitol sunt prezentate rezultatele bazate pe modelul de evaluare a maturității securității cibernetice asupra dezvoltării programului de securitate cibernetică pentru IC în Republica Moldova [139]. În perioada 2020-2021, sectorul medicinii a devenit o țintă principală de interes strategic în rândul criminalilor cibernetici. Astfel de atacuri cibernetice pot duce nu numai la breșe de securitate, ci și la evenimente de siguranță care afectează viețile oamenilor. Concluziile acestei cercetări confirmă recomandările anterioare privind cerințele de securitate cibernetică pentru domeniul medical sau alte IC cum ar fi nuclear și radiologic. Rezultatele se clasifică în funcție de cele patru dimensiuni ale modelului recent dezvoltat pentru evaluarea maturității securității cibernetice în IC [139]. Această analiză confirmă aplicabilitatea modelului pentru organizații aflate în diferite stadii de dezvoltare a securității cibernetice, precum și din diferite domenii.

Sectorul sănătății, critic în ultimii ani din cauza pandemiei, nu este, din păcate, o excepție de la atacurile cibernetice. Aproape o treime din atacurile legate de COVID-19 vizează autoritățile

publice și instituțiile de sănătate. Una dintre principalele cauze pentru aceasta este faptul că multe tehnologii din domeniul sănătății sunt depășite din perspectiva securității. Prin urmare, instalațiile din acest domeniu sunt atractive pentru răufăcători. Astfel de atacuri pot fi lansate de către dezvoltatorii de programe *malware* sau *ransomware*, axate pe frauda financiară, cât și pentru actorii statali [177].

În plus, pe măsură ce mai multe dispozitive medicale utilizează materiale nucleare sau radiologice, crește severitatea amenințării având în vedere prejudiciul și impactul pe care le pot avea astfel de incidente. Vectorii de atac variază, de la inginerie socială la exploatarea vulnerabilităților cunoscute sau necunoscute. Prin urmare, este necesară o viziune complexă asupra tuturor sistemelor digitale utilizate, a vulnerabilităților pe care acestea le-ar putea avea, precum și a politicilor și standardelor existente urmate de practicieni în asigurarea unui nivel adecvat de securitate cibernetică.

De menționat că, în timp ce peste 90% dintre întreprinderi au implementat cel puțin un control de securitate, 13% din aceste întreprindere au fost afectate de un incident de securitate [187]. Figura 3.4 prezintă procentul și tipurile de controale de securitate, care relevă anumite lacune în ceea ce privește funcțiile, politicile existente și acuratețea acestor politici.

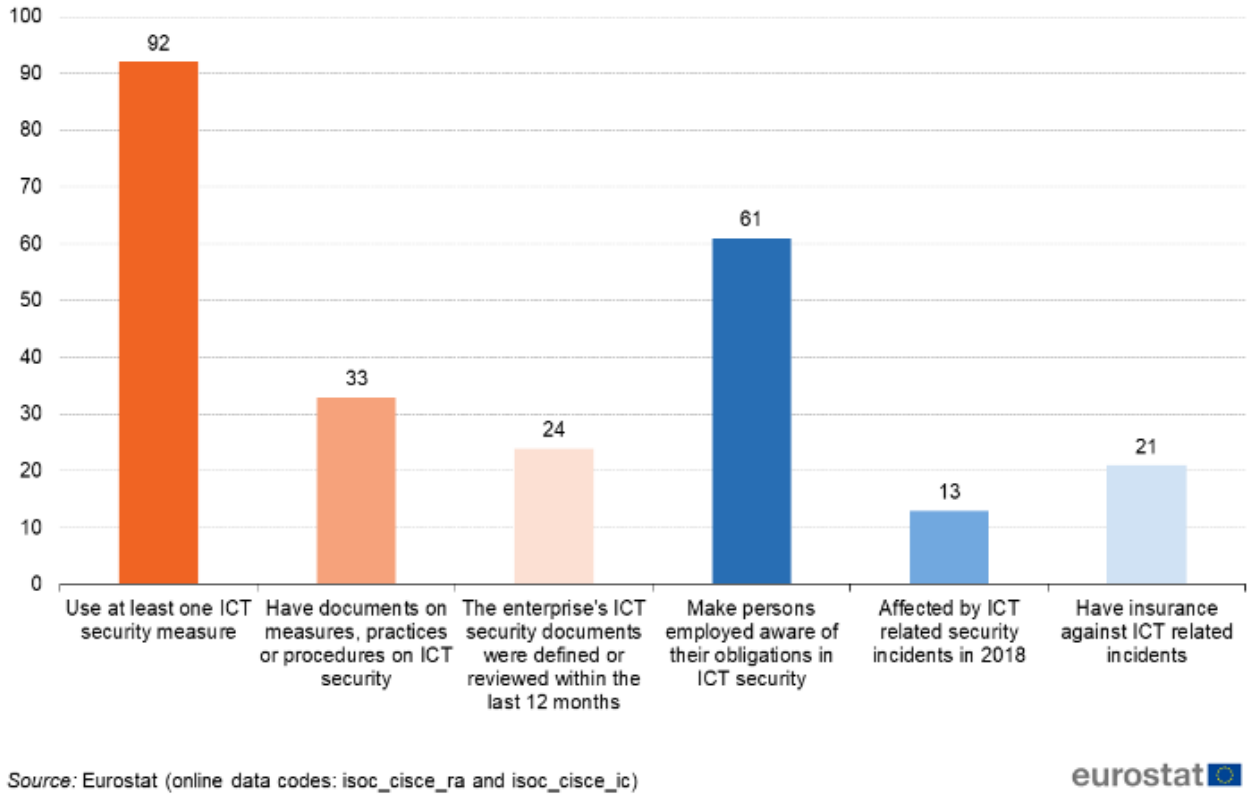

Fig. 3.4. Securitatea TI în întreprinderi, UE-27, 2019 (% întreprinderi), conform Eurostat [187]

În contextul Republicii Moldova au fost efectuate analize asupra dezvoltării programului de securitate cibernetică pentru domeniul nuclear și radiologic strâns legat și de domeniul medicinii, precum și corelarea cu îndrumările și recomandările internaționale în acest sens. Atacurile cibernetice împotriva IC la nivel internațional asupra entităților medicale sau nucleare și radiologice au crescut în frecvență în ultima perioadă, ceea ce necesită o protecție adecvată la nivel național [68, 106, 164, 176, 178, 179, 180]. Aceste circumstanțe impun statele să dezvolte și să îmbunătățească în continuare răspunsul la incidente.

În secțiunile următoare este prezentată evaluarea securității cibernetice utilizând modelul propus anterior pentru domeniile medicină, nuclear și radiologic [139].

3.3.1. Maturitatea securității cibernetice în Moldova

Una dintre primele analize din 2015 a identificat includerea elementelor de securitate cibernetică în legislația internă privind siguranța și securitatea obiectivelor nucleare și radiologice [164]. Acest lucru este strâns corelat cu îndrumările și recomandările internaționale din partea AIEA. Întrucât legislația în domeniul nuclear și radiologic include considerarea obligatorie a securității cibernetice, aceasta a creat premisele necesare pentru o cooperare orizontală cu organismele specializate în TI. Este cea mai bună soluție în situația în care cunoștințele aprofundate în domeniul securității cibernetice sunt insuficiente pentru personalul din alte domenii, atât în 2015, cât și în prezent. Furnizorii de asemenea recomandă implementarea cerințelor de securitate TI din domeniul IC [22, 58], precum și organizațiile de cercetare [102]. Acest lucru este dictat și de cerințe tehnice specifice, cum ar fi accesul utilizatorilor, monitorizarea și raportarea incidentelor sau confidențialitatea datelor care sunt derivate din legislația nucleară și radiologică actuală. Astfel de statut poate fi reflectat de modelul propus, atunci când toate dimensiunile au evaluări sub medie, și există o anumită conștientizare și cunoaștere, dar, totuși aceasta este foarte perturbată în toate dimensiunile [181, 182]. În Figura 3.5 sunt prezentate rezultatele aplicării modelului față de analiza din 2015 [164].

Din cele patru dimensiunile analizate: fără fundal colorat denotă o maturitate de securitate cibernetică foarte scăzută, cu fundal galben denotă nivel scăzut, verde deschis – mediu și verde închis un nivel de maturitate cibernetică înalt. Prin urmare, o prioritate în scenarii cu o maturitate scăzută este dezvoltarea și îmbunătățirea secțiunii de administrare și management.

O analiză ulterioară analizează interdependența nivelului cibernetic la nivel național și evoluțiile securității cibernetice în domeniul IC [179]. Cadrul legal în domeniul securității cibernetice a fost îmbunătățit în 2015 odată cu aprobarea unui nou Program național de securitate cibernetică, care acoperă aspecte precum funcții și responsabilități pentru securitatea informațiilor,

indicatorii de formare, precum și o primă încercare de a clarifica termenii cheie și de a construi un sistem de management al securității [1, 181].

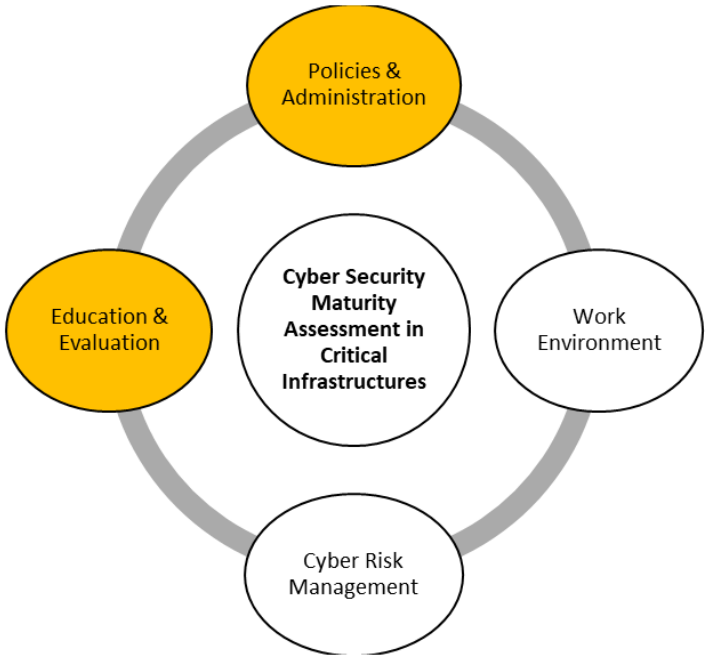

Fig. 3.5. Maturitatea securității cibernetice în 2015

Considerând aceste evoluții la evaluarea efectuată prin intermediul modelului, se observă necesitatea dezvoltării componentei de educație și evaluare (Figura 3.5). Acest lucru este esențial pentru a ne asigura că alte dimensiuni interdependente, cum ar fi managementul riscurilor cibernetice și mediul de lucru (Figura 3.6), vor avea condițiile prealabile necesare pentru a fi dezvoltate. Acest lucru este dictat direct de dezvoltarea cadrului legal și indirect de conștientizarea riscurilor cibernetice.

O altă etapă importantă în dezvoltarea programului de securitate cibernetică în Moldova este aprobarea cerințelor minime de securitate cibernetică [30]. Acest document oferă o perspectivă complexă, dar și tehnică, asupra tuturor domeniilor securității cibernetice. Așa cum se poate deduce din denumirea documentului, acesta se concentrează pe cerințe tehnice și funcționale care promovează dezvoltarea programului de securitate cibernetică.

Acest lucru poate fi tradus în diferite atribute și dimensiuni ale modelului propus, acoperind aspecte precum controalele tehnice și configurarea acestora, ridicarea nivelului de conștientizare a utilizatorilor și instruirea acestora. Prin urmare, evaluarea retroactivă a maturității securității cibernetice prin intermediul modelului arată o îmbunătățire semnificativă față de anul 2015. În primul rând, se remarcă o dezvoltare continuă a legislației, care are impact direct asupra tuturor dimensiunilor modelului. Acest scenariu și calea de dezvoltare pot fi considerate ca o foaie de parcurs standard.

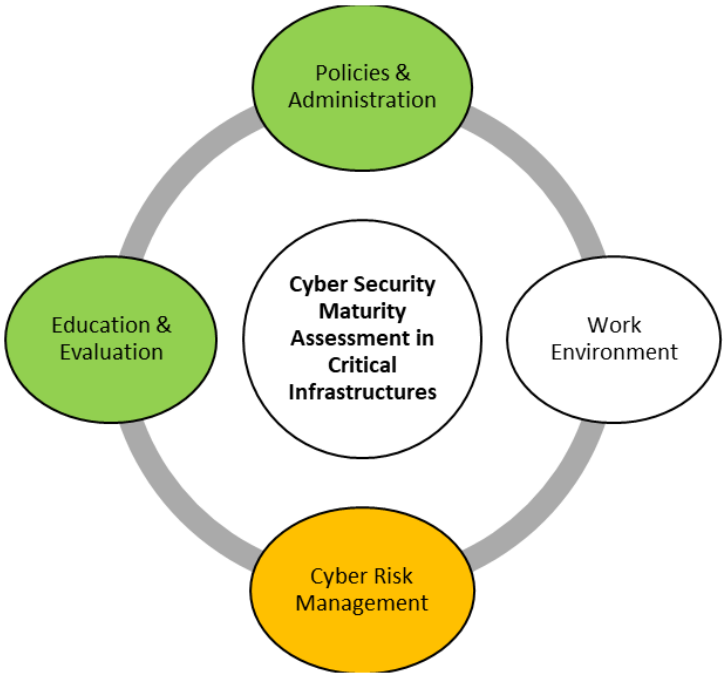

Fig. 3.6. Dezvoltarea practicilor de management al riscurilor cibernetice

O ultimă etapă atinsă în programul de securitate cibernetică al Republicii Moldova este Strategia de securitate a informațiilor pentru anii 2019-2024 cu Planul de acțiuni pentru implementarea acesteia, aprobate de către Parlament [38]. Strategia identifică aceleași amenințări și preocupări, totuși acoperă acțiuni și obiective cuprinzătoare pentru a asigura un nivel adecvat de securitate cibernetică în toate domeniile țării. Strategia menționează scopul său de a acoperi în mod explicit organizațiile din domeniul IC, precum și reflectă asupra importanței pe care instituțiile IC o au în procesul de luare a deciziilor. Este remarcată de asemenea armonizarea cu politicile UE privind definirea infrastructurilor critice, care a fost menționată în strategie. În plus, sunt susținute obiectivele de a efectua un audit de securitate cibernetică pentru toate tipurile de IC, precum și de a dezvolta planuri pentru a securiza un astfel de tip de organizații. Astfel, modelul propus ar putea servi și în scopul auditării/acreditării unor astfel de organizații, având în vedere maturitatea și contextul securității cibernetice din Republica Moldova. Evaluarea maturității securității cibernetice a stării actuale pe baza acestei strategii este reprezentată în Figura 3.7.

Sunt remarcate și acțiunile întreprinse de CNSSN al UTM de dezvoltare și aprobare a curriculum-ului specific interferenței securității cibernetice cu securitatea, siguranța nucleară și neproliferarea (Anexa 4), ce se încadrează și contribuie la realizarea prevederilor Planului de acțiuni pentru implementarea Strategiei de securitate a informațiilor pentru anii 2019-2024 (Legea 257, 2018; Titl. I, pct. 10; pct.11, al. 7; Titl. IV, pct. 22, al. 3) [63, 38].

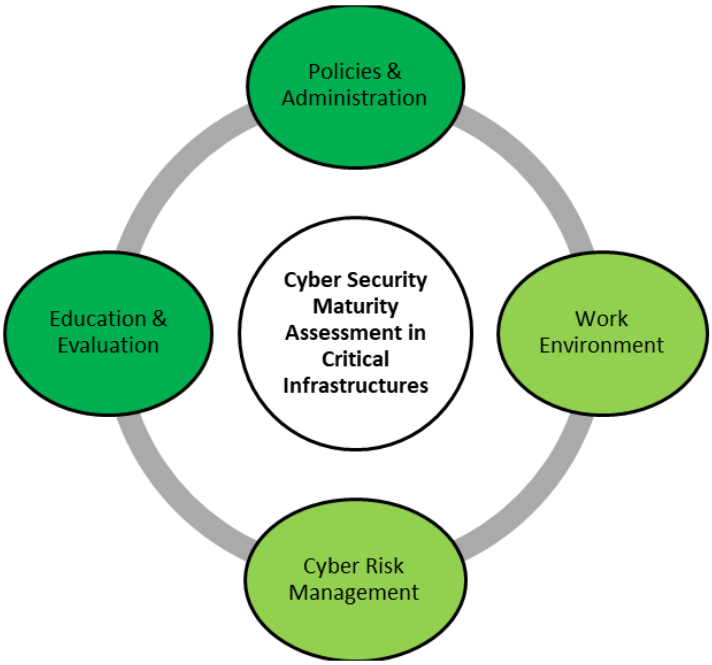

Fig. 3.7. Rezultatele dezvoltării programului de securitate cibernetică

Ghidurile elaborate recent și integrarea subiectelor în programele de studii de master în diverse domenii ale USM, UTM, care includ, printre altele, elemente de securitate cibernetică, sunt, de asemenea, rezultate ale intereselor de a consolida în continuare programul național de securitate cibernetică prin formarea experților, creșterea gradului de conștientizare și a culturii generale de securitate [64, 65]. Prin urmare, pentru a asigura maturitatea cibernetică în entitățile IC, este necesară prezența și dezvoltarea (*in situ* sau *prin cooperare*) a tuturor dimensiunilor [182].

Analizele efectuate în domeniul sănătății, în 2016 și respectiv 2019, au arătat că, deși există tehnologii, acestea nu pot fi puse în aplicare în lipsa unei politici și reglementări naționale în acest sens [68, 178]. Acest rezultat este strâns corelat cu mentalitatea și cultura generală de securitate, deoarece dimensiunea umană are o influență puternică asupra dezvoltării cadrului legal.

În faza de dezvoltare a programelor a fost identificată o corelare care este confirmată de primele două dimensiuni ale modelului, cheie pentru declanșarea dezvoltărilor tehnice generale. Prin urmare, orice modificare în ceea ce privește controalele de securitate ar trebui să declanșeze o reevaluare completă. Acest lucru este implicat din cauza dimensiunilor modelului, care sunt puternic corelate [182]. De exemplu, o modificare a politicii și a administrației ar putea duce la schimbări benefice în toate dimensiunile modelului, cum ar fi educația și evaluarea sau modul în care riscurile cibernetice sunt abordate, în managementul riscurilor cibernetice. Viceversa, un management mai eficient al riscurilor cibernetice ar putea fi o contribuție pentru adaptarea și îmbunătățirea în continuare a atributelor măsurate din dimensiunile Educație și Evaluare sau Administrare și Management. O prezentare generală a acestui proces este dată în Figura 3.8.

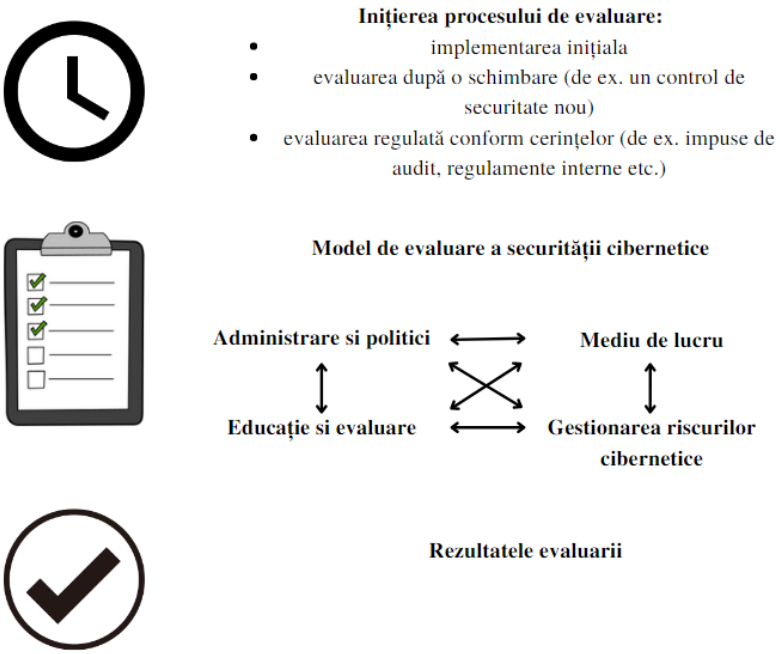

Fig. 3.8. Procesul și declanșatorii pentru evaluarea maturității securității cibernetice

Și iarăși cooperarea orizontală cu alte organizații IC, autorități naționale sau furnizori, ar fi soluția optimă pentru fi la curent cu evoluțiile din acest domeniu. Un exemplu practic legat de Republica Moldova ar fi sincronizarea organizațiilor IC din diferite domenii, cum ar fi între asistența medicală și domeniul nuclear sau radiologic, pentru a învăța din evoluțiile și calea în construirea capacității pentru a gestiona mai bine riscurile cibernetice. În plus, această soluție ar putea fi aplicată având în vedere utilizarea surselor de radiații ionizante în domeniul sănătății, precum și necesitatea iminentă de a asigura securitatea cibernetică a dispozitivelor de îngrijire a sănătății în contextul pandemiei de Covid-19.

3.3.2. Evoluții în securitatea cibernetică

Exemplul considerării securității cibernetice în interferență cu securitatea nucleară și radiologică, ca model de preluare a bunelor practici internaționale [33, 34], actualizat și extins, pe domenii de activități, continuu în Republica Moldova în ultimii ani [52, 54, 55, 56], denotă importanța și complexitatea subiectului de securitate & siguranței și a potențialelor amenințări la adresa statelor. Aprobarea Regulamentului privind securitatea fizică în activități nucleare și radiologice [56], care a fost prezentat la Conferință de Securitate a Computerelor a AIEA din 2015, este menționat ca o realizare în fortificarea cadrului legislativ național nuclear. Conform noilor cerințe din Republica Moldova, fiecare operator din domeniul nuclear și radiologic este responsabil să își protejeze activele digitale, inclusiv rețeaua, de atacurile cibernetice pentru obținerea licenței (autorizației) de activitate. Termenii actualizați din cadrul normativ din

Republica Moldova privind securitatea cibernetică în conexiune cu cea nucleară și radiologică sunt apreciate ca un pas important înainte în dezvoltarea ulterioară a contextului legislativ și sub-legislativ necesar pentru o mai bună implementare în practică.

Cu toate acestea, lipsa resurselor umane calificate în securitatea cibernetică la operatori ar putea duce, cu regret, la implementarea insuficientă a cerințelor din Legea 132 [31] privind desfășurarea în siguranță a activităților nucleare și radiologice, altor acte sublegislative. Acest fapt poate diminua importanța procesului de evaluare și autorizare (licențiere). În acest context, rolul unor organizații de asistență științifică tehnică este important pentru a neutraliza lacunele de personal, cunoștințe și experiență și pentru a oferi suport specializat, prin contractarea de experți sau entități specializate și abilitate în securitatea cibernetică aplicată în domenii de nișă precum cel nuclear și radiologic, medical etc.

Pe de altă parte, Planul de acțiuni pentru implementarea Strategiei de securitate a informațiilor pentru anii 2019-2024 (Legea 257, 2018; Titl. I, pct. 10; pct.11, al. 7; Titl. IV, pct. 22, al. 3) [38] denotă sprijinul ferm al guvernării pentru cercetări, pentru formarea și dezvoltarea resurselor umane în domeniul securității cibernetice cu impact major pozitiv atât asupra domeniului public cât și asupra IC, inclusiv radiologic, nuclear, medical etc. Noua strategie de securitate a informațiilor, programul de securitate cibernetică cu propuneri privind cerințele minime de securitate cibernetică reprezintă un avans în procesul de securizare a sistemelor și informațiilor critice în ceea ce privește securitatea computerelor. Se preconizează că acțiunile planificate vor avea o îmbunătățire generală a securității autorităților publice și operatorilor care utilizează date sau materiale critice. Aprobarea unui regulament la un nivel înalt și dezvoltarea acestuia pe o abordare bazată pe risc sunt bune practici în stabilirea regimurilor de securitate, însă nu este întotdeauna ușor de găsit echilibrul între reglementările prea tehnice și cele generale. Cerințele specificate în documente trebuie să fie clar definite și realiste pentru a fi implementate de către operatorii din organizațiile lor și să decurgă din obiectivele strategiilor sau programelor de securitate. Procesul de definire a cerințelor este dificil, deoarece necesită cunoștințe și experiență profundă în securitatea TI - cerințele prea detaliate ar putea fi greu de implementat și ar putea deveni depășite într-o perioadă scurtă de timp, unde cele generale ar putea lăsa spațiu pentru interpretare. Prin urmare, bunele practici în elaborarea cerințelor ar trebui să fie luate în considerare, precum și posibilele experiențe anterioare din alte state. Aceasta ar fi o acțiune pe termen lung, deoarece operatorii, precum și entitățile de reglementare ar trebui să ia măsuri (identificarea resurselor umane și financiare) pentru a se alinia cerințelor.

Domeniul nuclear și radiologic din Republica Moldova este un exemplu relevant în care este necesară cooperarea între entitățile IC cu alte organizații specializate în securitate cibernetică

la nivel național, datorită cunoștințelor specifice necesare unui management complex și modern al securității fizice care utilizează componente TI. Pentru a crește gradul de conștientizare în materie de securitate și nivelul culturii de securitate nucleară, este necesar să se dezvolte cadre de cooperare prin consultarea experților din alte domenii, inclusiv cibernetice. Un alt motiv pentru promovarea acestei cooperări este numărul limitat de experți naționali în domenii conexe. De asemenea, implementarea cerințelor de securitate cibernetică va necesita participarea unor astfel de experți pentru a asigura înțelegerea corectă a cerințelor unui domeniu specific precum nuclear și radiologic. Ca recomandare, Seria 17 de Securitate Nucleară (NSS-17) a AIEA [33] ajută operatorii în implementarea acestor controale, deoarece oferă îndrumări cu privire la definirea nivelurilor de securitate, precum și a controalelor tehnice și administrative. De asemenea, contribuie la înțelegerea rolului securității computerelor pentru sistemele de control industrial sau securitatea fizică și siguranța, precum și oferă un bun punct de plecare pentru dezvoltarea politicilor de securitate în cadrul organizației. Dezvoltarea viitoare în securitatea cibernetică și nucleară ar trebui să se bazeze și pe cooperarea la nivel național și internațional, deoarece în prezent amenințările modelează politicile și cerințele pe care statele le dezvoltă și le aplică în strategiile și reglementările de securitate.

Rolul organizațiilor academice sau specializate (în alți termeni organizațiile de sprijin tehnic și științific) este important în astfel de cazuri pentru a acoperi lipsurile de cunoștințe și experiență și pentru a oferi suport specializat, cum ar fi contractarea de experți sau organizații care au abilitățile necesare în securitatea cibernetică aplicată pe domenii specifice și critice, precum cel nuclear și radiologic.

Multiple tentative de trafic ilicit cu materiale nucleare și radioactive în arealul bazinului Mării Negre, inclusiv prin Republica Moldova, precum și angajamentele noastre în securitatea regională sunt motive serioase pentru a impune implementarea controlului securității cibernetice la operatorii nucleari și radiologici, precum și pentru a perfecționa procesul de autorizare. Aprobarea Legii nr.132 [31] este a fost un pas important spre îmbunătățirea sistemelor de securitate fizică prin luarea în considerare a chestiunilor de securitate cibernetică. Pe lângă aprobarea de Guvern a cerințelor explicite în securitatea fizică, procedurilor de autorizare [56] care delimitează acțiunile și responsabilitățile reglementatorului și operatorului sunt necesare și alte acțiuni de suport la nivel departamental / ramural, precum și educațional. Implementarea noilor programe universitare, cu tematică din securitatea cibernetică, ar permite ridicarea nivelului de conștientizare a utilizatorilor în rândul personalului relevant în domeniul securității nucleare, precum și reducerea la minimum a riscului factorului uman la utilizarea TI în domeniul nuclear și radiologic. Dezvoltarea continuă a capacității CNSSN UTM de a desfășura cursuri de formare, precum și de

a sprijini organismul de reglementare, precum și operatorii în creșterea gradului de conștientizare ar contribui la minimizarea decalajului în acest domeniu în autoritățile publice responsabile de domeniile nuclear și radiologic. Cooperarea internațională în domeniu și schimbul de date va asigura un nivel ridicat de securitate cibernetică. Există multiple modalități de cooperare la nivel internațional cu alte organizații din domeniul securității cibernetice. Acestea pot fi prin intermediul organizațiilor naționale care sunt specializate în securitatea TI și au stabilit acorduri de schimb de informații, cum ar fi cu privire la date despre amenințări sau cursuri comune, precum și, de exemplu, prin intermediul Organismului de reglementare care are o cooperare foarte bună cu AIEA și alte organisme similare din străinătate, dacă vorbim de domeniul nuclear și radiologic. În ansamblu, integrarea sistemelor informatice în tehnologiile utilizate în domeniul nuclear și radiologic, necesită un plan cuprinzător de acțiuni în domeniul securității informatice, începând de la formarea de conștientizare a utilizatorilor de bază, până la formarea de specialitate pentru practicieni și operatorii nucleari și radiologici. Actualmente acest lucru poate fi realizat de către instituția de reglementare doar cu sprijin extern, cum ar fi din partea organizațiilor de suport tehnic-științific, de exemplu al CNSSC, precum și din partea partenerilor externi care au stabilit deja un plan educațional în acest domeniu.

Dezvoltarea programelor de securitate cibernetică este un proces continuu care necesită o abordare complexă. Cadrul legal de securitate cibernetică din Republica Moldova a înregistrat un ciclu de dezvoltare pozitiv și este actualizat în mod regulat în conformitate cu îndrumările internaționale, recomandările sau peisajul amenințărilor. Acest fapt a fost reflectat și în cea mai recentă Evaluare a pregătirii digitale realizată de Programul Națiunilor Unite pentru Dezvoltare , bazată pe algoritmi și proceduri proprii [183]. Pot fi aplicate diferite metode de evaluare a progresului și a priorităților, cum ar fi prin evaluări externe care analizează anumiți indicatori [184] sau modele practice. Cercetările efectuate rezultate cu aplicarea metodologiei practice de evaluare propusă în Model [185, 186] a identificat anumite constatări în legătură cu foaia de parcurs de dezvoltare a securității cibernetice la nivel național care are un impact direct asupra domeniului IC. Aceasta înseamnă că în Republica Moldova cadrul legislativ actual poate fi suficient pentru a ajuta la îmbunătățirea și dezvoltarea celorlalte dimensiuni conform modelului. Cu toate acestea, securitatea cibernetică fiind un proces continuu necesită adaptări dinamicii de amenințări, bunelor practici, precum și evoluțiilor programelor naționale de securitate cibernetică. De exemplu, un ghid de implementare publicat recent de AIEA abordează integrarea securității informatice pentru securitatea nucleară. Acest ghid specific acoperă în mod explicit dezvoltarea securității cibernetice ca parte a securității nucleare la nivel național. Prin urmare, deși securitatea cibernetică poate fi îmbunătățită și derivată din reglementările naționale, există încă anumite domenii IC, cum ar fi cel

nuclear, care necesită o atenție suplimentară. Acest lucru, pe de altă parte, este benefic și pentru țară, deoarece poate servi drept exemplu pentru dezvoltarea de concepte și strategii pentru alte domenii, cum ar fi asistența medicală. Necesitatea actualizării continue a cadrului legal de securitate cibernetică a fost evidențiată și de organizațiile internaționale, pe baza unui cadru comun de evaluare aplicat la nivel mondial [183]. Adițional, o evaluare a unor indici a nivelului de dezvoltare a securității informației din Republica Moldova pentru tot tipul de organizații relevă rezultate similare, în care domeniul este în curs de dezvoltare [184].

O altă latură a evoluțiilor în securitatea cibernetică este oferită și de modelele de maturitate de utilizare. Aceste model reprezintă o colecție de practici bune de securitate și controale pe care organizațiile trebuie să le urmeze. În timp ce unele modele sau standarde, cum ar fi ISO 27001, sunt adoptate de majoritatea întreprinderilor, alte modele sunt destinate în mod special organizațiilor IC din sectorul energiei, apărării sau din alte sectoare. Exemple de astfel de modele sunt cele de la NIST – *Cybersecurity Framework, Cybersecurity Capability Maturity Model* și altele. Aceste modele au diverse similitudini: acestea sunt dezvoltate prin cooperare între mai multe entități, urmează un proces de îmbunătățire continuu în raport cu mediul de amenințare, și au tendința de simplificare și agregare a controalelor. Modelul propus în această lucrare are proprietăți similare și este aliniat cu tendințele actuale în ceea ce privește nivelurile de maturitate [188].

3.4. Concluzii la capitolul III

Capitolul reflectă rezultatele evaluării cuprinzătoare a conceptului de SSD propus, modul în care un SSD este perceput de către utilizatorii finali, eficiența acestuia precum și modul în care SSD poate fi aplicat în scenarii reale. A fost prezentat un model de evaluare a maturității securității cibernetice, care este ușor de citit și înțeles și poate fi adaptat la cerințele oricărei organizații din domeniul IC. Acest model ameliorează procesul de luare a deciziilor în managementul riscurilor cibernetice și identifică zonele care necesită atenție pentru a crește nivelul de maturitate. Modelul este multidimensional și poate fi aplicat atât pentru a evalua eficiența SSD din punct de vedere tehnologic cât și al dimensiunii umane. De asemenea, modelul servește ca bază pentru algoritmii sau funcțiile dezvoltate ulterior în cadrul conceptului de SSD propus. A fost elaborată în premieră Baza de cunoștințe „Securitatea cibernetică în infrastructuri critice”, sistemul formal metric inteligent „Securitatea cibernetică în infrastructuri critice” și a fost elaborat prototipul aplicației „Securitatea cibernetică în infrastructuri critice”.

A fost evaluată starea securității cibernetice în domeniul sănătății, proces ce a permis identificarea tipurilor comune de atacuri împotriva dispozitivelor din medicină, impactul negativ

și rolul pe care dimensiunea umană îl are în acest aspect, precum și cerințele legale pentru a proteja astfel de sisteme împotriva atacurilor cibernetice. Au fost prezentate recomandări și propuneri în termeni de controale tehnice și bune practici de securitate, cât și pe partea de politică și management, cu privire la modul de îmbunătățire a cooperării în acest domeniu, atât la nivel național, cât și internațional.

În continuare, sunt prezentate rezultatele multiplelor analize efectuate în domeniul securității nucleare și radiologice în Republica Moldova. Este descrisă o evoluție cronologică a cadrului juridic nuclear și radiologic și modul în care rolul și atenția acordată securității cibernetice a crescut în timp. De asemenea, a fost evaluat modul în care legislația națională în domeniul securității cibernetice a afectat domeniul IC și în special pe cel nuclear și radiologic. De asemenea, s-au propus recomandări cu privire la îmbunătățirea cadrului legal, a cooperării naționale, a schimbului de expertiză la nivel orizontal, precum și a programului general de securitate cibernetică. Constatările sunt aliniate cu modelul propus anterior și confirmă aplicabilitatea și autenticitatea acestuia.

Ulterior au fost prezentate rezultatele aplicării modelului la evoluțiile din domeniul nuclear și radiologic, precum și al asistenței medicale. Acestea se confirmă cu avize pozitive de la organizații din domenii, cât și un drept de autor înregistrat la AGEPI privind sistemul formal metric inteligent. Rezultatele obținute confirmă valabilitatea modelului, precum și căile comune privind dezvoltarea programului de securitate cibernetică la nivel național. Politicile și managementul, precum și conștientizarea riscurilor cibernetice, se numără printre factorii inițiali care conduc la dezvoltarea unui program de securitate. Modelul aplicat permite monitorizarea dezvoltării și corijării celorlalte dimensiuni, precum instruirea și managementul riscurilor cibernetice, corespunderea cadrului normativ în dinamica schimbărilor, bunelor practici terților operatori naționali și internaționali.

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 gestionarea 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 (Subcapitolul 2.1). 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 (Subcapitolul 2.2). A fost propusă și argumentată dezvoltarea SSD ca modul, pentru a spori eficiența costurilor și rata de implementare (Subcapitolul 2.3). A fost identificată, ca necesitate critică evaluarea factorului uman în timpul proiectării, dezvoltării și utilizării SSD (Subcapitolul 2.4).

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 (Subcapitolul 2.4). 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 (Subcapitolul 2.2, 2.3, 2.4). 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 (Subcapitolul 2.3). 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 (Subcapitolul 2.4). Ca o soluție pentru a depăși limitările cunoscute cauzate de elementele factorului uman precum percepția, abilitățile, capacitatea de a lua decizii corecte atunci 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 (Subcapitolul 2.4).

3. **A fost dezvoltat un model de evaluare a maturității securității cibernetice** care a demonstrat aplicabilitate și eficiență pentru diferite tipuri de IC (Subcapitolul 3.1). 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 evaluat de organizații externe (Anexa 2, Anexa 3, Anexa 4 și Anexa 5), 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” de la Universitatea Tehnică a Moldovei (Anexa 5). În premieră a fost dezvoltată Baza de cunoștințe „Securitatea cibernetică în infrastructuri critice” (Anexa 1), 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” (Secțiunea 3.1.2, 3.1.3, Anexa 7). 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 (Subcapitolul 1.5, 3.2), 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 (Subcapitolul 3.3).

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 elementele de securitate cibernetică în evaluarea sistemelor de securitate fizică (Subcapitolul 1.5). A fost realizată o analiză cronologică a rolului și atenției securității cibernetice în cadrul legislativ nuclear și radiologic. Securitatea cibernetică în domeniul medicinii a fost evaluată dintr-o prezentare generală la nivel înalt (Subcapitolul 3.2). Ca urmare, au fost identificate vulnerabilități comune împotriva sistemelor din medicină, precum și limitările legate de elementele factorului uman (Subcapitolul 3.2). Au fost propuse recomandări din perspectiva controalelor tehnice care trebuie implementate, precum și pe partea de politici și management pentru a îmbunătăți cooperarea orizontală atât la nivel național, cât și internațional. Au fost de asemenea prezentate tendințele pe care organizațiile le urmează în procesul de creștere a nivelului de maturitate a securității cibernetice (Subcapitolul 3.3).

Recomandări de cercetări viitoare

Deși cercetarea s-a axat pe utilizarea SSD în IC, s-a observat că această întrebare 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 ce ameliorează managementul riscurilor în IC;
- Perfecționarea cadrului legislativ a securității cibernetice în domeniul medicinii și analiza eficienței modelului propus pentru țări sau regiuni selectate;
- Implementarea controalelor de securitate integrate.

BIBLIOGRAFIE

1. Hotărârea Guvernului nr. 811 din 29.10.2015 - *privind Programul Național de Securitate Cibernetică al Republicii Moldova pentru anii 2016-2020*, Monitorul Oficial al Republicii Moldova, nr. 306-310 din 13.11.2015.
2. Comisia Europeană 2020, *Comunicare comună către Parlamentul European și Consiliu - Strategia UE de securitate cibernetică pentru deceniul digital*, JOIN/2020/ 18, accesat la data de 3 august 2021, [Online] la adresa https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=JOIN:2020:18:FIN.
3. Comisia Europeană 2020, *Propunere de directivă a Parlamentului European și a Consiliului privind reziliența entităților critice*, COM(2020) 829 final, 2020 accesat la data de 3 august 2021, [Online] la adresa https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN .
4. 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 data de 20 martie 2020.
5. ONU 2021, *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security* (A/76/135), accesat la data de 20 July 2021.
6. BONGIORNI, L. *How Threat Modeling Can Influence ICS Security Posture*, retrieved from: https://ics.kaspersky.com/media/ics-conference-2019/01-Luca-Bongiorni-How-Threat-Modeling-can-Influence-ICS-Security-Posture.pdf.
7. Agenția Europeană pentru Medicamente 2018, *Data anonymization - a key enabler for clinical data sharing*, [Workshop report], 2018, accesat la data de 3 august 2021, [Online] la adresa https://www.ema.europa.eu/en/documents/report/report-data-anonymisation-key-enabler-clinical-data-sharing_en.pdf, pp 14-15.
8. ENISA 2020, *ENISA Threat Landscape 2020*, accesat la data de 3 august 2021, [Online] la adresa https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport.
9. The Guardian 2020, *Prosecutors open homicide case after cyber-attack on German hospital*, accesat la data de 3 august 2021, [Online] la adresa https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital.
10. The Guardian 2020, *Shocking' hack of psychotherapy records in Finland affects thousands*, accesat la data de 3 august 2021, [Online] la adresa https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland.
11. VERIZON - 2021 Data Breach Investigations Report, 2021.
12. Fișa Disciplinei Securitatea Nucleară și Radiologică, Universitatea Tehnică din Moldova, [Online] la adresa: http://mib.utm.md/files/master_mn_program/SNR.pdf.
13. Comisia Europeană 2004, Comunicarea Comisiei către Consiliu și Parlamentul European - Protecția infrastructurii critice în lupta împotriva terorismului /* COM/2004/0702 final */. 2004. accesat la data de 3 august 2021, [Online] la adresa https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52004DC0702&from=EN.
14. Cybersecurity and Infrastructure Security Agency 2020, accesat la data de 3 august 2021, [Online] la adresa https://www.cisa.gov/critical-infrastructure-sectors.
15. Government of Canada 2020, *National strategy for critical infrastructure*, 2020, accesat la data de 3 august 2021, [Online] la adresa https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

16. BUCOVETSCHI, O., GEORGESCU, A., LAZAR, M., CIRNU, C. (2018) *Securitatea națională a României în contextul infrastructurilor critice spațiale*, Revista Română de Informatică și Automatică (Romanian Journal of Information Technology and Automatic Control), ISSN 1220-1758, Vol. 28, No. 4, pp. 31-40.
17. Merriam-Webster, Merriam-Webster.com Dictionary, accesat la data de 3 august 2021, [Online] la adresa https://www.merriam-webster.com/dictionary/cybersecurity.
18. WILLIAMS, T.J., *The Purdue Enterprise Reference Architecture*, IFAC Proceedings Volumes, Volume 26, Issue 2, Part 4, 1993, pp 559-564, ISSN 1474-6670, DOI:10.1016/S1474-6670(17)48532-6.
19. Comisia Europeană 2021, *Privire de ansamblu asupra riscurilor dezastrelor naturale și provocate de om cu care se poate confrunta Uniunea Europeană*, accesat la data de 3 august 2021, [Online] la adresa https://ec.europa.eu/echo/sites/default/files/overview_of_natural_and_man-made_disaster_risks_the_european_union_may_face.pdf.
20. Healthcare Information and Management Systems Society 2019, *HIMSS Cybersecurity Survey*, accesat la data de 3 august 2021, [Online] la adresa https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf.
21. Deloitte 2013. *Networked medical device cybersecurity and patient safety: Perspectives of healthcare information cybersecurity executives*. accesat la data de 3 august 2021, [Online] la adresa https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf.
22. Siemens 2019, *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?* accesat la data de 3 august 2021, [Online] la adresa https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf.
23. ICS-CERT 2021, *ICS-ALERT-14-281-01B*, accesat la data de 3 august 2021, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.
24. CERNEI, V., *Models and methods for governamental cyber risk management*. In: The Collection. Economic security in the context of sustenable development. Ediția 6, 10 dec 2021, Universitatea de Stat „Alecu Russo" din Bălți, 2021, pp. 258-261. ISBN 978-9975-155-01-4.
25. HEMSLEY, K., FISHER, R. *History of Industrial Control System Cyber Incidents*, Idaho National Laboratory, 2018. [Online] la adresa https://www.osti.gov/servlets/purl/1505628
26. Defense Science Board 2017, *Report of Defense Science Board Task Force on Cyber Deterrence*,. accesat la data de 3 august 2021, [Online] la adresa https://fas.org/irp/agency/dod/dsb/cyber-deter.pdf.
27. NIST 2018, *Risk Management Framework for Information Systems and Organizations*, NIST Special Publication 800-37, DOI:10.6028/NIST.SP.800-37r2.
28. FILIP, F. G., SUDUC, A.-M., BÎZOI, M. *DSS in numbers*. Technological and Economic Development of Economy, 20(1), 154-164, 2014, DOI:10.3846/20294913.2014.890139.
29. ŢURCANU, D., SPINU, N., POPOVICI, S., ȚURCANU, T. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. In: Journal of Social Sciences. 2021, nr. 4(1), pp. 74-83. ISSN 2587-3490.10.52326/jss.utm.2021.4(1).10.
30. Hotărârea Guvernului nr. 201 din 28.03.2017 – *privind Aprobarea cerințelor minime de securitate pentru asigurarea securității cibernetice a sistemelor informatice, hardware și software*. Monitorul Oficial al Republicii Moldova nr.109-118 din 07.04.2017.
31. Legea nr. 132 din 08.06.2012 *privind desfășurarea în siguranță a activității nucleare și radiologice,* Monitorul Oficial al Republicii Moldova nr.229-233 din 02.11.2012.

32. AIEA 2011, *Nuclear Security Series No.13: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*, Vienna, accesat la data de 3 august 2021, [Online] la adresa https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.
33. AIEA 2011b, *Nuclear Security Series No.17-T: Computer Security at Nuclear Facilities*, Vienna accesat la data de 3 august 2021, [Online] la adresa https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf.
34. AIEA 2021, Nuclear Security Series No. 42-G: *Computer Security for Nuclear Security*, Vienna, accesat la data de 3 august 2021, [Online] la adresa https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.
35. Ministerul Economiei și Infrastructurii, *Ordin nr. 402 din 28 decembrie 2017 privind aprobarea politicii interne de Securitate cibernetică a Ministerului Economiei și Infrastructurii*, accesat la data de 3 august 2021, [Online] la adresa http://mei.gov.md/ro/content/ordinul-nr402-din-28122017-cu-privire-la-aprobarea-politicii-interne-privind-securitatea-1.
36. ISO 2018, *Information technology - Security techniques - Information security management systems* - Overview and vocabulary, accesat la data de 3 august 2021, [Online] la adresa https://www.iso.org/standard/73906.html.
37. Legea nr. 299 din 21.12.2017 *privind aprobarea conceptului de securitate a informațiilor al Republicii Moldova,* Monitorul Oficial al Republicii Moldova nr.48-57 din 16.02.2018.
38. Legea nr. 257 din 22.11.2018 *privind aprobarea Strategiei de securitate a informațiilor a Republicii Moldova pentru anii 2019-2024*, Monitorul Oficial al Republicii Moldova nr.13-21 din 18.01.2019.
39. ISO 2009, ISO GUIDE 73:2009 *Risk management - Vocabulary*, accesat la data de 3 august 2021, [Online] la adresa https://www.iso.org/standard/44651.html.
40. RAATIKAINEN, P. "Gödel's Incompleteness Theorems", The Stanford Encyclopedia of Philosophy (Spring 2022 Edition), Edward N. Zalta (ed.).
41. FILIP, F.G., *Decision support and control for large-scale complex systems*, Annual Reviews in Control. 32. 61–70. 10.1016/j.arcontrol.2008.03.002., 2008.
42. GEERTMAN, S., STILLWELL, J., *Planning Support Systems: An Introduction*. In: Geertman S., Stillwell J. (eds) Planning Support Systems in Practice. Advances in Spatial Science. Springer, Berlin, Heidelberg, 2003.
43. DELDEN, H., LUJA, P., ENGELEN, G. *Integration of multi-scale dynamic spatial models of socio-economic and physical processes for river basin management,* Environmental Modelling & Software, Volume 22, Issue 2, 2007, pp 223-238 , ISSN 1364-8152, DOI:10.1016/j.envsoft.2005.07.019.
44. 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.
45. CĂPĂŢÂNĂ, Gh.: *Tehnologii informaționale inteligente*. In: Fizica și Tehnologiile Moderne. nr. 3(3), pp. 9-13. ISSN 1810-6498, (2003), accesat la data de 3 august 2021, https://ibn.idsi.md/sites/default/files/imag_file/Tehnologii%20informationale%20inteligente.pdf.
46. AVERKIN A., HAAZE-RAPOPORT M., POSPELOV D. *Explanatory Dictionary of Artificial Intelligence*. – ed. Radio and communications (in Russian) http://www.raai.org/library/tolk/ (1992).
47. CĂPĂŢÂNĂ, Gh., *Software Applications Oriented to Families of Problems*. In: Information Technologies, Systems and Networks. Volumul 1, 17-18 octombrie 2017, Chișinău. Chișinău: Editura ULIM, 2017, pp. 24-29. ISBN 978-9975-45-069-0.

48. FILIP, F.G.: *Sisteme suport pentru decizii ("Decision Support Systems"),* 2nd Edition, Editura Tehnică, București (in Romanian), (2007).
49. FILIP, F.G., *A decision-making perspective for designing and building information systems*, International Journal of Computers Communications & Control, Volume 7-2, pp 264-272 (2012).
50. HOLSAPPLE, C.: *DSS Architecture and Types*. In: Handbook on Decision Support Systems 1. International Handbooks Information System. Springer, Berlin, Heidelberg. DOI:10.1007/978-3-540-48713-5_9, (2008).
51. POWER, D. J.: *Decision Support Systems: Concepts and Resources for Managers*. Faculty Book Gallery. 67. [Online] la adresa https://scholarworks.uni.edu/facbook/67 (2002).
52. Hotărârea Guvernului nr. 153 din 28.02.2014 *pentru aprobarea Regulamentului privind controlul şi supravegherea de stat a activităţilor nucleare, radiologice şi a regimului de neproliferare a armelor nucleare,* Publicat: 21.03.2014 în Monitorul Oficial Nr. 66-71 art Nr : 195.
53. CrowdStrike 2013, *Global Threat Report 2013 Year In Review*, accesat la data de 3 august 2021, [Online] la adresa https://icscsi.org/library/Documents/Threat_Intelligence/CrowdStrike%20-%20Global%20Threat%20Report%202013.pdf.
54. Hotărârea Guvernului nr. 1017 din 01.09.2008 *cu privire la Registrul naţional al surselor de radiaţii ionizante şi al persoanelor fizice şi persoanelor juridice autorizate*, Publicat : 09-09-2008 în Monitorul Oficial Nr. 169-170 art. 102.
55. Hotărârea Guvernului nr. 727 din 08.09.2014 *Autorizarea activităţilor nucleare şi radiologice* Publicat : 12.09.2014 în Monitorul Oficial Nr. 270-274 art Nr : 778.
56. Hotărârea Guvernului nr. 1268 din 23.11.2016 - *privind Regulamentul privind securitatea fizică a activității nucleare și radiologice*. Monitorul Oficial al Republicii Moldova nr. 415 din 29.11.2016.
57. CrowdStrike 2021, *Global Threat Intel Report 2021,* accesat la data de 3 august 2021, [Online] la adresa https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf.
58. Trend Micro 2013, *The SCADA That Didn't Cry Wolf*, accesat la data de 3 august 2021, [Online] la adresa http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-scada-that-didnt-cry-wolf.pdf.
59. NRC 2021, *Regulation 10 CFR*, accesat la data de 3 august 2021, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html.
60. Hotărârea Guvernului nr. 434 din 16.07.2015 *pentru aprobarea Regulamentului cu privire la transportarea în siguranţă a materialelor radioactive* Publicat : 24.07.2015 în Monitorul Oficial Nr. 190-196 art Nr : 491, MODIFICAT HG1143 din 21.11.18, MO13-21/18.01.19 art.7; în vigoare 18.01.19.
61. AIEA 2015, *Nuclear Security Series No. 23-G: Security of Nuclear Information*, Vienna, accesat la data de 3 august 2021, [Online] la adresa https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf.
62. **BUZDUGAN, A**; BUZDUGAN, Ar. *The interplay between cyber and nuclear security in Republic of Moldova*. In: Microelectronics and Computer Science Ediția 9, 19-21 octombrie 2017, Chișinău, Rep. Moldova: Universitatea Tehnică a Moldovei, 2017, pp. 382-385. ISBN 978-9975-4264-8-0.
63. BUZDUGAN, Ar., **BUZDUGAN, A**., (2020) *Revision of the Curriculum on Nuclear Safety and Security in the Light of Recent International Recommendations*. In: Tiginyanu I., Sontea V., Railean S. (eds) 4th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2019. IFMBE Proceedings, vol 77, pp.815-819, Springer Nature Switzerland AG 2020, DOI:10.1007/978-3-030-31866-6_145.

64. BUZDUGAN, AR., **BUZDUGAN, A**., *Converging knowledge and Technology Role in University's Non-Proliferation Culture*. SnT 2021. CTBT Science and Technology Conference, 28 June – 02 July 2021. Vienna, Austria, (2021), accesat la data de 26 septembrii 2021, [Online] la adresa https://conferences.ctbto.org/event/7/book-of-abstracts.pdf.
65. BUZDUGAN, AR., RAILEAN, S., **BUZDUGAN, A**., *Nanotechnology and Nonproliferation*, 5th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME-2021, November 3-5, 2021, Chisinau, Republic of Moldova, Program and Abstract Book, S5-1.9, ISBN 978-9975-72-592-7, pp. 122 (2021).
66. BUZDUGAN, AR., RAILEAN, S., **BUZDUGAN, A**., *Nanotechnology and Nonproliferation*, 5th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME-2021, November 3-5, 2021, Chisinau, Republic of Moldova, IFMBE Proceedings, pp. 463-469, vol 87. Springer, Springer Nature Switzerland, (2022), doi:10.1007/978-3-030-92328-0.
67. **BUZDUGAN, A**., BUZDUGAN, Ar. *The Synergy Between Cyber and Nuclear Security. Case Study of Moldova.* In: Sidorenko A., Hahn H. (eds) Functional Nanostructures and Sensors for CBRN Defence and Environmental Safety and Security. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht, 2020.
68. **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.
69. BUZDUGAN, Ar., **BUZDUGAN, A**., *Technical and Scientific Support Organizations and Strengthening of Nuclear Regulation (Case study of Moldova),* International Conference on Challenges Faced by Technical and Scientific Support Organizations (TSOs) in Enhancing Nuclear Safety and Security, IAEA-CN-181/15, Japan, 2010.
70. KITCHENHAM, B., STUART, C., *Guidelines for performing Systematic Literature Reviews in Software Engineering.* 2007, Vol. 2.
71. KITCHENHAM, B, PEARL BRERETON, O., BUDGEN, D., TURNER, M, BAILEY, J, Linkman S. *Systematic literature reviews in software engineering – A systematic literature review, Information and Software Technology*, Volume 51, Issue 1, 2009, pp 7-15, DOI:10.1016/j.infsof.2008.09.009.
72. AMANTINI, A., CHORAŚ, M., D'ANTONIO, S., EGOZCUE, E., GERMANUS, D., HUTTER, R., *The human role in tools for improving robustness and resilience of critical infrastructures*. Cognition, Technology and Work, 14(2), 143–155, 2012, DOI:10.1007/s10111-010-0171-2.
73. CHORAŚ, M., KOZIK, R., FLIZIKOWSKI, A., RENK, R., HOŁUBOWICZ, W., *Ontology-based decision support for security management in heterogeneous networks*. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009, 5755 LNAI, 920–927. DOI:10.1007/978-3-642-04020-7_99.
74. CHORAŚ, M., FLIZIKOWSKI, A., KOZIK, R., HOŁUBOWICZ, W., *Decision aid tool and ontology-based reasoning for critical infrastructure vulnerabilities and threats analysis*. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2010a, 6027 LNCS, 98–110. DOI:10.1007/978-3-642-14379-3_9.
75. CHORAŚ, M., KOZIK, R., FLIZIKOWSKI, A., HOŁUBOWICZ, W., *Ontology applied in decision support system for critical infrastructures protection.* Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and

Lecture Notes in Bioinformatics), 2010b, 6096 LNAI (PART 1), 671–680. DOI:10.1007/978-3-642-13022-9_67.
76. SETOLA, R., LUIIJF, E., THEOCHARIDOU, M., *Managing the Complexity of Critical Infrastructures*. In Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach (Vol. 90, Issue Ci)., 2017, DOI:10.1007/978-3-319-51043-9.
77. KOZIK, R., CHORAŚ, M., HOŁUBOWICZ, W., *Fusion of Bayesian and ontology approach applied to decision support system for Critical Infrastructures protection.* Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, 45 LNICST, 451–463. DOI:10.1007/978-3-642-16644-0_39.
78. **BUZDUGAN, A**., (2020) *Review on use of decision support systems in cyber risk management for critical infrastructures*, Journal of Engineering Science Vol. XXVII, no. 3 (2020), pp. 134 - 145 Fascicle-Electronics and Computer, Science Topic-Computers and Information Technology, ISSN 2587-3474, eISSN 2587-3482, DOI:10.5281/zenodo.3949684, UDC 004.056.5.
79. KODUAH, S. T., PRASAD, R., *The Threats of Infrastructure Obsolescence to Smart Grid: A case study*. 2020. DOI:10.1007/s11277-020-07406-y.
80. PANGULURI, S., PHILLIPS, W., CUSIMANO, J., *Protecting water and wastewater infrastructure from cyber attacks*. Frontiers of Earth Science, 2011, 5(4), DOI:10.1007/s11707-011-0199-5.
81. DI CRISTO, C., LEOPARDI, A., DE MARINIS, G., *Water infrastructure protection against intentional attacks: An experience in Italy*. Frontiers of Earth Science, 2011, 5(4), 390–399. DOI:10.1007/s11707-011-0208-8.
82. VAMVAKERIDOU-LYROUDIA, L. S., CHEN, A. S., KHOURY, M., GIBSON, M. J., KOSTARIDIS, A., STEWART, D., WOOD, M., DJORDJEVIC, S., SAVIC, D. A., *Assessing and visualizing hazard impacts to enhance the resilience of Critical Infrastructures to urban flooding*. Science of the Total Environment, 2020, 707, 136078, DOI:10.1016/j.scitotenv.2019.136078.
83. ENESCU, F. M., BIZON, N., *SCADA applications for electric power system*. In Power Systems. 2017, DOI:10.1007/978-3-319-51118-4_15.
84. TSAI, F. S., CHAN, K. L., *Blog data mining for cyber security threats*. Data Mining for Business Applications, 2009, 169–182. DOI:10.1007/978-0-387-79420-4_12.
85. SA, C., HUTCHISON, D., *Theory and Models for Cyber Situation Awareness State-of-the-Art*. 2017, Vol 4, 3–25. DOI:10.1007/978-3-319-61152-5.
86. HELIL, A., GERMANUS, D., SURI, N., *Protection of SCADA communication channels.* Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2012, 7130, 177–196. DOI:10.1007/978-3-642-28920-0_9.
87. MOTZEK, A., MÖLLER, R., *Context- and bias-free probabilistic mission impact assessment.* Computers and Security, 2017, 65, 166–186. DOI:10.1016/j.cose.2016.11.005
88. STAVROULAKIS, P., KOLISNYK, M., KHARCHENKO, V., DOUKAS, N., MARKOVSKYI, O. P., BARDIS, N. G., *Reliability, fault tolerance and other critical components for survivability in information warfare.* In Communications in Computer and Information Science (Vol. 990), 2019, Springer International Publishing. DOI:10.1007/978-3-030-11039-0_17.
89. HICKFORD, A. J., BLAINEY, S. P., ORTEGA HORTELANO, A., PANT, R., *Resilience engineering: theory and practice in interdependent infrastructure systems*. Environment Systems and Decisions, 2018, 38(3), 278–291. DOI:10.1007/s10669-018-9707-4.

90. ANI, D.A., JEREMY, D.M., WATSON, J.R., NURSE, J., COOK, A., MAPLE, C. (2019). *A Review of Critical Infrastructure Protection Approaches: Improving Security through Responsiveness to the Dynamic Modelling Landscape.*
91. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh.: *Factors for a decision support system in critical infrastructure cyber risk management*, Romanian Cyber Security Journal, ISSN 2668-6430, ISSN-L 2668-1730, Vol 2(2), Pg.67-73 (2020).
92. NIST 2016, NIST Special Publication 800-160, *Systems Security Engineering,* accesat la data de 3 august 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf.
93. ELLERBY, Z., Mcculloch J., WILSON, M., WAGNER, C. (2019). *Exploring how Component Factors and their Uncertainty Affect Judgements of Risk in Cyber-Security*. accesat la data de 3 august 2021, [Online] la adresa https://www.researchgate.net/publication/336230531_Exploring_how_Component_Factors_and_their_Uncertainty_Affect_Judgements_of_Risk_in_Cyber-Security.
94. Centrul Comun de Cercetare al Comisiei Europene Institutul pentru Protecția și Securitatea Cetățeanului 2012. *Metodologii de evaluare a riscurilor pentru Protecția Infrastructurii Critice*. Partea I: Un stadiu al tehnicii, accesat la data de 3 august 2021, [Online] la adresa https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf.
95. Centrul Comun de Cercetare al Comisiei Europene Institutul pentru Protecția și Securitatea Cetățeanului 2015. *Metodologii de evaluare a riscurilor pentru protecția infrastructurii critice. Partea II: O nouă abordare*, accesat la data de 3 august 2021, [Online] la adresa https://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf.
96. ALCARAZ, C., ZEADALLY, S. (2015). *Critical infrastructure protection: Requirements and challenges for the 21st century*. International Journal of Critical Infrastructure Protection. 8. 53-66.
97. OUYANG, M. (2014). *Review on modeling and simulation of interdependent critical infrastructure systems.* Reliability Engineering and System Safety, Elsevier, vol. 121(C), pages 43-60. doi: 10.1016/j.ress.2013.06.040.
98. RABE, M., ANGEL A.J, NAVONIL, M, ANDERS, S, SHEFALI, J., BIRGER, J. (2018). *Cyber risk of coordinated attacks in critical infrastructures.* accesat la data de 20 martie 2020 [Online] la adresa https://pdfs.semanticscholar.org/0d49/8506ff4d764f87e9770827227db62acb1a14.pdf.
99. FIELDER, A., PANAOUSIS, E., MALACARIA, P., HANKIN, C., SMERALDI, F.: *Decision support approaches for cyber security investment*, Decision Support Systems, Volume 86, pp. 13-23, ISSN 0167-9236, DOI:10.1016/j.dss.2016.02.012 (2016).
100. KÖNIG, S., RASS, S., SCHAUER, S. (2019). *Cyber-attack impact estimation for a port*. In: Jahn, Carlos Kersten, Wolfgang Ringle, Christian M. (Ed.): Digital Transformation in Maritime and City Logistics: Smart Solutions for Logistics. Proceedings of the Hamburg International Conference of Logistics, Vol. 28, ISBN 978-3-7502-4949-3, pp. 164-183.
101. CHORAŚ M., KOZIK R., FLIZIKOWSKI A., HOŁUBOWICZ W., RENK R. (2016). *Cyber Threats Impacting Critical Infrastructures*. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds) Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control, vol 90. Springer, Cham. doi:10.1007/978-3-319-51043-9_7.
102. MITRE 2020, ATT*&CK® for Industrial Control Systems*, accesat la data de 3 august 2021, [Online] la adresa https://collaborate.mitre.org/attackics/index.php/Main_Page
103. ALEXANDER, O., BELISLE, M., STEELE, J.: *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy* (2020).

104. FireEye 2019, TRITO*N Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping*, accesat la data de 3 august 2021, [Online] la adresa https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html.
105. MITRE 2020, *CVE Numbering Authority Rules*, accesat la data de 3 august 2021, https://cve.mitre.org/cve/cna/rules.html#section_8-1_cve_entry_information_requirements.
106. **BUZDUGAN, A**., BUZDUGAN Ar., *Advances in security requirements for high-risk object*s, IAEA International Conference on Nuclear Security (ICP presentation), 2016b.
107. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh. (2020) *Architecture Considerations for a Decision Support System in Cyber Risk Management*. 9th International Workshop on Soft Computing Applications (SOFA 2020), Arad, Romania (in press).
108. FILIP, F.G., ZAMFIRESCU, C. B., CIUREA, C. (2017) *Computer-Supported Collaborative Decision-Making Series*: Automation, Collaboration, & E-Services, Volume 4, Springer, 216 pp. DOI: 10.1007/978-3-319-47221-8.
109. **BUZDUGAN, A**. *Adequate domain-based security* [abstract], (2019) In: Book of Abstracts -Vienna Cyber Security Week 2019 - Protecting Critical Infrastructure. Vienna, Austria.
110. NIXON, J., MCGUINNESS, B.: *Framing the Human Dimension in Cybersecurity*. Transactions on Security and Safety. 13. e2. 10.4108/trans.sesa.01-06.2013.e2. (2013).
111. KHRIPUNOV, I.(eds): *The Human Dimension of Security for Radioactive Sources: From Awareness to Culture.* Center for International Trade and Security, University of Georgia, Indonesia's National Nuclear Energy Agency (2014).
112. ISO 2019, *Ergonomics of human-system interaction*, accesat la data de 3 august 2021, https://www.iso.org/standard/77520.html.
113. SCHEPERS, J., WETZELS, M. (2007) *A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects*. Information and Management, 44(1): 90-103.
114. VENKATESH, V., BROWN, S. (2001) *A longitudinal investigation of personal computers in homes: Adoption determinants and emerging challenges*. MIS Quarterly, 25(1): 71-102.
115. KIM, J., FORSYTHE, S. (2008) *Sensory enabling technology acceptance model (se-tam): A multiple-group structural model comparison.* Psychology and Marketing, 25(9): 901-922.
116. LIN, C., SHIH, H., SHER, P. (2007) *Integrating technology readiness into technology acceptance: The tram model.* Psychology and Marketing, 24(7): 641-657.
117. BOSSOMAIER, T., D'ALESSANDRO, S., BRADBURY, R. (2019) *Human dimensions of cybersecurity*. (1st ed.) Taylor & Francis.
118. LEGRIS, P., INGHAM, J., COLLERETTE, P. (2003). *Why do people use information technology? A critical review of the technology acceptance model*. Information and Management, 40(3): 191-204. DOI:10.1016/S0378-7206(01)00143-4.
119. HUIGANG, L., YAJIONG, X. (2010) *Understanding security behaviors in personal computer usage: A threat avoidance perspective.* Journal of the Association for Information Systems, 11(7):394-413.
120. PARASURAMAN, R., SHERIDAN, T. B., WICKENS, C. D., (2000) *A model for types and levels of human interactions with automation*. IEEE Transactions on Systems, Man and Cybernetics-Part A: Systems and Humans, 30: 286-297.
121. PEW, R. W., MAVOR, A. S. (2007) *Human-System Integration in the System Development Process:* A New Look. Washington, DC: National Academies Press.

122. BOYCE, M.W., MUSE-DUMA, K., HETTINGER, L.J., MALONE, T.B., WILSON, D.P., LOCKETT-REYNOLDS, J., (2011) *Human performance in cybersecurity: A research agenda*. In Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting.
123. WILDING, R., (2007) *Insiders are the biggest enemy*, Strategic Risk.
124. ANTHONY, M., BOARDMAN, M. (2016) *Human Factors Integration (HFI): The Means of Considering the Human Component of Capability within Acquisition*, [Online] la adresa https://www.incose.org/docs/default-source/default-document-library/incose-hsi_mod2_oct2016.pdf?sfvrsn=b53d8ec6_0.
125. BETSCH T., HABERSTROH S., MOLTER B., GLOCKNER A. (2004). *Oops, I did it again - relapse errors in routinized decision making*, Organizational Behavior and Human Decision Processes, Vol 93-1, pp 62-74, DOI:10.1016/j.obhdp.2003.09.002.
126. VEVERA, A.V., ALBESCU, A.R. (2018) *Factorul uman vs. securitatea cibernetică*, Revista Română de Informatică şi Automatică (Romanian Journal of Information Technology and Automatic Control), ISSN 1220-1758, Vol. 28, No. 4, 67-74.
127. SYMONS, S., FRANCE, M., BELL, J., BENNETT, W. (2006) *Linking Knowledge and Skills to Mission Essential Competency-Based Syllabus Development for Distributed Mission Operations*. Air Force Research Laboratory, Report AFRL-HE-AZ-TR-2006-0041.
128. GEORGESCU, A., VEVERA, A.V., CIRNU, C. (2020) *Cyber as a Transformative Element in the Critical Infrastructure Protection Framework,* Romanian Cyber Security Journal, Vol. 1(2), Pg. 37-44.
129. SAVE, L., FEUERBERG, B., (2012) *Designing human-automation interactions: a new level of automation taxonomy.* In: De Waard D, Brookhuis K, Dehais F, Wickert C, Röttger Manzey, D., Biede, S., Reuzeau, F., Terrier, P. (2007) Human Factors: A View from Integrative Perspective. Proc. HFES Europe Chapter Conference, Toulouse: p. 43-55.
130. SHERIDAN, T.B., VERPLANK, W. (1978) *Human and Computer Control of Undersea Teleoperators.* Man-Machine Systems Laboratory, Dept. of Mechanical Engineering, MIT, Cambridge, MA.
131. MILES, C., (2020) *ITIL 4 and automation - opening up improvement and transformation*.
132. LEITE, L., ROCHA, C., KON, F., MILOJICIC, D., MEIRELLES, P. (2019) *A Survey of DevOps Concepts and Challenges*. ACM Comput. Surv. 52, 6, Article 127. DOI:10.1145/3359981.
133. SHERIDAN, T. B. (1992) Telerobotics. *Automation and Human Supervisory Control*. MIT Press.
134. GREEN, L., ALEXANDROV, N., BROWN, S., CERRO, J., GUMBERT, C., SOROKACH, M., BURG, C. (2012) *Decision Support Methods and Tools*, 11th AIAA/ISSMO Multidisciplinary Analysis and Optimization Conference, DOI:10.2514/6.2006-7028.
135. FILIP, F.G. (1989) *Creativity and decision support systems*. Studies and Research in Computers and Informatics, 1 (1): 41-49.
136. FILIP, F. G. (1995) *Toward more humanized real-time decision support systems*. In: Camarinha-Matos L, Afsarmanesh H eds, Balanced Automation Systems. Architectures and Design Methods. Chapman & Hall, London: p. 230-240.
137. 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).

138. FILIP, F. G., LEIVISKA, L. *Large-Scale Complex Systems,* In book: Springer Handbook of Automation (pp.619-638). 10.1007/978-3-540-78831-7_36. (2009).
139. **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. https://doi.org/10.1007/978-981-16-8866-9_19.
140. LESZCZYNA, R.: Cybersecurity Controls. In: *Cybersecurity in the Electricity Sector*. Springer, Cham. DOI:10.1007/978-3-030-19538-0_7 (2019).
141. GIACOMELLO, G., PESCAROLI, G.: *Managing Human Factors*. In: Kott A., Linkov I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. DOI:10.1007/978-3-319-77492-3_11 (2019).
142. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh., *Decision support systems for cyber risk management*. Proceedings of the Workshop on Intelligent Information Systems WIIS2020, December 04-05, 2020, Chisinau, Republic of Moldova, (2020).
143. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh., *Impact of Human Dimension upon Decision Support Systems,* Romanian Journal of Information Technology and Automatic Control, Vol. 31, No. 3, 31-44, 2021 (2021).
144. DAVIS, F. *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, 13(3):319–340, (1989).
145. LEDGARD, H., SINGER, A., WHITESIDE, J.: *Directions in human factors for interactive systems.* In: Ledgard H., Singer A., Whiteside J. (eds) Directions in Human Factors for Interactive Systems. Lecture Notes in Computer Science, vol 103. Springer, Berlin, Heidelberg. DOI:10.1007/3-540-10574-3_2 (1981).
146. KRÜCKEBERG, F.: *Human factor aspects in organizations and information systems supporting them.* In: Blaser A., Zoeppritz M. (eds) Enduser Systems and Their Human Factors. IBM 1983. Lecture Notes in Computer Science, vol 150. Springer, Berlin, Heidelberg. DOI:10.1007/3-540-12273-7_20, (1983).
147. ALTAF, A., FAILY, S., DOGAN, H., MYLONAS, A., THRON, E.: *Identifying Safety and Human Factors Issues in Rail Using IRIS and CAIRIS.* In: Katsikas S. et al. (eds) Computer Security. CyberICPS 2019, SECPRE 2019, SPOSE 2019, ADIoT 2019. Lecture Notes in Computer Science, vol 11980. Springer, Cham. DOI:10.1007/978-3-030-42048-2_7 (2020).
148. GHAFIR, I., SALEEM, J., HAMMOUDEH, M. et al.: *Security threats to critical infrastructure: the human factor*. J Supercomput 74, 4986–5002 DOI:10.1007/s11227-018-2337-2 (2018).
149. MUSHI, M., DUTTA, R. *Human Factors in Network Reliability Engineering*. J Netw Syst Manage 26, 686–722. DOI:10.1007/s10922-017-9440-1 (2018).
150. ANDERSON, T., BUSBY, J., GOUGLIDIS, A., HOUGH, K., HUTCHISON, D., ROUNCEFIELD M.: *Human and Organizational Issues for Resilient Communications*. In: Rak J., Hutchison D. (eds) Guide to Disaster-Resilient Communication Networks. Computer Communications and Networks. Springer. DOI:10.1007/978-3-030-44685-7_32 (2020).
151. PADAYACHEE, K.: *Taxonomy of compliant information security behavior*. Comput. Secur. 31(5), 673–680. DOI:10.1016/j.cose.2012.04.004 (2012).
152. WANG, H., LAU, N., GERDES, R.: *Application of Work Domain Analysis for Cybersecurity*. In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science, vol 10292. Springer, Cham. DOI:10.1007/978-3-319-58460-7_27 (2012).
153. GÓRNY, A.: *Human Factor and Ergonomics in Essential Requirements for the Operation of Technical Equipment*. In: Stephanidis C. (eds) HCI International 2014 -

Posters' Extended Abstracts. HCI 2014. Communications in Computer and Information Science, vol 435. Springer, Cham. DOI:10.1007/978-3-319-07854-0_78, (2014).
154. GUVEYI, E., AKTAS, M.S., KALIPSIZ, O.: *Human Factor on Software Quality: A Systematic Literature Review.* In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12252. Springer, Cham. DOI:10.1007/978-3-030-58811-3_65 (2020).
155. POMMERANZ, A., BROEKENS, J., WIGGERS, P. BRINKMAN W-P. JONKER, C.M. *Designing interfaces for explicit preference elicitation: a user-centered investigation of preference representation and elicitation process.* User Model User-Adap Inter 22, 357–397 DOI:10.1007/s11257-011-9116-6 (2012).
156. OREHEK, Š., PETRIČ, G., ŠINIGOJ, J. *Assessing the Human Factor of Cybersecurity: Can Surveys Tell the Truth?*. In: Stephanidis C., Marcus A., Rosenzweig E., Rau PL.P., Moallem A., Rauterberg M. (eds) HCI International 2020 - Late Breaking Papers: User Experience Design and Case Studies. HCII 2020. Lecture Notes in Computer Science, vol 12423. Springer, Cham. DOI:10.1007/978-3-030-60114-0_18 (2020).
157. SCHIEFERDECKER, I. *Responsible Software Engineering*. In: Goericke S. (eds) The Future of Software Quality Assurance. Springer. DOI:10.1007/978-3-030-29509-7_11 (2020).
158. Comisia Europeană 2019, *Ethics Guidelines for Trustworthy* AI, p. 41. Grupul de experți la nivel înalt al Comisiei Europene privind inteligența artificială, Brüssel 2019, accesat la data de 3 august 2021, [Online] la adresa https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
159. **BUZDUGAN, A**., *IT Security as a driver of economics competitiveness*. International conference - SMEs development and innovation: building competitive future of South-Eastern Europe: book of abstracts / International conference, Ohrid, 3-4 October, 2014. - Prilep: Faculty of economy, 2014. – 155 стр.; 23 см ISBN 978-9989-695-55-1, DOI: 10.13140/2.1.4082.4324 (2014).
160. LINKOV, I., KOTT, A. *Fundamental Concepts of Cyber Resilience: Introduction and Overview*. In: Kott A., Linkov I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. DOI:10.1007/978-3-319-77492-3_1 (2019).
161. LINKOV, I., EISENBERG, D. A., BATES, M. E., CHANG, D., CONVERTINO, M., ALLEN, J. H., FLYNN, S. E., SEAGER, T. P.: *Measurable resilience for actionable policy.* Environmental Science and Technology, 47(18), 10108–10110 (2013a).
162. LINKOV, I., EISENBERG, D. A., PLOURDE, K., SEAGER, T. P., ALLEN, J., KOTT, A.: *Resilience metrics for cyber systems.* Environment Systems and Decisions, 33(4), 471–476 (2013b).
163. BUZDUGAN, Ar., **BUZDUGAN, A**.: *The increasing role of TSO in the Moldovan Nuclear and Radiological Infrastructure,* International Conference on Challenges Faced by Technical and Scientific Support Organizations (TSOs) in Enhancing Nuclear Safety and Security, IAEA CN-214, (2014).
164. **BUZDUGAN, A**., BUZDUGAN Ar. *Information Security Development in the Moldovan Nuclear and Radiological Infrastructure,* IAEA International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, 1-5 June, (2015)
165. DUMITRESCU D. *Principiile inteligenţei artificiale*. - Cluj-Napoca, Editura Albastră, 1999. - 289 p.
166. Spatiu metric, accesat la data de 3 august 2021, [Online] la adresa https://math.fandom.com/ro/wiki/Spa%C8%9Biu_metric.
167. Palladog 2019, *python-menu-function*, accesat la data de on 3 august 2021, [Online] la adresa https://github.com/palladog/python-menu-function.

168. Cybersecurity and Infrastructure Security Agency 2021, *ICS Medical Advisory (ICSMA-21-343-01)* accesat la data de 11 decembrie 2021, [Online] la adresa https://www.cisa.gov/uscert/ics/advisories/icsma-21-343-01.
169. Healthcare Information and Management Systems Society 2021, *What are Maturity Models*?, accesat la data de 12 decembrie 2021, [Online] la adresa https://www.himss.org/what-we-do-solutions/digital-health-transformation/maturity-models.
170. IEEE Spectrum 2018, *Healthcare IT Systems: Tempting Targets for Ransomware*, accesat la data de 3 august 2021, [Online] la adresa https://spectrum.ieee.org/riskfactor/computing/it/healthcare-it-systems-tempting-targets-for-ransomware.
171. MIRSKY, Y., MAHLER, T., SHELEF, I., ELOVICI, Y. (2019) CT-GAN: *Malicious Tampering of 3D Medical Imagery using Deep Learning,* accesat la data de 3 august 2021, [Online] la adresa https://www.researchgate.net/publication/330357848_CT-GAN_Malicious_Tampering_of_3D_Medical_Imagery_using_Deep_Learning.
172. ALEMZADEH, H. et al. (2013) *Analysis of safety-critical computer failures in medical devices.* IEEE Security and Privacy (July–Aug. 2013), 14–26, Co-published by the IEEE Computer and Reliability Societies.
173. Comisia Europeană 2019, Com*isia facilitează accesul cetățenilor la datele de sănătate în condiții de securitate transfrontaliere*, [Comunicat de presă], accesat la data de 3 august 2021, [Online] la adresa http://europa.eu/rapid/press-release_IP-19-842_en.htm.
174. RANSFORD, B., KRAMER, D. B., FOO KUNE, D., AUTO DE MEDEIROS, J., YAN, C., XU, W., FU, K. (2017). *Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists*. PACE - Pacing and Clinical Electrophysiology. Blackwell Publishing Inc. DOI:10.1111/pace.13102.
175. MOHAN, A. (2014) *Cyber Security for Personal Medical Devices Internet of Things*, 2014 IEEE International Conference on Distributed Computing in Sensor Systems, Marina Del Rey, CA, 2014, pp. 372-374. DOI:10.1109/DCOSS.2014.49.
176. **BUZDUGAN, A**., *An overview of cybersecurity in the healthcare sector*. In: Telecommunications, Electronics and Informatics. 6, 24-27 mai 2018. Chișinău, Republica Moldova: Tehnica UTM, 2018, pp. 261-262. ISBN 978-9975-45-540-4.
177. Autoritatea Națională pentru Certificare Electronică și Securitate Cibernetică, 2021, Cyber Security in Health Sector, accesat la data de 3 august 2021, [Online] la adresa https://cesk.gov.al/publicAnglisht_html/Publikime/2021/Cybersecurity%20in%20health%20system.pdf.
178. **BUZDUGAN, A**., *Role of Cyber Security along with Nuclear and Radiological Safety in Medicine*. Book of Abstracts. 3rd International Conference of Health Technology Management. Ed. in chief Victor Sontea, Chisinau, Pontos (Europress), p. 102, (2016). ISBN 978-9975-51-774-4.
179. **BUZDUGAN, A**., BUZDUGAN, Ar. (2016a) *Cyber Security in the Nuclear and Radiological Domain: Case Study of Republic of Moldova*. In: Sontea V., Tiginyanu I. (eds) 3rd International Conference on Nanotechnologies and Biomedical Engineering. IFMBE Proceedings, vol 55. Springer, Singapore. DOI:10.1007/978-981-287-736-9_127.
180. **BUZDUGAN, A**., (2020) *Opportunities for improving cyber risk management in critical Infrastructures*, National scientific conference with international participation, Institute for Development and Innovation, Moldova State University, Conference Proceedings.
181. **BUZDUGAN, A**., *Model for cyber security maturity assessment in critical infrastructures*, Catalogul oficial al salonului „Cadet INOVA", ISSN 2501-3157, 6/2021, pp. 154-157, (2021).

182. **BUZDUGAN, A**., *The state of cyber security development for certain critical domains in the Republic of Moldova,* (2021), Proceedings of XXI All-Ukrainian Scientific and Technical Conference of Young Scientists, Postgraduates and Students "State, Achievements and Prospects of Information Systems and Technologies", Odessa National Academy of Food Technologies, 22-23 April 2021, pp. 38-39.
183. UNDP 2021, *Digital Readiness Assessment,* accesat la data de 11 septembrie 2021, [Online] la adresa https://moldova.un.org/en/143458-digital-readiness-assessment.
184. 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.
185. **BUZDUGAN, A**. *Assessment of cyber security maturity for critical domains in Republic of Moldova,* 5th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME-2021, November 3-5, 2021, Chisinau, Republic of Moldova, Program and Abstract Book, S8-1.8, ISBN 978-9975-72-592-7, pp. 100, (2021).
186. **BUZDUGAN, A**. *Assessment of cyber security maturity for critical domains in Republic of Moldova*, 5th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME-2021, November 3-5, 2021, Chisinau, Republic of Moldova, IFMBE Proceedings, pp. 649-656, vol 87.Springer Nature Switzerland, (2022), doi:10.1007/978-3-030-92328-0.
187. Eurostat 2020, *ICT security in enterprises* (2020). accesat la data de 3 august 2021, [Online] la adresa https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises.
188. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh. (2022) *The trends in cybersecurity maturity models*, 21st International Conference on Informatics in Economy 2022, ASE Bucharest (Accepted).
189. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh. (2022) *Sistem formal metric inteligent „Securitatea cibernetică în infrastructurile critice”,* Certificat AGEPI de înregistrare a Obiectelor Dreptului de Autor și Drepturilor Conexe, Seria O (Operă), Nr. 7305 din 04.08.2022.
190. **BUZDUGAN, A.,** *Information system for cyber security maturity assessment*. In: Metodologii contemporane de cercetare şi evaluare, Ştiinţe biologice şi chimice Ştiinţe fizice şi matematice Ştiinţe economice. 22-23 aprilie 2021, Chişinău: CEP USM, 2021, pp. 98-102.
191. **BUZDUGAN, A.,** *Sistemul formal metric „Securitatea cibernetică în infrastructuri critice”*. În „Salonul Internațional de Invenții, Inovații „Traian Vuia””. Timișoara, 08-10 octombrie 2022, coord. : Romi Rădulescu. Timișoara, Editura Politehnica, 2022, p. 81, ISBN 978-606-35-0496-9.

Anexa 1. Baza de cunoștințe „Securitatea cibernetică în infrastructurile critice”

NIVELUL DE MATURITATE A SECURITĂȚII CIBERNETICE (N_{MA} =)					
FOARTE INALT	**ÎNALT**	**MEDIU**	**SCĂZUT**	**FOARTE SCĂZUT**	**Notarea**
POLITICI ȘI ADMINISTRARE					
Cerințele de securitate cibernetică și reziliență sunt luate în considerare în faza de proiectare și evaluare a sistemului și sunt recunoscute ca o combinație între tehnologie și dimensiunea umană. **5**	Cerințele de securitate cibernetică și reziliență sunt reglementate de politici sau reglementări organizaționale/naționale, dar nu sunt întotdeauna integrate în faza de proiectare sau evaluare. Acestea sunt recunoscute ca o combinație între tehnologie și dimensiunea umană. **5**	Cerințele de securitate cibernetică și rezistență sunt impuse de reglementări din afara organizației, dar sunt considerate de conducerea superioară ca fiind legate doar de tehnologie. **3**	Cerințele de securitate cibernetică și reziliență sunt impuse de reglementări din afara organizației, însă nu sunt pe deplin luate în considerare în tehnologie sau în organizație. Principalii factori de rezistență sunt legați doar de siguranță. **2**	Factorii de decizie nu recunosc importanța securității cibernetice și rezistența sistemelor informaționale. Cerințele sunt percepute exclusiv ca o povară pentru procesul tehnologic de bază. Importanta acestor criterii se vede temporar, după incidente. **1**	$E_{1,1}(o) = e_{1,1}$
În procesul decizional, securitatea cibernetică și factorul de reziliență au o pondere mai mare în comparație cu costurile. **5**	Factorul cost are o influență minoră asupra luării deciziilor, uneori poate avea aceeași pondere în comparație cu cerințele funcționale, de securitate cibernetică sau de rezistență. **4**	Factorul cost are o pondere mai mare în comparație cu cerințele funcționale, de securitate cibernetică sau de rezistență. **3**	Costul este principalul factor în luarea deciziilor, adesea în dezavantajul cerințelor funcționale. **3**	Costul este întotdeauna factorul determinant în luarea deciziilor. **0**	$E_{1,2}(o) = e_{1,2}$
Responsabilitățile pentru securitatea cibernetică sunt clare și bine definite în funcție de structura și funcțiile respective. Procesul de schimb de informații este bine stabilit pe verticală și pe orizontală,	Sunt definite responsabilitățile pentru securitatea cibernetică. Schimbul de informații poate avea loc atât pe verticală, cât și pe orizontală, dar și cu părți externe. Există o funcție responsabilă de securitatea cibernetică.	Responsabilitățile pentru securitatea cibernetică nu sunt clar delimitate. Există o funcție responsabilă de securitatea cibernetică.	Nu este nimeni responsabil pentru securitatea cibernetică. Deși pot exista unele controale și sisteme de securitate, acestea nu sunt supravegheate.	Nu este nimeni responsabil pentru securitatea cibernetică. Controalele de securitate nu există, sau controalele sunt implicit integrate în anumite sisteme.	

inclusiv pe plan extern. Există o funcție responsabilă de securitatea cibernetică. **5**	**5**	**3**	**0**	**0**	$E_{1,3}(o) = e_{1,3}$
Funcțiile de management și supraveghere a riscurilor cibernetice sunt stabilite și joacă un rol major în procesul decizional. **5**	Funcțiile de management și supraveghere a riscurilor cibernetice sunt stabilite, dar nu influențează procesul decizional. Această responsabilitate revine personalului administrativ superior. **4**	Funcțiile de supraveghere a riscurilor cibernetice sunt responsabilitatea operatorilor, ceea ce poate fi uneori un conflict de interese. **3**	Funcțiile de supraveghere nu există. Deși uneori sunt întreprinse anumite acțiuni, acestea nu sunt întreprinse cu bună știință de către un manager. **0**	Funcțiile de supraveghere nu există. **0**	$E_{1,4}(o) = e_{1,4}$
Scorul total mediu $E_1(o) = E_{1,1}(o) + E_{1,2}(o) + E_{1,3}(o) + E_{1,4}(o)$					$E_1(o)$
EDUCAȚIE ȘI EVALUARE					
Sunt stabilite și revizuite programe de formare cuprinzătoare și regulate pe baza celor mai bune practici existente în domeniu. Instruirea se bazează pe performanță și conține evaluări. **5**	Sunt stabilite programe regulate de formare și acoperă majoritatea proceselor organizaționale. Instruirea se bazează pe performanță și conține evaluări. **5**	Sunt stabilite programe regulate de instruire pentru toți utilizatorii. Acestea includ aspecte formale și generale legate de procesele organizaționale. **3**	Instruirea utilizatorilor finali ai sistemelor informatice este considerată necesară doar pentru anumite roluri tehnice. **2**	Programul de instruire este formalizat la maximum, adesea exclusiv prin rapoarte și înregistrări fără sesiuni live. **2**	$E_{2,1}(o) = e_{2,1}$
Instruirea utilizatorilor finali ai sistemului informațional este obligatorie. Programul de formare ia în considerare dimensiunea umană și tehnologii. **5**	Instruirea utilizatorilor finali ai sistemului informațional este selectivă. Programul de formare ia în considerare dimensiunea umană și tehnologii. **5**	Instruirea utilizatorilor finali ai sistemului informatic este opțională. Programul de pregătire ia în considerare tehnologiile și doar anumite elemente ale factorului uman. **3**	Sunt definite strategii generice și programe generale de instruire care, printre altele, conțin aspecte de securitate cibernetică. **2**	Valoarea instruirilor și a exercițiilor nu este recunoscută și este considerată o povară. Formarea este văzută în primul rând ca o cerință de conformitate. Formarea nu acoperă evaluări. **1**	$E_{2,2}(o) = e_{2,2}$

Procedurile și cerințele se aplică tuturor rolurilor din cadrul organizației. Evaluarea are în vedere impactul real și riscul factorului uman. **5**	Procedurile și cerințele se aplică majorității organizației pentru rolurile cu risc ridicat. Evaluarea ia în considerare impactul real și riscul factorului uman. **4**	Procedurile și cerințele se aplică rolurilor selective pe baza profilului de risc. Evaluarea se concentrează pe riscurile legate de tehnologie. **3**	Procedurile și cerințele se aplică rolurilor selective pe baza profilului de risc, însă importanța și impactul benefic al instruirii nu sunt recunoscute. Evaluarea este formală și nu ia în considerare impactul real și riscul tehnologiilor sau factorul uman. **2**	Procedurile și cerințele nu se aplică. **0**	$E_{2,3}(o) = e_{2,3}$
Respectarea indicatorilor bazați pe performanță este obligatorie pentru îndeplinirea sarcinilor operaționale. **5**	Indicatorii minimi bazați pe performanță sunt definiți numai pentru îndeplinirea sarcinilor operaționale, dar nu sunt evaluați în mod regulat. **4**	Indicatorii minimi pentru îndeplinirea sarcinilor operaționale se bazează pe finalizarea programelor de formare sau dezvoltare, cu toate acestea programele de formare sunt percepute de toți ca o povară. **3**	Indicatorii minimi pentru îndeplinirea sarcinilor operaționale sunt definiți, dar nu corespund realității. Acești indicatori nu sunt evaluați. **0**	Indicatorii minimi pentru îndeplinirea sarcinilor operaționale nu sunt definiți. **0**	$E_{2,4}(o) = e_{2,4}$
Scorul total mediu $E_2(o) = E_{2,1}(o) + E_{2,2}(o) + E_{2,3}(o) + E_{2,4}(o)$					$E_2(o)$
MEDIUL DE LUCRU					
Mediul de lucru și politicile sunt percepute ca fiind favorabile în raport cu personalul; feedback-ul este pozitiv.	Mediul de lucru și politicile sunt orientate spre minimizarea majorității impactului negativ al potențialelor elemente ale factorilor umani. Feedback-ul este în general pozitiv.	Mediul de lucru și politicile minimizează doar anumite efecte negative majore ale potențialului factor uman. Feedback-ul este mediu.	Mediul de lucru și politicile sunt în vigoare în mod oficial și sunt considerate selective ca urmare a incidentelor. Feedback-ul este scăzut.	Mediul de lucru și politicile nu sunt luate în considerare sau adoptate în mod oficial. Evaluarea feedback-ului lipsește sau nu este concludentă deoarece se bazează pe evaluări care nu	

5	**4**	**3**	**2**	sunt adaptate contextului. **1**	$E_{3,1}(o) = e_{3,1}$
Toți angajații înțeleg impactul și vectorii atacului de risc cibernetic asupra tehnologiilor operaționale. Toți angajații înțeleg metodele de atenuare și sunt capabili să le implementeze în funcție de rolul lor. **5**	Impactul potențial al riscurilor cibernetice asupra tehnologiilor operaționale este înțeles colectiv, totuși există un decalaj în recunoașterea autoeficacității individuale în atenuarea și prevenirea acestora. **4**	Impactul potențial al riscurilor cibernetice asupra tehnologiilor operaționale este parțial recunoscut. Un număr mic de angajați știu cum și sunt capabili să implementeze atenuările necesare. **3**	Impactul potențial al amenințărilor cibernetice asupra tehnologiilor operaționale nu este recunoscut. Cultura securității cibernetice este evaluată într-o manieră limitată pentru necesitățile operaționale. **2**	Importanța securității cibernetice pentru tehnologiile operaționale este înțeleasă doar de unii indivizi. Acest fapt nu este raportat, nici escaladat. **1**	$E_{3,2}(o) = e_{3,2}$
Gradul de confort social al lucrătorilor este considerat un factor important. **5**	Gradul de confort social al lucrătorilor este luat în considerare numai în timpul dezvoltării politicilor. **4**	Gradul de confort social al lucrătorilor este considerat un factor parțial important. **3**	Gradul de confort social al lucrătorilor nu este considerat un factor important. **2**	Gradul de confort social al lucrătorilor nu este evaluat. **1**	$E_{3,3}(o) = e_{3,3}$
Scorul total mediu $E_3(o) = E_{3,1}(o) + E_{3,2}(o) + E_{3,3}(o) + E_{3,4}(o)$					$E_3(o)$
MANAGEMENTUL RISCURILOR CIBERNETICE					
Managementul riscurilor cibernetice este implementat pe baza celor mai bune practici și integrat cu managementul riscurilor organizațional e. Riscurile cibernetice sunt gestionate atât din perspectiva dimensiunii tehnologice, cât și a factorului uman. **5**	Managementul riscurilor cibernetice este implementat pe baza celor mai bune practici, dar parțial integrat cu managementul riscurilor organizațional. Riscurile cibernetice sunt gestionate atât din perspectiva dimensiunii tehnologice, cât și a factorului uman. **5**	Managementul riscurilor cibernetice este implementat oficial pentru a respecta bunele practici și standardele. Riscurile cibernetice sunt gestionate din perspectiva dimensiunii tehnologice. **3**	Managementu l propriu-zis al riscurilor cibernetice nu există. Incidentele sunt identificate ad-hoc de către operatori, sau din mediul extern, și remediate conform procedurilor existente. Riscurile cibernetice sunt gestionate ca orice alt risc. **2**	Managementul propriu-zis al riscurilor cibernetice nu există. Incidentele sunt cel mai adesea raportate de entități externe. Riscurile sunt gestionate fără a respecta bunele practici sau standarde. **1**	$E_{4,1}(o) = e_{4,1}$

Riscurile cibernetice sunt înțelese și recunoscute de management / factori de decizie / operatori. **5**	Riscurile cibernetice sunt înțelese și recunoscute de către management / factorii de decizie / majoritatea operatorilor. **4**	Riscurile cibernetice sunt înțelese și recunoscute de factorii de decizie / majoritatea operatorilor. Managementul oferă suport numai în cazul unor riscuri cu impact major. **3**	Riscurile cibernetice sunt recunoscute de majoritatea în organizație, dar atenția este acordată doar sub presiunea circumstanțelor. **2**	Riscurile cibernetice nu sunt înțelese și recunoscute de management/factorii de decizie. Incidentele cauzate de riscurile cibernetice nu sunt legate de amenințările cibernetice. **0**	$E_{4,2}(o) = e_{4,2}$
Instruirea și exercițiile sunt regulate și acoperă scenarii reale. **5**	Instruirea și exercițiile sunt regulate și acoperă scenarii care nu sunt întotdeauna adaptate la amenințările actuale. **4**	Instruirea este definită și efectuată periodic. Exercițiile de masă sunt efectuate numai la invitația sau solicitarea structurilor externe. **3**	Instruirea este organizată, dar exercițiile nu sunt instituționalizate. **2**	Instruirea sau exerciții nu există. **0**	$E_{4,3}(o) = e_{4,3}$
Sistemele informaționale pentru managementul riscurilor cibernetice sunt utilizate pentru sarcini critice; automatizarea este implementată acolo unde este posibil. Sistemele informaționale sunt, utilizate pentru a sprijini luarea deciziilor. **5**	Sistemele informaționale sunt utilizate în sarcini critice pentru managementul riscurilor cibernetice. Automatizarea este parțial utilizată. Există o dependență ridicată de sistemele informaționale pentru procesele operaționale legate de riscurile cibernetice. **4**	Sistemele informaționale sunt utilizate de anumiți utilizatori pentru a gestiona riscurile cibernetice. Necesitățile majore sunt acoperite de acest sistem. Performanța și beneficiile acestor sisteme sunt considerate medii. **3**	Sistemele informaționale nu sunt utilizate pentru sarcini de bază în managementul riscurilor cibernetice. Metodologiile de management al riscului nu sunt susținute de un sistem informațional dedicat. Beneficiile sistemelor informaționale sunt considerate reduse. **2**	Avantajele utilizării unui sistem informațional pentru managementul riscurilor nu sunt recunoscute. Managementul riscurilor cibernetice lipsește, sau aceste riscuri sunt văzute ca riscuri tehnologice, neglijând importanța și impactul potențial al amenințărilor tehnologice. **1**	$E_{4,4}(o) = e_{4,4}$
Modelul de acceptare a tehnologiei are	Modelul de acceptare a tehnologiei are indicatori înalți.	Modelul de acceptare a tehnologiei are	Modelul de acceptare a tehnologiei	Modelul de acceptare a tehnologiei are	

indicatori excelenți. **5**	**4**	indicatori medii. **3**	are indicatori scăzuți. **2**	indicatori foarte scăzuți. **1**	$E_{4,5}(o) = e_{4,5}$
Scorul total mediu $E_4(o) = E_{4,1}(o) + E_{4,2}(o) + E_{4,3}(o) + E_{4,4}(o) + E_{4,5}(o)$					$E_4 =$
$E(o) = E_1(o) + E_2(o) + E_3(o) + E_4(o)$					$E(o) =$
NIVELUL RISCURILOR CIBERNETICE ($N_{RC}(o)$)					
FOARTE JOS	**SCĂZUT**	**IN MEDIE**	**ÎNALT**	**FOARTE INALT**	$N_{RC}(o) =$

Anexa 2. Avizul modelului de la Administrația Slovenă pentru Securitate Nucleară (Slovenia)

REPUBLIC OF SLOVENIA
MINISTRY OF THE ENVIRONMENT AND SPATIAL PLANNING
SLOVENIAN NUCLEAR SAFETY ADMINISTRATION

Litostrojska cesta 54, 1000 Ljubljana, Slovenia

T: +386 1 472 11 00
F: +386 1 472 11 99
E: gp.ursjv@gov.si
www.ursjv.gov.si

Mr. Aurelian Buzdugan
Vienna International Center
Wagramer Strasse 5
PO BOX 400
A-1400, Vienna, Austria

No: 382-1/2021/7
Date: 15.03.2021

SUBJECT: Review of the Model for assessing the Cyber Security Maturity Level in Critical Infrastructures

Dear Mr. Buzdugan,

The proposed Model for Assessing the Cyber Security Maturity Level in Critical Infrastructures (hereinafter the Model), developed by you, PhD Student at the Doctoral School of Informatics and Mathematics, Moldova State University, looks promising and useful for application in nuclear sector.

Although the assessment questionnaire is quite general, the results show a clear picture of current maturity level for cyber security of the assessed entity from different standpoints.

We find the Model to be indeed multidimensional and cover certain dimensions of cyber security. We believe the Model can be extended in the future to accommodate specific requirements such as incident response planning, cyber security culture or cross-sectoral cooperation, based on the needs and requirements of the implementing organization.

Yours sincerely,

Igor Sirc
DIRECTOR

Anexa 3. Avizul Institutului Naţional de Metrologie privind modelul SSD

Institutul Național de Metrologie

MINISTERUL ECONOMIEI SI INFRASTRUCTURII

AVIZ
privind modelul de evaluare a maturităţii securităţii cibernetice în infrastructuri critice

Modelul propus pentru evaluare este multidimensional şi poate fi aplicat evaluării culturii securităţii cibernetice in organizaţii de tip infrastructura critica din domeniile nuclear, radiologic, medicina, bancar. Aceste organizaţii sunt critice pentru societate si economie.

Constatam ca securitatea cibernetica este un domeniu foarte actual, având in vedere numărul si impactul ameninţărilor cibernetice, Acest domeniu, a devenit parte intrinsecă a gestionarii riscurilor de securitate, datorita integrării in majoritatea proceselor tehnologice, administrative sau a protecţiei de date personale sau confidenţiale. Domeniul securităţii cibernetice are un rol cheie în prezent in prevenirea acţiunilor maliţioase, cum ar fi perturbarea cu rea-voinţă a economiei sau infrastructurii civile şi militare, si joacă un rol trivial în securitatea nucleară şi securitatea fizică a obiectivelor de profil, dar şi integral a obiectivelor strategice de interes naţional, din care face parte şi Institutul Naţional de Metrologie.

Necesitatea considerării securităţii cibernetice în activităţi din domeniul infrastructurile critice, este de exemplu reflectată şi de Legea privind desfăşurarea în siguranţă a activităţilor nucleare şi radiologice (Legea 132 din 08.06.2012, Art. 35,d, publ. M.O. nr.229-233, art. 739) la capitolul condiţiile de autorizare a activităţii.

Modelul de evaluare a securităţii cibernetice este compus din 4 categorii şi se bazează pe rolul major al factorului uman şi a tehnologiilor în interacţiune evidentă. Astfel modelul se caracterizează prin elemente inovative şi este binevenit pentru determinarea expresă de autorităţi a lacunelor existente în managementul riscurilor cibernetice cu repercusiuni asupra securităţii şi luarea de măsuri operative în redresarea situaţiei existente la entitate.

O autoevaluare test efectuată în Laboratorul Măsurări Ionizante a INM denotă o corespundere majoră a rezultatelor propriilor evaluări interne efectuate. Categoriile şi atributele propuse reprezintă un concept interesant, ce reflectă nivelul culturii securităţii într-un mod transparent, şi poate fi utilizat cât pentru autoevaluare sau evaluare externă, cât şi pentru prioritizarea planurilor de remediere.

Director al INM **Anatolie MELENCIUC**

Ex. T. Birca
Tel. 022 903 104

Republica Moldova, mun. Chişinău MD-2064, Str. Eugen Coca nr. 28
tel: 022 903 100 fax: 022 903 111
E-mail: office@inm.gov.md
www.inm.md

Anexa 4. Avizul FCIM UTM privind modelul SSD propus

Aviz

privind Sistemul de Suport Decizional pentru gestionarea riscurilor cibernetice în infrastructuri critice, propus de Aurelian Buzdugan, drd al Universității de Stat din Moldova

Impactul digitalizării infrastructurilor critice, la care atribuim și cele din domeniul sănătății și nuclear sau radiologic, este foarte mare și se așteaptă să fie chiar mai profund în viitor. Ca și pentru alte activități este important să se evalueze impactul digitalizării, în special asupra securității și siguranței materialelor nucleare, diverselor instalații și/sau softuri utilizate, inclusiv din medicină.

Digitalizarea pe de o parte ridică performanțele sistemelor per ansamblu, dar pe de altă parte oferă noi breșe pentru penetrarea nesancționată a sistemelor din exterior.

Din aceste considerente problema evaluării periodice a maturității sistemului de securitate cibernetică devine tot mai actuală pentru mentenanța unui standard înalt al sistemului de securitate și siguranță a activității entităților critice. Sunt de fapt niște probleme ce aparțin domeniului securității statului.

Modelul propus de evaluare expresă a gradului de pregătire a entităților în domeniul securității cibernetice permite organelor de conducere de grad superior să obțină simplificat, prin sondaj, date privind maturitatea securității cibernetice la organizație. Această metodă este necesară pentru luarea de măsuri adecvate la timp, precum și din următoarele considerente:

- în procesul de audit necesar conform Standardului ISO 27001;
- în procesul de obținere a autorizației de funcționare conform cerințelor înaintate entităților cu activități nucleare sau radiologice solicitate prin HG RM Nr. 1268/2016;
- în caz de protecția a datelor cu caracter personal, etc.

Un astfel de sistem de management al securității informațiilor, menționat în mod obișnuit de standarde din seria ISO 27000, este un bun punct de plecare și în identificarea resurselor critice pentru organizație și pentru a se asigura că procesele existente sunt documentate și respectate.

SSD este apreciat prin recenzarea experților la publicarea în reviste de specialitate Romanian Cyber Security Journal, (2020), Romanian J. of Information Technology and Automatic Control (2021), medaliat la Salonul cu participare internațională "Cadet INOVA" din Iași (2021).

Legeritatea aplicării modelului, gradul de corespundere cu cerințele ISO/IEC seria 27000 în securitatea informațională, permite utilizarea în cadrul lucrărilor practice referitoare la securitate fizică a obiectivelor nucleare/radiologice din medicină, cercetare, industrie, etc. Metoda este reflectată din 2021 în Fișa disciplinei F.02.O.007 Securitatea Nucleară și Radiologică la specialitățile Ingineria Biomedicală, Microelectronica și Nanotehnologii, destinată stidiilor superioare de masterat, ciclul II.

Avizul este aprobat la ședința DMIB nr. 4 din 22 decembrie 2021.

Decanul Facultății Calculatoare, Informatică și Microelectronică,
Ciorbă Dumitru, dr. conferențiar universitar

Șef interimar, Departamentul MIB,
Director executiv, Centrul Național de Suport al Securității Nucleare, FCIM
Rallean Serghei, dr., conferențiar universitar

Director, Centrul Național de Inginerie Biomedicală, FCIM
Șontea Victor, dr., profesor universitar

Anexa 5. Medalia de bronz acordată pentru model în cadrul „Cadet INOVA'21”

The International Student Innovation and Scientific Research Exhibition
- "Cadet INOVA'21" -
The "Nicolae Bălcescu" Land Forces Academy of Sibiu, Romania
15-17 April 2021

THE BRONZE MEDAL
OF THE "Cadet INOVA'21" EXHIBITION

Is bestowed on the researcher

Aurelian Buzdugan

for the innovation:

Model for cyber security maturity assessment in critical infrastructures

President of the Jury,
Dipl. – Eng.
Andrei Victor SANDU PhD

President of the Exhibition,
Dipl. – Eng.
Silviu Mihai PETRIȘOR PhD

MB-CI-2021

Anexa 6. Publicațiile autorului pe tema tezei

Reviste

1. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh., Impact of Human Dimension upon Decision Support Systems, Romanian Journal of Information Technology and Automatic Control, Vol. 31, No. 3, 31-44, 2021 (2021).
2. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh.: Factors for a decision support system in critical infrastructure cyber risk management, Romanian Cyber Security Journal, ISSN 2668-6430, ISSN-L 2668-1730, Vol 2(2), Pg. 67-73 (2020).
3. **BUZDUGAN, A**., (2020) Review on use of decision support systems in cyber risk management for critical infrastructures, Journal of Engineering Science Vol. XXVII, no. 3 (2020), pp. 134 - 145 Fascicle-Electronics and Computer, Science Topic-Computers and Information Technology, ISSN 2587-3474, eISSN 2587-3482, DOI:10.5281/zenodo.3949684, UDC 004.056.5.

Lucrările conferințelor și prezentare în cadrul evenimentelor (conferințe, workshop-uri)

4. **BUZDUGAN, A**., BUZDUGAN, Ar. Advances in security requirements for high-risk objects, IAEA International Conference on Nuclear Security (ICP presentation), 2016b.
5. **BUZDUGAN, A**., BUZDUGAN, Ar. (2016) Cyber Security in the Nuclear and Radiological Domain: Case Study of Republic of Moldova. In: Sontea V., Tiginyanu I. (eds) 3rd International Conference on Nanotechnologies and Biomedical Engineering. IFMBE Proceedings, vol 55. Springer, Singapore. DOI:10.1007/978-981-287-736-9_127 **(indexed by SCOPUS, EI Compendex, Japanese Science and Technology Agency (JST), SCImago)**.
6. **BUZDUGAN, A**; BUZDUGAN, Ar. The interplay between cyber and nuclear security in Republic of Moldova. In: Microelectronics and Computer Science. Ediția 9, 19-21 octombrie 2017, Chișinău, Moldova: Universitatea Tehnică a Moldovei, 2017, pp. 382-385. ISBN 978-9975-4264-8-0.
7. **BUZDUGAN, A**., An overview of cybersecurity in the healthcare sector. In: Telecommunications, Electronics and Informatics. 6, 24-27 mai 2018. Chișinău, Republica Moldova: Tehnica UTM, 2018, pp. 261-262. ISBN 978-9975-45-540-4.
8. **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 **(indexed by WoS, SCOPUS, EI Compendex, Japanese Science and Technology Agency (JST), SCImago)**.

9. **BUZDUGAN, A**., (2020) Opportunities for improving cyber risk management in critical Infrastructures, National scientific conference with international participation, Institute for Development and Innovation, Moldova State University, Conference Proceedings.
10. **BUZDUGAN, A**., BUZDUGAN, AR. The Synergy Between Cyber and Nuclear Security. Case Study of Moldova. In: Sidorenko A., Hahn H. (eds) Functional Nanostructures and Sensors for CBRN Defence and Environmental Safety and Security. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht, 2020 **(indexed by EMBiology, INSPEC, Norwegian Register for Scientific Journals and Series, SCImago, SCOPUS, WTI Frankfurt eG)**.
11. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh., Decision support systems for cyber risk management. Proceedings of the Workshop on Intelligent Information Systems WIIS2020, December 04-05, 2020, Chisinau, Republic of Moldova, (2020).
12. **BUZDUGAN, A**., CĂPĂȚÂNĂ, GH. (2020) Architecture Considerations for a Decision Support System in Cyber Risk Management. 9th International Workshop on Soft Computing Applications (SOFA 2020), Arad, Romania (in press with Springer).
13. **BUZDUGAN, A**., Model for cyber security maturity assessment in critical infrastructures, Catalogul oficial al salonului "Cadet INOVA", ISSN 2501-3157, 6/2021, pp. 154-157, (2021).
14. **BUZDUGAN, A**. Assessment of cyber security maturity for critical domains in Republic of Moldova, 5th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME-2021, November 3-5, 2021, Chisinau, Republic of Moldova, IFMBE Proceedings, pp. 649-656, vol 87. Springer, Springer Nature Switzerland, 2022. **(indexed by SCOPUS, EI Compendex, Japanese Science and Technology Agency (JST), SCImago)** DOI:10.1007/978-3-030-92328-0 (2022).
15. **BUZDUGAN, A**., The state of cyber security development for certain critical domains in the Republic of Moldova, (2021), Proceedings of XXI All-Ukrainian Scientific and Technical Conference of Young Scientists, Postgraduates and Students "State, Achievements and Prospects of Information Systems and Technologies", Odessa National Academy of Food Technologies, 22-23 April 2021, pp. 38-39.
16. **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 **(indexed by DBLP, EI Compendex, INSPEC, JST, SCImago, SCOPUS, WTI Frankfurt eG, zbMATH)**.

17. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh. (2022) The trends in cybersecurity maturity models, The 21st International Conference on Informatics in Economy 2022, Bucharest University of Economic Studies, (Accepted, to be published with Springer).
18. BUZDUGAN, AR., **BUZDUGAN, A**., Technical and Scientific Support Organizations and Strengthening of Nuclear Regulation (Case study of Moldova), International Conference on Challenges Faced by Technical and Scientific Support Organizations (TSOs) in Enhancing Nuclear Safety and Security, IAEA-CN-181/15, Japan, 2010.
19. BUZDUGAN, AR., **BUZDUGAN, A**., (2020) Revision of the Curriculum on Nuclear Safety and Security in the Light of Recent International Recommendations. In: Tiginyanu I., Sontea V., Railean S. (eds) 4th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2019. IFMBE Proceedings, vol 77, pp.815-819, Springer Nature Switzerland AG 2020, DOI:10.1007/978-3-030-31866-6_145 **(indexed by WoS, SCOPUS, EI Compendex, Japanese Science and Technology Agency (JST), SCImago)**.
20. BUZDUGAN, AR., RAILEAN, S., **BUZDUGAN, A**., Nanotechnology and Nonproliferation, 5th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME-2021, November 3-5, 2021, Chisinau, Republic of Moldova, (2022) IFMBE Proceedings, pp. 463-469, vol 87. Springer, Springer Nature Switzerland, 2022. **(indexed by SCOPUS, EI Compendex, Japanese Science and Technology Agency (JST), SCImago)** doi:10.1007/978-3-030-92328-0.

Rezumate publicate

21. **BUZDUGAN, A**., BUZDUGAN Ar. Information Security Development in the Moldovan Nuclear and Radiological Infrastructure, IAEA International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, 1-5 June, (2015).
22. **BUZDUGAN, A**., Role of Cyber Security along with Nuclear and Radiological Safety in Medicine. Book of Abstracts. 3rd International Conference of Health Technology Management. Ed. in Chief Victor Sontea, Chisinau, Pontos (Europress), p. 102, (2016). ISBN 978-9975-51-774-4.

23. **BUZDUGAN, A**. Adequate domain-based security [abstract], (2019) In: Book of Abstracts -Vienna Cyber Security Week 2019 - Protecting Critical Infrastructure. Vienna, Austria, Abstract nr 117.
24. BUZDUGAN, AR., **BUZDUGAN, A**., Converging knowledge and technology role in university's non-proliferation culture. SnT 2021. CTBT Science and Technology Conference, 28 June – 02 July 2021. Vienna, Austria, (2021), viewed 26 September 2021, https://conferences.ctbto.org/event/7/book-of-abstracts.pdf.
25. BUZDUGAN, AR., **BUZDUGAN, A**.: The increasing role of TSO in the Moldovan Nuclear and Radiological Infrastructure, International Conference on Challenges Faced by Technical and Scientific Support Organizations (TSOs) in Enhancing Nuclear Safety and Security, IAEA CN-214, (2014).
26. **BUZDUGAN, A**., IT Security as a driver of economics competitiveness. International conference - SMEs development and innovation: building competitive future of South-Eastern Europe: book of abstracts / International conference, Ohrid, 3-4 October, 2014. - Prilep: Faculty of economy, 2014. – 155 стр.; 23 см ISBN 978-9989-695-55-1, DOI: 10.13140/2.1.4082.4324 (2014).
27. **BUZDUGAN, A**. Assessment of cyber security maturity for critical domains in Republic of Moldova, 5th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME-2021, November 3-5, 2021, Chisinau, Republic of Moldova, Program and Abstract Book, S8-1.8, ISBN 978-9975-72-592-7, pp. 100, (2021).
28. BUZDUGAN, AR., RAILEAN, S., **BUZDUGAN, A**., Nanotechnology and Nonproliferation, 5th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME-2021, November 3-5, 2021, Chisinau, Republic of Moldova, Program and Abstract Book, S5-1.9, ISBN 978-9975-72-592-7, pp. 122 (2021).
29. **BUZDUGAN, A.,** *Sistemul formal metric „Securitatea cibernetică în infrastructuri critice"*. În „Salonul Internațional de Invenții, Inovații „Traian Vuia"". Timișoara, 08-10 octombrie 2022, coord. : Romi Rădulescu. Timișoara, Editura Politehnica, 2022, p. 81, ISBN 978-606-35-0496-9.

Drepturi de autor

30. **BUZDUGAN, A**., CĂPĂȚÂNĂ, Gh. (2022) Sistem formal metric inteligent „Securitatea cibernetică în infrastructurile critice", Certificat AGEPI de înregistrare a Obiectelor Dreptului de Autor și Drepturilor Conexe, Seria O (Operă), Nr. 7305 din 04.08.2022.

Anexa 7. Cod sursă pentru prototip

App.py

```
from userinterface import UserInterface
import csv
from datetime import date
from statistics import mean
import pickle
import glob
import os

class Model:

	def __init__(self):
		self.ui = UserInterface()

	def f1(self):
		print_general(self, indicators)
		a.app_menu()

	def f4(self):
		quit()

	def assess1(self):
		x=a.print_att('pol_adm', 'assess')
		indicators.append(x)
		savelist(self, indicators)
		a.app_menu()

	def assess2(self):
		x=a.print_att('ed_ev', 'assess')
		indicators.append(x)
		savelist(self, indicators)
		a.app_menu()

	def assess3(self):
		x=a.print_att('work_ev', 'assess')
		indicators.append(x)
		savelist(self, indicators)
		a.app_menu()

	def assess4(self):
		x=a.print_att('crm', 'assess')
		indicators.append(x)
		savelist(self, indicators)
		a.app_menu()

	def assess5(self):
		a.print_results(indicators)
		a.app_menu()
```

```
        def changeorg(self):
                indicators = []
                indicators = openlist(indicators)
                a.app_menu()

        def compare(self):
                os.system('cls')
                current = get_results(self, indicators)
                compareto = temp_indicators(self)
                print ("Comparison results:\n")
                print ("\t\t\t\t", organizatia, "\t\t", comp_organizatia, "\n")
                print ("Policy and administration:\t\t",current[1],"\t\t\t\t", compareto[1], "\n\n")
                print ("Training and Education:\t\t\t",current[3],"\t\t\t\t", compareto[3], "\n\n")
                print ("Work Environment:\t\t\t",current[5],"\t\t\t\t", compareto[5], "\n\n")
                print ("Cyber Risk Management:\t\t\t",current[7],"\t\t\t\t", compareto[7], "\n\n")
                print ("\nAverage Score:\t\t\t\t",
float(((float(current[1])+float(current[3])+float(current[5])+float(current[7]))/4)), "\t\t\t\t",
float((float(compareto[1])+float(compareto[3])+float(compareto[5])+float(compareto[7]))/4), "\n\n")
                input("\nPress Enter to continue...")
                a.app_menu()
        def app_menu(self):

                """The main menu of the app."""
                print("Organization: ", organizatia)
                # The nested dict to be sent as an argument
                MAIN_MENU = {

                        1: {
                                "label": "General Information",
                                "func": self.f1
                        },

                        2: {
                                "label": "Assessment: Policies and administration",
                                "func": self.assess1
                        },
                        3: {
                                "label": "Assessment: Training and Education",
                                "func": self.assess2
                        },
                        4: {
                                "label": "Assessment: Work Environment",
                                "func": self.assess3
                        },
                        5: {
                                "label": "Assessment: Cyber Risk Management",
                                "func": self.assess4
                        },
                        6: {
                                "label": "Print latest results",
                                "func": self.assess5
                        },
```

```
                7: {
                        "label": "Change organization",
                        "func": self.changeorg
                },
                8: {
                        "label": "Compare maturity",
                        "func": self.compare
                },
                9: {
                        "label": "Exit",
                        "func": self.f4
                }
        }

        # Menu heading and nested dict are sent as arguments
        self.ui.choose_menu("MAIN MENU", MAIN_MENU)
    def print_att(self, criteria, action):
        a=[] # list for storing assessment results
        a.append(date.today())
        a.append(criteria)
        with open("model2.csv", 'r') as file:
            reader = csv.reader(file, quoting=csv.QUOTE_ALL, skipinitialspace=True)
            temp = [] # read rows matching specific criteria
            nr = [] # get nr of attributes per specific level
            for row in reader:
                if row[1]==criteria:
                    temp.append(row)
                    nr.append(row[2])
            elements = int(max(nr))+1
            for i in range(1,elements):
                print ('\n\n\n\n\n**************************')
                for row in temp:
                    if row[2]==str(i):
                        print(row[0],':',row[3],'\n')
                if action == 'assess':
                    while True:
                        try:
                            print ('**************************')
                            value= int(input("\nChoose the digit that
corresponds to the cyber security maturity level of your organization:\n (5-Very High, 4-High, 3-Average,
2-Low, 1-Very Low)\n"))
                            break
                        except:
                            print("ERROR! Please enter the result as a
number. The number of points that corresponds to each level is: VH=5,HI=4,AV=3,LO=2,VL=1. \n ")
                    a.append(value)


        a.append(mean(a[-(elements-1):]))
        return a

    def print_results(self, indicators):
```

```
                temp = []
                temp.append(date.today())
                temp.append('gen_score')
                print ("Latest assessment results per each dimension are:\n")
                for element in reversed(indicators):
                        if element[1] == "pol_adm":
                                print ("-Policies and Administration, last assessment performed on: "+
str(element[0])+", latest average score:", round (element[-1],1))
                                temp.append(element[-1])
                                break
                        continue
                for element in reversed(indicators):
                        if element[1] == "ed_ev":
                                print ("-Education and Evaluation, last assessment performed on: "+
str(element[0])+", latest average score:", round (element[-1],1))
                                temp.append(element[-1])
                                break
                        continue
                for element in reversed(indicators):
                        if element[1] == "work_ev":
                                print ("-Work Environment, last assessment performed on: "+
str(element[0])+", latest average score:", round(element[-1],1))
                                temp.append(element[-1])
                                break
                        continue
                for element in reversed(indicators):
                        if element[1] == "crm":
                                print ("-Cyber Risk Management, last assessment performed on: "+
str(element[0])+", latest average score:", round(element[-1],1))
                                temp.append(element[-1])
                                break
                        continue
                print ('\n\n*** Overall cyber security score is ' + str(round(mean(temp[2:]),1))
+'***\n\n')
                temp.append(mean(temp[2:]))
                indicators.append(temp)
                savelist(self, indicators)

def get_results(self, indicators):
        temp = []
        for element in reversed(indicators):
                if element[1] == "pol_adm":
                        temp.append(element[0])
                        temp.append(element[-1])
                        break
                continue
        for element in reversed(indicators):
                if element[1] == "ed_ev":
                        temp.append(element[0])
                        temp.append(element[-1])
                        break
                continue
```

```
        for element in reversed(indicators):
                if element[1] == "work_ev":
                        temp.append(element[0])
                        temp.append(element[-1])
                        break
                continue
        for element in reversed(indicators):
                if element[1] == "crm":
                        temp.append(element[0])
                        temp.append(element[-1])
                        break
                continue
        return temp
def print_general(self, indicators):
                print(indicators)
                for element in reversed(indicators):
                        if element[1] == "gen_score":
                                print ("\n\n\n***** General information about cyber security maturity
level *****")
                                print ("Last assessment performed on: ",str(element[0]))
                                print ("Latest average score:", round(element[-1],1))
                                print ("\n\n")
                                if element[-1] < 3:
                                        print ("***WARNING***\nOverall cyber security maturity is
below average. Actions are required to improve the security stance\n")
                                        print ("To view the results per dimension select PRINT LATEST
RESULTS\n" )
                                print ("\n\n")
                                break
                        continue

def savelist(self, indicators):
        print (path)
        with open(path, 'wb') as fp:
                pickle.dump(indicators, fp)

def temp_indicators(self):
        global comp_organizatia
        print("Own organization is - ", organizatia, "\n")
        print ("**********")
        nr=1
        x=(glob.glob("./organizations/*"))
        for i in x:
                print(str(nr) + ". " + str(i[16:]))
                nr+=1
        org= int(input("\nChoose the organization to compare with (enter digit)\n"))
        org-=1
        print ("Comparing with organization: ",str((x[org])[16:]))
        comp_organizatia=str((x[org])[16:])
        with open (x[org], 'rb') as fp:
                temp_indicators = pickle.load(fp)
        tc_temp = get_results(self, temp_indicators)
```

```
        return tc_temp
def openlist(self):
        os.system('cls')
        global organizatia
        global org
        global path
        global indicators
        indicators= []
        organizatia=""

        print ("Organizations found in database are the following")
        nr=1
        x=(glob.glob("./organizations/*"))
        for i in x:
                print(str(nr) + ". " + str(i[16:]))
                nr+=1
        org= int(input("\nChoose the digit that corresponds to the organization you want to assess:\n"))
        org-=1
        path = x[org]
        with open (x[org], 'rb') as fp:
                indicators = pickle.load(fp)
                organizatia=str((x[org])[16:])
        return indicators
indicators = []
indicators = openlist(indicators)
a = Model()
a.app_menu()
```

Declarație de răspundere

Subsemnatul declar pe răspundere personală că materialele prezentate în teza de doctorat sunt rezultatul propriilor cercetări și realizări științifice. Sunt conștient de faptul ca in caz contrar voi suporta consecințele in conformitate cu legislația in vigoare.

Buzdugan, Aurelian

Semnătură

Data

Curriculum Vitae

Aurelian BUZDUGAN

Chișinău, Moldova | Email: aurelian.buzdugan@yahoo.com

EXPERIENȚĂ PROFESIONALĂ

- 01/2018 – prezent – Austria
  EXPERT SECURITATE IT – ORGANIZAȚIA NAȚIUNILOR UNITE PENTRU DEZVOLTARE INDUSTRIALĂ.
- 06/2015 – 12/2017 – Germania
  INGINER SECURITATE IT – SERCO.
- 06/2014 – 06/2015 Germania
  TRAINEE, SECURITATE IT – BANCA CENTRALĂ EUROPEANĂ.
- 09/2013 – 06/2014 – Moldova
  MANAGER SECURITATEA INFORMAȚIEI – SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ.

EDUCAȚIE ȘI FORMARE PROFESIONALĂ

- 2019 – ÎN CURS – Moldova
  DOCTORAT – Universitatea de Stat din Moldova.
- 09/2011 – 06/2013 – Chisinau, Moldova
  MASTER ÎN ȘTIINȚE EXACTE - DEZVOLTAREA PRODUSELOR SOFTWARE – Universitatea de Stat din Moldova.
- 01/2013 – 07/2013 – Groningen, Țările de Jos
  ERASMUS MUNDUS EMERGE PROGRAM – Universitate din Groningen.
- 03/2012 – 06/2012 – Vienna, Austria.
  CENTRAL EUROPEAN EXCHANGE PROGRAM FOR UNIVERSITY STUDIES – Universitatea de Științe Aplicate Technikum din Vienna.
- 09/2008 – 06/2011 – Chisinau, Moldova
  LICENȚIAT ÎN ȘTIINȚE EXACTE - INFORMATICA APLICATĂ – Universitatea de Stat din Moldova.
- 08/2010 – 05/2011 – Portland
  GLOBAL UNDERGRADUATE EXCHANGE PROGRAM – Lewis and Clark College.

COMPETENȚE LINGVISTICE

- Limbă(i) maternă(e): română.
- Alte limbi: engleză (C2), germana (B2), rusă (C2), franceză (B1) .

PARTICIPĂRI LA CONFERINȚE

- Participarea la 23 de conferințe naționale și internaționale organizate de instituții precum USM, UTM, Institutul de Matematică și Informatică "Vladimir Andrunachievici", Academia de Studii Economice Bucuresti, Universitatea din Arad, Academia Forțelor Terestre Nicolae Bălcescu, Agentia Internationala de Energie Atomică, NATO, Organizația Tratatului pentru Interzicerea Totală a Testelor Nucleare, ISACA Romania & Banca Nationala a Romaniei, Academia Națională de Tehnologii Alimentare din Odesa.
- Membru juriu la conferinta 2022 International Competition of Student Scientific Works “Black Sea Science”, organizat de Academia Națională de Tehnologii Alimentare din Odesa (Ucraina).
- ICNBME 2021 - conducătorul sesiunii Health Informatics, E-Health and Telemedicine; prezentare în cadrul sesiunii.

- Vienna Cyber Security Week 2019 - conducătorul sesiunii "Security by design"; prezentare în cadrul sesiunii.

PUBLICAȚII

- 22 articole ca autor principal, 6 articole - coautor; 8 articole mono-autor și 3 rezumate mono-autor; ◦ 3 articole publicate în reviste științifice de specialitate, dintre care 2 în străinătate și 1 în Moldova (B+).
- 2 articole indexate de Web of Science și 7 articole indexate în Scopus.
- 7 articole publicate în Springer și 1 articol acceptat pentru publicare în Springer la momentul depunerii tezei.
- 24 de articole, inclusiv rezumate, publicate în lucrările conferinței (în 18 articole ca autor principal).

CERTIFICĂRI INTERNAȚIONALE

- GIAC Certified Forensic Examiner (GCFE) (2017).
- GIAC Certified Incident Handler (GCIH) (2016) ◦ Cisco CCNA Cyber Ops (2017).
- EC-Council Certified Ethical Hacker (2014).
- EC-Council N etwork and System Administrator (2014).
- ISO 27001 Certified ISMS Foundation CIS F (2019).

ACTIVITĂȚI EXTRA ȘI CURSURI DE FORMARE

- Evaluator invitat la revista Studies in Informatics and Control (Romania).
- Lector pentru AIEA în domeniul securității calculatoarelor (Cursuri de formare de bază și avansate), 2015-2017.
- MISP Training - Threat intelligence Analyst and Administrator (2019).
- MISP Training - Developer (2019).
- DevOps Fundamentals (2021).
- Information Security Risk Management Advanced Course, Moldova (2014).
- Cyber Defense Hands-On Training Course for System Administrators of Moldova, 12-24 January 2014, Middle East Technical University, Ankara, Turkey.
- Network Vulnerability Assessment Course, Germany, 25 November 2013 29 January 2014; ◦ Project Cycle Management Training, IREX Moldova, 3-4 September, 2011.