UNIVERSITATEA TEHNICĂ A MOLDOVEI

Cu titlu de manuscris
C.Z.U.: 621.39:004.056:
378(478)(043)

ALEXEI ARINA

CADRUL SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE PENTRU INSTITUȚIILE DE ÎNVĂȚĂMÂNT SUPERIOR DIN REPUBLICA MOLDOVA

Specialitatea: ***231.02. Ingineria și tehnologia comunicațiilor electronice***

Teză de doctor în științe inginerești

Conducător științific: **NISTIRIUC Pavel**
conf. univ., dr.

Autor: **ALEXEI Arina**

CHIȘINĂU, 2023

CUPRINS

ADNOTARE **5**
LISTA TABELELOR **8**
LISTA FIGURILOR **9**
LISTA ABREVIERILOR **11**
INTRODUCERE **13**
1. SECURITATEA COMUNICAȚIILOR ELECTRONICE **18**
1.1. Considerații generale și termeni specifici domeniului 18
1.2. Amenințări de securitate ale comunicațiilor electronice 23
1.3. Dispozitive de securitate ale rețelelor de comunicațiilor electronice 28
1.4. Cadrul normativ național și european cu privire la securitatea CE 29
1.5. Esența și particularitățile CE ale IÎS 31
1.5.1. Specificul CE universitare 31
1.5.2. Provocări de securitate ale domeniului 33
1.5.3. Amenințări de securitate ale RCE universitare 35
1.5.4. Stadiul cercetărilor în domeniul securității CE în IÎS 37
1.6. Studiul empiric al situației actuale în IÎS din Republica Moldova 38
1.7. Definirea problemei de cercetare 43
1.8. Concluzii la capitolul 1 45
2. METODOLOGIA DE DEZVOLTARE A CADRULUI SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE **47**
2.1. Identificarea problemei și motivația 48
2.2. Definirea obiectivelor CSSCE 49
2.3. Design și dezvoltare CSSCE 50
2.3.1. Standarde/cadre de securitate utilizate în IÎS 50
2.3.2. Metode și materiale pentru dezvoltarea CSSCE 62
2.4. Demonstrarea CSSCE 65
2.5. Evaluarea CSSCE 66
2.6. Comunicarea rezultatelor cercetării 67
2.7. Resurse utilizate 68
2.8. Concluzii la capitolul 2 68
3. CADRUL SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE UNIVERSITARE **70**
3.1. Fundamentarea teoretică a cadrului sistemic de securitate a CE 70

3.1.1. Conceptul de securitate a CE 71
3.1.2. Modelul formal pentru descrierea sistemelor de securitate 72
3.2. Dezvoltarea CSSCE 77
3.2.1. Abordarea sistemică a securității CE în mediul universitar 77
3.2.2. Dezvoltarea aspectelor organizaționale 79
3.2.3. Dezvoltarea aspectelor operaționale ale CSSCE 86
3.3. Dezvoltarea instrumentului i-CSSCE 108
3.4. Concluzii la capitolul 3 111
4. EVALUAREA CADRULUI SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE 113
4.1. Studiu de caz 113
4.2. Utilizarea metodei Delphi pentru evaluarea prototipului CSSCE 123
4.2.1. Aplicarea statisticii descriptive 125
4.2.2. Aplicarea statisticii inferențiale 127
4.3. Evaluarea calitativă a prototipului CSSCE 129
4.4. Analiza comparativă a cadrelor de securitate 130
4.5. Concluzii la capitolul 4 131
CONCLUZII FINALE ȘI RECOMANDĂRI 133
BIBLIOGRAFIE 137
Anexa 1. Publicații științifice ale autorului 160
Anexa 2. Active de suport universitare bazate pe CE 161
Anexa 3. Amenințări generice și specifice de securitate 162
Anexa 4. Sondajul final 169
Anexa 5. Model Proiect de implementare a CSSCE 172
Anexa 6. Politica de utilizare acceptabilă a resurselor TIC universitare 173
Anexa 7. Depozit cerințe de securitate ruter/switch 175
Anexa 8. Varianta inițială a depozitului de securitate 176
Anexa 9. Întrebări evaluare cantitativă 177
Anexa 10. Acte de implementare 179
Declarația privind asumarea răspunderii 183
CURRICULUM VITAE 184

ADNOTARE

Alexei Arina, *"Cadrul sistemic de securitate a comunicațiilor electronice pentru instituțiile de învățământ superior din Republica Moldova"*, teză de doctor în științe inginerești, specialitatea *231.02. Ingineria și tehnologia comunicațiilor electronice,* Chișinău, 2023

Structura tezei: introducere, 4 capitole, concluzii finale și recomandări, bibliografie din 243 titluri, 10 anexe, 121 pagini de text, 19 tabele și 46 figuri. Rezultatele cercetării au fost publicate în 11 lucrări științifice.

Cuvinte-cheie: cadru sistemic, securitate, comunicații electronice, rețele de comunicații electronice, servicii de comunicații electronice, instituții de învățământ superior, amenințări de securitate, cerințe de securitate, risc cibernetic.

Scopul: realizarea cercetărilor privind elaborarea unui cadru sistemic de securitate a comunicațiilor electronice (CSSCE) care va contribui la securizarea e-serviciilor academice prestate de instituțiile de învățământ superior din Republica Moldova.

Obiectivele de cercetare: identificarea și analizarea problemelor de securitate care se referă la comunicațiile electronice cu accent pe instituțiile de învățământ superior; selectarea metodei științifice de dezvoltare a CSSCE; dezvoltarea CSSCE orientat spre procesul educațional academic al instituțiilor de învățământ superior din Republica Moldova; evaluarea CSSCE conform criteriilor de valoare.

Noutatea şi originalitatea științifică: abordarea sistemică și cuprinzătoare a procesului de asigurare a securității comunicațiilor electronice în instituțiile de învățământ superior.

Rezultatul obținut ce contribuie la soluționarea problemei științifice: elaborarea unui cadru sistemic național de securitate a comunicațiilor electronice pentru instituțiile de învățământ superior din Republica Moldova, care ar aborda holistic problemele aferente securității comunicațiilor electronice prioritate la nivel internațional în ultimii ani.

Semnificația teoretică: contribuții importante la dezvoltarea bazei teoretico-metodologice în domeniul securității sistemelor.

Valoarea aplicativă: elaborarea unei soluții practice, a cadrului sistemic național de securitate a comunicațiilor electronice.

Implementarea rezultatelor științifice: rezultatele au fost implementate în trei instituții de învățământ superior – Universitatea Tehnică a Moldovei, Universitatea de Stat de Medicină și Farmacie „Nicolae Testemițanu" și Universitatea Liberă Internațională din Moldova în procesul educațional academic din cadrul Universității Tehnice a Moldovei.

АННОТАЦИЯ

Алексей Арина, «*Системный фреймворк безопасности для электронных коммуникаций в высших учебных заведениях Республики Молдова*», докторская диссертация по техническим наукам, специальность 231.02. *Инженерия и технологии электронных коммуникаций*, Кишинев, 2023

Структура диссертации: введения, 4 глав, итоговые выводы и рекомендации, библиографии из 243 наименований, 10 приложений, 121 страниц текста, 19 таблиц и 46 рисунков. Результаты исследований опубликованы в 11 научных работах.

Ключевые слова: системная структура, безопасность, электронные коммуникации, электронные коммуникационные сети, сервисы электронных коммуникаций.

Цель: заключается в проведении исследований по разработке системного фреймворка безопасности электронных коммуникаций (CSSCE).

Задачи исследования: выявление и анализ проблем безопасности, связанных с электронными коммуникациями, с акцентом на высшие учебные заведения; выбор научного метода для разработки CSSCE; развитие CSSCE, ориентированного на академический образовательный процесс высших учебных заведений.

Научная новизна и оригинальность заключается в системном и комплексном подходе к процессу обеспечения безопасности электронных коммуникаций в высших учебных заведениях. Полученным результатом, способствующим решению научной задачи является: разработка национального системного фреймворка безопасности электронных коммуникаций для высших учебных заведений Республики Молдова, который обеспечил бы целостный подход к вопросам, связанным с безопасностью электронных коммуникаций, приоритетом на международном уровне в последние годы.

Теоретическая значимость заключается в важном вкладе в развитие теоретико-методологической базы в области системной безопасности.

Прикладная ценность состоит в: разработке практического решения системного фреймворка безопасности для электронных коммуникаций.

Внедрение научных результатов в трех высших учебных заведениях: Технический Университет Молдовы, Государственный Медицинский и Фармацевтический Университет ”Николае Тестемицану”, Международный Независимый Университет Молдовы.

ANNOTATION

Alexei Arina, "*Systemic security framework of electronic communications for higher education institutions in the Republic of Moldova*", PhD thesis in engineering sciences, specialty 231.02. *Electronic communications engineering and technology*, Chisinau, 2023

The structure of the thesis consists of: introduction, 4 chapters, final conclusions and recommendations, a bibliography of 243 titles, 10 annexes, 121 pages of text, 19 tables and 46 figures. The research results were published in 11 scientific papers.

Keywords: system framework, security, electronic communications, electronic communications networks, electronic communications services, Higher Education Institutions, security threats, security requirements, cyber risk.

The goal of the research is to carry out research for the development of a systemic framework for the security of electronic communications (CSSCE), which will contribute to the security of electronic academic services provided by higher education institutions in the Republic of Moldova. **Research objectives** are: the identification and analysis of security issues related to electronic communications, with emphasis on higher education institutions; selection of the scientific method for the development of CSSCE; the development of CSSCE oriented on the academic educational process of Higher Education Institutions from the Republic of Moldova; the CSSCE evaluation according to the value criteria.

The novelty and scientific originality consist of systemic and comprehensive approach to the process of ensuring the security of electronic communications in higher education institutions. The result obtained that contributes to solving the scientific problem is: the development of a national systemic framework for the security of electronic communications for higher education institutions in the Republic of Moldova, for a holistic approach to issues related to the security of electronic communications, a priority at the international level in recent years.

The theoretical significance consists in: important contributions to the development of the theoretical-methodological base in the field of system security.

The applicative value consists in: the development of a practical solution, of the national systemic security framework for electronic communications.

Implementation of scientific results in three higher education institutions: the Technical University of Moldova, the State University of Medicine and Pharmacy "Nicolae Testemițanu" and the International Free University of Moldova; in the academic educational process of the Technical University of Moldova.

LISTA TABELELOR

Tabelul 2.1. Criteriile de valoare ale CSSCE 49
Tabelul 2.2. Criterii de cercetare 52
Tabelul 2.3. Relevanța lucrărilor științifice 52
Tabelul 3.1. Procesul Educațional Academic 85
Tabelul 3.2. Indicatori cheie de performanță a CSSCE 87
Tabelul 3.3. Structura politicii de securitate manageriale (elaborat de autor) 92
Tabelul 3.4. Active de suport (elaborat de autor) 95
Tabelul 3.5. Dependența obiectivelor de securitate de sistemul universitar (elaborat de autor) ...96
Tabelul 3.6. Criteriile de evaluare a impactului (elaborat de autor) 98
Tabelul 3.7. Criterii de evaluare a probabilității (elaborat de autor) 100
Tabelul 3.8. Valoarea riscului cibernetic (elaborat de autor) 100
Tabelul 3.9. Identificarea proprietarilor activelor informaționale (elaborat de autor) 101
Tabelul 3.10. Conversia costului activului într-o valoare calitativă (elaborat de autor) 102
Tabelul 3.11. Conversia impactului activului în procesul academic (elaborat de autor) 102
Tabelul 4.1. Calificative scara Likert 125
Tabelul 4.2. Rezultate ale Statisticii Descriptive (elaborat de autor) 126
Tabelul 4.3. Interpretarea rezultatelor (adaptat după [193]) 128
Tabelul 4.4. Ranguri obținute (elaborat de autor) 128
Tabelul 4.5. Analiza comparativă a cadrelor de securitate (elaborat de autor) 130

LISTA FIGURILOR

Fig. 1.1. Procesul de CE 19
Fig. 1.2. Active bazate pe CE 22
Fig. 1.3. Atacuri cibernetice asupra CE 24
Fig. 1.4. Consumul de bandă în urma atacurilor de tip DoS/DDoS 25
Fig. 1.5. Modelul cascadă 31
Fig. 1.6. Modelul ierarhic 32
Fig. 1.7. Procentajul atacurilor DoS/DDoS asupra resurselor educaționale: 36
Fig. 1.8. Procedura realizată pentru investigație 39
Fig. 1.9. Amenințări de securitate ale IÎS din RM în anul 2020 40
Fig. 1.10. Amenințări de securitate frecvente 41
Fig. 1.11. Acțiuni pentru gestiunea riscului de securitate și răspunsul la incidente 41
Fig. 1.12. Realizarea managementului securității 43
Fig. 2.1. Design-ul cercetării conform etapelor DSR 48
Fig. 2.2. Studiul literaturii în baza metodei lui Kitchenham 51
Fig. 2.3. Cadrul/Standardul recomandat pentru implementare în IÎS 54
Fig. 2.4. Modelul PDCA 55
Fig. 2.5. Cadre recomandate pentru managementul riscului 58
Fig. 2.6. Clasificarea vulnerabilităților, conform standardului ISO 27005 58
Fig. 2.7. Operaționalizare CSSCE 65
Fig. 3.1. Conceptul de securitate a CE 71
Fig. 3.2. Graful relației Amenințare-Cerință-Obiect 73
Fig. 3.3. Graful sistemului de securitate 74
Fig. 3.4. Dezvoltarea CSSCE conform ciclului Deming 78
Fig. 3.5. Dezvoltare aspecte organizaționale 79
Fig. 3.6. Schema de interconectare a RCE, UTM 84
Fig. 3.7. Cadrul generic pentru dezvoltarea politicilor de securitate în IÎS 91
Fig. 3.8. Politică de securitate bazată pe sistem 93
Fig. 3.9. Configurare listă de acces al controlului 93
Fig. 3.10. Atacul DDoS/DoS pentru o rețea cu capacitatea de 10 Gbps 99
Fig. 3.11. Model pentru Registrul Riscurilor de Securitate 103
Fig. 3.12. Model pentru Planul de Tratare a Riscului 103
Fig. 3.13. Model pentru Declarația de Aplicabilitate 104
Fig. 4.1. Meta model infrastructura RCE redundantă 114

Fig. 4.2. Crearea proiectului 114
Fig. 4.3. Roluri predefinite pentru utilizatori.....115
Fig. 4.4. Completarea proiectului 115
Fig. 4.5. Adăugare politici de securitate.....116
Fig. 4.6. Adăugare active de suport.....117
Fig. 4.7. Dependența față de obiectivele de securitate 117
Fig. 4.8. Amenințări de securitate.....118
Fig. 4.9. Valoarea calitativă a activelor de suport 119
Fig. 4.10. Cerințe de securitate pentru activele de suport cu risc redus 120
Fig. 4.11. Cerințe de securitate pentru activele de suport cu risc mediu 120
Fig. 4.12. Cerințe de securitate pentru activele de suport cu risc sporit.....121
Fig. 4.13. Depozit cerințe de securitate 122
Fig. 4.14. Raport evaluare implementare CSSCE 122

LISTA ABREVIERILOR

ARP	-	Address Resolution Protocol
BDMC	-	bază de date de management al configurației
BGP	-	Border Gateway Protocol
BYOD	-	Bring Your Own Device
CAN	-	rețea din campus (Campus Area Network)
CDMA	-	Code Division Multiple Access
CDSI	-	Consiliul de Dezvoltare Strategică Instituțională
CE	-	comunicații electronice
CIA	-	confidențialitate, integritate, disponibilitate (Confidentiality, Integrity, Availability)
COBIT	-	Control Objectives for Information and Related Technologies
CSSCE	-	cadrul sistemic de securitate a comunicațiilor electronice
DDoS	-	Distributed Denial of Service
DNS	-	Domain Name System
DoS	-	Denial of Service
DSR	-	cercetarea în știința proiectării (original din engleză: Design Science Research)
ENISA	-	Agenția Uniunii Europene pentru Securitate Cibernetică
FTP	-	File Transfer Protocol
GSM	-	Global System for Mobile Communications
HG	-	hotărâre de guvern
HTTP	-	HyperText Transfer Protocol
IBN	-	Instrument Bibliometric Național
ICMP	-	Internet Control Message Protocol
IÎS	-	instituții de învățământ superior
IMAP	-	Internet Message Access Protocol
IP	-	Internet Protocol
ISO	-	Organizația Internațională pentru Standardizare
ITIL	-	Information Technology Infrastructure Library

ITU	-	Uniunea Internațională a Telecomunicațiilor (International Telecommunication Union)
LAN	-	rețea locală (Local Area Network)
MAC	-	Media Access Control
MAN	-	rețea metropolitană (Metropolitan Area Network)
MCSS	-	Minimum Cyber Security Standard
MitM	-	Man in the Middle
NIST	-	Institutul Național de Standarde și Tehnologie
OSI	-	Open Systems Interconnection
QoS	-	Quality of service
PDCA	-	Plan, Do, Check, Act
POP	-	Post Office Protocol
RCE	-	rețele de comunicații electronice
RM	-	Republica Moldova
SCE	-	servicii de comunicații electronice
SE	-	servicii electronice
SMTP	-	Simple Mail Transfer Protocol
SMSI	-	sistem de management al securității informațiilor
SRE	-	ingineria cerințelor de securitate (original din engleză: Security Requirements Engineering
SSL	-	Secure Sockets Layer
TCP	-	Transmission Control Protocol
TLS	-	Transport layer security
UDP	-	User Datagram Protocol
VLAN	-	rețea locală virtuală (Virtual Local Area Network)
VPN	-	rețea virtuală privată (Virtual Private Network)
WAN	-	Wide Area Network
WLAN	-	rețea locală fără fir (Wireless Local Area Network)

INTRODUCERE

Actualmente, organizațiile guvernamentale și non-guvernamentale, persoanele juridice și fizice își desfășoară majoritatea activităților și interacțiunilor economice, comerciale, culturale, sociale și guvernamentale, utilizând rețelele și serviciile de comunicații electronice (CE) [1]. Odată cu digitalizarea la nivel internațional și dezvoltarea serviciilor electronice, care devin tot mai cunoscute, cresc și riscurile asociate tehnologiilor comunicaționale [2]. Astfel, în raportul prezentat de ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) pentru perioada 2020-2021, atacurile asupra rețelelor de CE (RCE) atestă o creștere îngrijorătoare atât în diversitatea vectorilor de atac, cât și a numărului de atacuri anuale înregistrate și impactul avut [3].

Impactul atacurilor cibernetice poate fi estimat în pierderi financiare semnificative, cât și în volumul informațiilor compromise. Potrivit raportului anual realizat de Institutul Ponemon în baza a 550 organizații din 17 țări și industrii diferite, analizând perioada martie 2021–martie 2022, pierderile financiare raportate la încălcarea securității datelor au crescut din 2017 până în 2022 de la 3,62 mln $ la 4,35 mln $ [4], cu o creștere procentuală de aproximativ 12%. Impactul lunar asociat volumului de date compromise relatat doar atacurilor cu programele malițioase de tip ransomware a crescut de la 8 TB (terabytes) în mai 2021 la 136 TB în iunie 2022 [5]. Atacuri cu impact major au avut loc asupra infrastructurilor critice de stat [2], care au fost posibile datorită RCE, precum sunt atacurile asupra bazelor de date ale poliției chineze din iulie 2022, care au compromis peste 1 miliard de înregistrări; distribuitorilor de gaze din Grecia din august 2022, care au provocat o întrerupere a sistemului de distribuție; site-urilor web din sectorul public și privat ale Ministerului Apărării din România, poliției de frontieră, Companiei naționale de căi ferate și a unei bănci comerciale care nu au fost disponibile o perioadă de timp; Guvernului Ucrainei prin compromiterea computerele agențiilor guvernamentale [6].

Conform raportului prezentat de Microsoft și Check Point Software [7], furnizorul multinațional de soluții pentru securizarea organizațiilor, cele mai vizate industrii, în 2022, au fost sectorul educației și cercetării, sectorul TIC (Tehnologia Informației și a Comunicațiilor) și organizațiile non-guvernamentale. Deși riscurile cibernetice aferente domeniului educațional sunt foarte ridicate, cercetările privind abordarea sistemică a procesului de asigurare a securității CE și implementarea cadrelor de securitate sunt limitate [8, 9], la fel, și atenția din partea autorităților centrale [10]. Cu toate că domeniul educației nu face parte din infrastructura critică de stat, gestionează totuși un volum imens de date sensibile, așa ca datele personale, rezultatele cercetărilor și proprietatea intelectuală, iar digitalizarea instituțiilor, mai ales ca urmare a pandemiei Covid-19, a avut loc în ritm alert.

Un rol important în acest sens îl are Guvernul, care poate influența abordarea problemelor aferente securității CE și armonizarea strategiilor de securitate cu standardele industriale, pentru a se asigura conformitatea și recunoașterea internațională [11], prin emiterea recomandărilor și politicilor la nivel superior, în special în cazul instituțiilor publice, așa cum sunt și instituțiile de învățământ superior (IÎS).

Scopul și obiectivele cercetării: scopul prezentei teze de doctor ***este de a realiza cercetări privind elaborarea unui cadru sistemic de securitate a CE (CSSCE), care va contribui la securizarea rețelelor și serviciilor de comunicații electronice în instituțiile de învățământ superior din Republica Moldova.***

Astfel, pentru realizarea scopului tezei au fost determinate următoarele obiective de cercetare:

1. *Identificarea și analizarea problemelor de securitate ce se referă la rețelele și serviciile de CE, la nivel național și internațional, cu accent pe instituțiile de învățământ superior.*
2. *Analiza situației actuale privind securitatea rețelelor și serviciilor de CE în instituțiile de învățământ superior din Republica Moldova.*
3. *Selectarea metodei științifice de elaborare a cadrului sistemic de securitate a CE orientat spre îmbunătățirea procesului educațional academic al instituțiilor de învățământ superior din Republica Moldova.*
4. *Elaborarea cadrului sistemic de sporire a securității CE pentru instituțiile de învățământ superior din Republica Moldova în baza prevederilor standardului internațional ISO 27001 și contextul CSSCE.*
5. *Evaluarea cadrului sistemic de securitate a CE pentru instituțiile de învățământ superior din Republica Moldova conform criteriilor de valoare.*

Ipoteza cercetării: definirea, elaborarea și implementarea cu succes a măsurilor de securizare a comunicațiilor electronice în IÎS cu eforturi rezonabile (umane, financiare, materiale etc.) poate fi soluționată printr-o abordare sistemică a problemei. Un cadru sistemic de securitate a comunicațiilor electronice reușit, bazat pe identificarea și sistematizarea aspectelor definitorii și controlul riscurilor de securitate, ar putea servi ca bază metodologică ce ar facilita și eficientiza elaborarea/dezvoltarea și implementarea de către fiecare IÎS din Republica Moldova a propriului sistem de securitate holistic și scalabil. De asemenea, acesta ar oferi un suport semnificativ pentru certificarea sistemelor de securitate ale IÎS conform standardului ISO 27001.

Metodologia cercetării științifice: pentru a realiza scopul și obiectivele de cercetare ale tezei au fost utilizate astfel de tehnici ca studiul contextual, conceptual și empiric pentru care au

fost selectate metode științifice relevante, care au permis obținerea rezultatelor științifice teoretice și practice.

Pentru studiul contextual a fost efectuată analiza literaturii, conform metodei propuse de Kitchenham [12], completată cu următoarele metode: observația, abstractizarea, analiza și sinteza studiilor științifice relevante domeniului cercetat.

La baza dezvoltării Cadrului Sistemic de Securitate a CE a stat studiul conceptual, iar ca metodă principală în această etapă a fost utilizată Cercetarea în Știința Proiectării DSR (Design Science Research) [13]. Metoda complementară utilizată pentru operaționalizarea cadrului este Ingineria Cerințelor de Securitate SRE (Security Requirements Engineering) [14]. De asemenea, pentru dezvoltarea cadrului sistemic a fost utilizat modelul Clements–Hoffman, care descrie necesitatea abordării sistemice a securității CE.

Pentru studiul empiric a fost utilizată metoda de cercetare Delphi [15], care a permis perfectarea și evaluarea cadrului propus, deoarece se potrivește pentru obținerea recomandărilor experților, când se proiectează un nou cadru sau model. Pentru validarea CSSCE au fost utilizați indicatorii statistici: media, deviația standard și coeficientul de concordanță al lui Kendall [16]. Metoda Delphi a fost combinată cu metode calitative, așa ca interviurile semistructurate, și cu metode cantitative, așa ca sondajul bazat pe chestionare. Studiul de caz a fost utilizat pentru a simula procesul de implementare a CSSCE.

Noutatea și originalitatea științifică

Rezultatele științifice obținute în prezenta teză se referă la următoarele:

- definirea conceptului de securitate a comunicațiilor electronice (CE) și dezvoltarea bazelor de cunoștințe aferente domeniului cercetat;
- elaborarea cadrului sistemic de securitate a CE (CSSCE) și a metodologiei de evaluare a riscurilor de securitate, dezvoltarea unei aplicații prototip pentru reflectarea procesului de implementare a CSSCE în mediul universitar național.

Noutatea și originalitatea științifică a elaborării CSSCE constă în faptul că până la momentul actual în literatura de specialitate nu a fost expusă o astfel de abordare sistemică și cuprinzătoare a procesului de asigurare și îmbunătățire a securității CE în IÎS.

Teoretic, studiul va contribui la înțelegerea problemei securității CE existente în mediul academic; înțelegerea amenințărilor de securitate și analiza diferitor standarde și cadre de securitate dezvoltate și implementate până în prezent pentru managementul securității; identificarea etapelor de implementare a cadrelor de securitate care abordează sistemic problemele în domeniu.

Practic, analiza cercetării și constatările studiului vor informa administrațiile universităților și Guvernul Republicii Moldova despre importanța abordării sistemice a problemelor de securitate a CE în mediul academic; rezultatele cercetării vor ghida practicienii în domeniu asupra acțiunilor sistemice de securizare a tehnologiilor comunicaționale.

Problema științifică soluționată. Analiza publicațiilor științifice și a cadrelor normative naționale și europene au permis a formula problema științifică care constă în ***elaborarea unui cadru sistemic național de securitate a comunicațiilor electronice pentru instituțiile de învățământ superior din Republica Moldova, care ar asigura abordarea holistică a problemelor ce se referă la securitatea CE, prioritare la nivel internațional în ultimii ani***.

Astfel, problema științifică soluționată constă în elaborarea cadrului sistemic de securitate a CE la nivel superior, orientat spre specificul RCE universitare ce posedă caracter scalabil, pentru a fi ușor adaptat de orice IÎS națională, în dependență de complexitatea serviciilor academice electronice pe care le prestează și de infrastructura RCE. Cadrul sistemic de securitate se referă atât la aspectele organizaționale, așa ca stabilirea contextului și determinarea domeniului de aplicare, cât și la aspectele operaționale așa ca elaborarea politicilor de securitate, identificarea activelor informaționale, identificarea obiectivelor de securitate și dependența de sistem, identificarea amenințărilor de securitate, evaluarea riscului de securitate, identificarea cerințelor de securitate și completarea unui depozit cu controale de securitate relevante, care susțin asigurarea securității după modelul de sus în jos. Prototipul aplicației dezvoltate contribuie la evaluarea nivelului de implementare a cadrului sistemic de securitate și la determinarea cerințelor de securitate comune pentru domeniul educațional.

Publicații științifice. La tema tezei de doctor au fost publicate 11 lucrări științifice dintre care 6 articole ca autor principal și 5 articole semnate numai de autorul tezei; 6 publicații în reviste științifice de specialitate, dintre care 3 în străinătate și 3 în reviste naționale de categoria B+; 2 lucrări au fost prezentate la conferințe internaționale din străinătate, dintre care 1 a fost indexată în SCOPUS și 3 la conferințe internaționale care au avut loc în Moldova. Lista lucrărilor științifice publicate poate fi analizată în anexa 1 a tezei.

Structura tezei. În introducerea tezei de doctor a fost descrisă actualitatea temei, identificate scopul cercetării, obiectivele de realizat și problema științifică. Au fost descrise metodele științifice care au contribuit la identificarea soluției și descrisă noutatea și originalitatea științifică, precum și publicațiile la tema tezei de doctor.

În capitolul 1, ***Securitatea comunicațiilor electronice***, sunt definiți termenii specifici domeniului, este analizată problema securității CE în IÎS, sunt descrise provocările și principalele amenințări de securitate asupra RCE academice la nivel internațional. Au fost analizate cadrele

normative naționale și europene, ceea ce a contribuit deopotrivă cu studiul empiric al situației actuale în IÎS din Republica Moldova la identificarea problemei științifice și la stabilirea sarcinilor.

În capitolul 2, ***Metodologia de dezvoltare a Cadrului Sistemic de Securitate a Comunicațiilor Electronice***, au fost definite obiectivele și criteriile de valoare conform căruia urmează a fi evaluat CSSCE și realizat un studiu profund pentru a identifica standarde/cadre aplicabile privind managementul securității și al riscurilor de securitate recomandate de cercetători, cunoștințe utilizate ulterior la dezvoltarea CSSCE. De asemenea, au fost descrise metodele și materialele utilizate pentru dezvoltarea și evaluarea CSSCE.

În capitolul 3, ***Cadrul Sistemic de Securitate a Comunicațiilor Electronice universitare,*** a fost definit conceptul de securitate a CE și analizat modelul formal ce descrie sistemele de securitate, pentru a reprezenta grafic interacțiunea dintre elementele-cheie ale sistemelor de securitate și a argumenta implementarea CSSCE ca proces sistemic. Astfel, abordarea sistemică s-a bazat pe ciclul lui Deming. Dezvoltarea CSSCE a avut loc pe două dimensiuni: organizaționale (conform ISO 27001 [17]) și operaționale prin aplicarea metodei științifice SRE și a indicatorilor-cheie de performanță după care poate fi evaluată obiectiv securitatea. Au fost elaborate listele de verificare pentru elementele-cheie ale sistemului de securitate universitar: active de suport, amenințări generice și specifice și cerințe de securitate. A fost prezentat prototipul instrumentului i-CSSCE dezvoltat conform etapelor de implementare a CSSCE.

În capitolul 4, ***Evaluarea Cadrului Sistemic de Securitate a Comunicațiilor Electronice universitare***, este expus studiul de caz pentru a simula implementarea CSSCE în cadrul unei facultăți, utilizând instrumentul i-CSSCE. Sunt descrise rezultatele sondajului final, pentru care au fost create 2 paneluri de respondenți: în panelul 1 – experți naționali în domeniu din companiile RM și străinătate: în panelul 2 – specialiștii responsabili din IÎS. A fost aplicată tehnica Delphi prin care a fost evaluat prototipul CSSCE, conform criteriilor de evaluare stabilite în capitolul 2 al tezei.

În compartimentul ***Concluzii finale și recomandări*** sunt descrise rezultatele științifice obținute, contribuțiile privind bazele teoretice și practice/aplicative. De asemenea, sunt descrise implicațiile, limitările și recomandările pentru cercetările viitoare.

1. SECURITATEA COMUNICAȚIILOR ELECTRONICE

Tehnologiile de comunicații electronice actualmente înregistrează un ritm dinamic de dezvoltare și modificare continuă, aducând pe de o parte oportunități de acces rapid la informații și comunicare, utilizând canale integrate [18], iar pe de altă parte, natura dinamică de dezvoltare generează noi provocări în asigurarea securității CE.

Pentru a aduce justificări și raționamente bazate pe studiile științifice, utilizate ulterior pentru formularea problemei de cercetare din această teză de doctor, acest capitol se va concentra pe analiza domeniului cercetat, identificarea legislației naționale și internaționale, studiul empiric.

1.1. Considerații generale și termeni specifici domeniului

CE au fost definite prin ”Electronic Communications Privacy Act” ca și comunicații de date transmise atât prin sisteme cu fir, cât și prin sisteme fără fir [19]. De asemenea, CE se referă la orice informație trimisă între anumite părți prin liniile de telefon sau utilizând conexiunea la internet [20]. O definiție care extinde termenul face referire la CE ca totalitatea formelor de comunicații prin mijloace electronice, inclusiv, dar fără a se limita la comunicații prin linie fixă, telefon mobil, fax, internet, cablu sau satelit [18]. Totalitatea tehnologiilor, serviciilor, sistemelor sau alte resurse care furnizează sau asigură transmiterea datelor sau informațiilor în format electronic formează CE [21]. CE sunt deseori utilizate interschimbabil cu termenul ”telecomunicații”, prefixul ”tele” semnificând comunicarea de la distanță între două dispozitive terminale [21]. CE pot fi clasificate după modul în care are loc comunicarea între punctele terminale, ca fiind unidirecționale (simplex) sau bidirecționale (semiduplex, full-duplex), cât și după tipul semnalului transmis: analogice sau digitale [22]. Anume tranziția spre tehnologiile comunicaționale digitale a reprezentat fundamentul pentru integrarea sistemelor CE și a rețelelor de calculatoare. Exemple de comunicații electronice unidirecționale pot servi difuzarea radio și TV, televiziunea digitală, telemetria, internetul obiectelor (IoT) etc., iar de comunicații bidirecționale sunt serviciile de telefonie, radio bidirecțional, internetul, rețelele WAN, LAN, MAN [22]. Procesul de comunicații electronice include mai multe elemente, după cum este reflectat în figura 1.1.

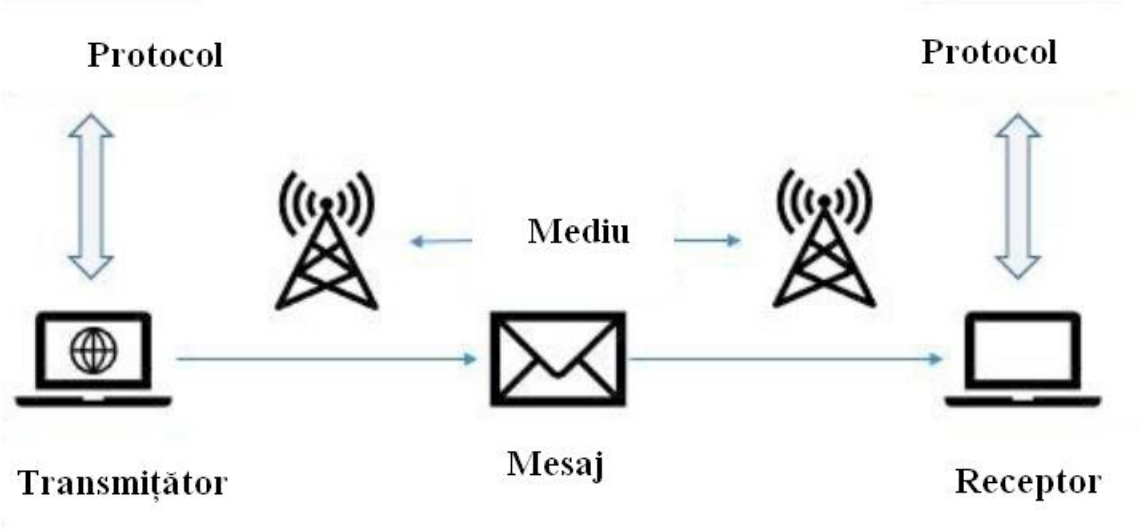

Fig. 1.1. Procesul CE (adaptat după [23]**)**

Transmițător poate fi orice dispozitiv capabil să trimită date, mesajul reprezintă orice date transmise prin mediile de CE, receptorul reprezintă orice dispozitiv care poate prelua mesajul, protocoalele determină regulile după care va avea loc întreg procesul, fără protocoale CE nu ar fi posibile [23] lățimea de bandă specifică, capacitatea maximă a transferului de date. Sistemele de CE reprezintă ansamblul tuturor elementelor care asigură procesul transferului de date, iar internetul reprezintă în acest sens, cel mai mare sistem de CE [22].

CE se referă la serviciile (SCE) și rețele (RCE). Mai mult ca atât, prin Legea RM, nr.241 din 15.11.2007, cu privire la CE, este stipulat că crearea RCE se realizează cu scopul furnizării SCE [24]. RCE au fost definite ca ansamblul echipamentelor de comunicații (calculator, laptop, telefon, televizor) interconectate prin intermediul mediilor fizice de transmisie (cablu torsadat, coaxial sau optic, linie telefonică etc.), în scopul comunicării folosind semnale voce, video sau de date, dar și a utilizării în comun a resurselor fizice, logice și informaționale ale rețelei de către un număr mare de utilizatori [25]. Definiția expusă în Legea nr. 241/2007, din 15.11.2007, cu privire la CE [24], descrie RCE ca ”*sisteme de transmisie şi, după caz, echipamente de comutare sau rutare, precum şi alte resurse care permit transmiterea semnalelor prin suport fizic, electromagnetic sau prin orice alte mijloace, incluzând reţele de comunicaţii prin satelit, reţele fixe (cu comutare de circuite sau comutare de pachete, inclusiv Internet) şi reţele mobile terestre, reţele de transport al energiei electrice, în cazul în care acestea sunt utilizate şi pentru transmiterea semnalelor, reţele utilizate pentru difuzarea programelor audiovizuale, reţele de televiziune prin cablu, indiferent de tipul informaţiei transmise”*. O abordare similară atestăm și în recomandările cu privire la termeni și definiții specifice domeniului prezentate de Uniunea Internațională pentru Telecomunicații (ITU), care definesc RCE ca fuziunea tuturor mijloacelor

de furnizare a SCE între un număr de locații în care dispozitivele oferă acces la aceste servicii [26]. Anume această definiție este preluată de către autorul acestei teze de doctor ca referință. Dispozitivele care oferă acces la SCE sunt dispozitivele terminale cum ar fi calculatoarele, laptop-urile, serverele, tabletele, televizoarele, fax-urile, telefoanele etc. Mijloacele prin care are loc furnizarea SCE se referă în primul rând la dispozitivele de rețea: switch-urile (comutatoarele) care interconectează local mai multe dispozitive terminale; ruterele utilizate pentru interconectarea mai multor rețele; punctele de acces care permit conectarea wireless și extinderea ariei de acoperire a RCE; modem-uri ce permit accesul utilizatorului la Internet, cât și la mediile de conexiune: fibră optică, cablul de cupru sau undele radio. SCE permit utilizatorilor să transmită sau să primească informații publice sau private, pentru a efectua diverse operațiuni, așa ca: încărcarea/descărcarea fișierelor, tranzacții comerciale sau bancare etc. [26], cel mai comun SCE fiind accesul la Internet [20]. Conform [25], RCE au fost clasificate în rețele de telefonie fixă, rețele de comunicații mobile, rețele de radio și televiziune, rețele de comunicații prin satelit și rețele de calculatoare.

Comunicațiile dintre echipamentele interconectate fizic și logic se realizează prin protocoale de comunicație. RCE actuale, bazate pe transmisiunile de date, folosesc protocolul Internet și stiva protocoalelor TCP/IP, iar tendințele arată că și rețelele mobile de CE, bazate pe o singură tehnologie, așa ca GSM sau CDMA, sunt în tranziție spre platforme eterogene în baza protocolului IP [27].

Una dintre preocupările majore ale organizațiilor, care se ocupă cu reglementări și standarde în domeniul telecomunicațiilor, este securitatea, ce rămâne a fi domeniul pentru care încă urmează să se elaboreze standarde [27], deoarece odată cu intensificarea utilizării standardelor deschise și a stivei protocoalelor TCP/IP, atacurile bazate pe rețea s-au intensificat [28]. Securitatea CE se referă la protecția tehnologiilor comunicaționale și a conținutului lor [22; 29]. Aceasta are ca scop prevenirea accesului neautorizat în zonele securizate legate de CE, atenuarea riscurilor aflate în afara controlului, prevenirea furnizării informațiilor inexacte sau incorecte și oprirea SCE [18]. Cercetători din Republica Moldova consideră că securitatea CE este relevantă rețelelor și tehnologiilor moderne ale informației, așa ca Internet, Intranet, Extranet, Web, VPN (rețele virtuale private) [30]. RCE sunt parte constituentă a infrastructurilor informaționale de stat, care la rândul său reprezintă componenta de bază a societății informaționale [31]. Securitatea CE poate fi atinsă prin securizarea tuturor elementelor bazate pe rețea [32], ce necesită un nivel înalt de securizare de care depinde atât securitatea dispozitivelor terminale și de rețea, cât și securitatea informației [29]. În articolul 2(21) al Directivei (EU) 2018/1972 cu privire la instituirea Codului european al CE, securitatea se referă la capacitatea RCE și SCE de a rezista, cu un anumit nivel de încredere, oricăror acțiuni care vizează confidențialitatea, integritatea și disponibilitatea RCE și

SCE, a datelor stocate, transmise sau prelucrate, sau a serviciilor conexe livrate sau accesibile prin rețelele și serviciile de CE [33].

Securitatea CE este parte a securității cibernetice, care acționează ca și termen-umbrelă, fiind cel mai utilizat termen aferent domeniului [2], ce poate fi definit ca ”securitate a spațiului cibernetic, care este un mediu complex ce apare ca urmare a interacțiunii dintre oameni, software și servicii de internet furnizate prin rețelele integrate” [34]. NIST se referă la spațiul cibernetic ca și la un mediu prin care este transmisă informația prin RCE [35]. Într-o abordare mai completă, spațiul cibernetic este definit ca ”domeniu global în mediul informațional, constând din rețele interdependente de infrastructuri ale sistemelor informaționale, inclusiv internetul, RCE, sistemele de calculatoare, procesoarele și controlerele încorporate” [35]. Astfel, din definițiile prezentate mai sus se poate conclude că securitatea cibernetică reprezintă o proprietate a RCE interconectate, a serviciilor electronice, deoarece partea esențială a spațiului cibernetic sunt rețelele și serviciile de CE. Securitatea cibernetică poate fi utilizată ca termen interschimbabil cu securitatea informației, acolo unde se referă la protecția informației din mediile cibernetice [2]. Astfel, principiile fundamentale pentru ambii termeni, adică, confidențialitatea, integritatea și disponibilitatea, sunt relevanți domeniului mai îngust așa ca cel al securității CE.

Deopotrivă cu datele din sistemele informaționale și rețelele de calculatoare care trebuie asigurate constant cu un anumit nivel de securitate, RCE care de cele mai dese ori sunt aceleași rețele, trebuie să fie asigurate cu un nivel optim de securitate [21]. Drept argument pot servi cerințele pentru parolele de acces în sistemele IT, care sunt identice cu cerințele pentru parolele de acces la tehnologiile de CE, cu excepția tehnologiilor care nu dețin o astfel de capabilitate, precum sunt telefoanele [36].

Asigurarea securității CE se referă atât la aspectele organizatorice, cât și la aspectele tehnice care necesită a fi luate în considerație [27, 33, 37]. Abordarea sistemică și centrată pe tipul organizației are un rol definitoriu, deoarece gândirea sistemică poate oferi cadre conceptuale în care componentele, factorii ce influențează și mediile sunt integrate dinamic [38], ceea ce permite abordarea problemelor organizației legate de complexitate, interoperabilitate și impredictibilitate; strategiile de securitate propuse organizațiilor sunt diferite, deoarece fiecare organizație este unică [39].

Securitatea nu poate fi absolută, deoarece nu reprezintă un scop în sine, ci mai degrabă un proces continuu de implementare și îmbunătățire [27, 29]. Mai mult ca atât, securitatea trebuie să includă toate straturile unui sistem, care fiind combinate cu un management puternic și aplicarea politicilor de securitate, să ofere un set de soluții de securitate modulare, flexibile și scalabile [27]. Fundamentele securității CE reprezintă ansamblul principiilor fundamentale ale securității, RCE

și protocoalelor utilizate, cerințelor de securitate implementate pentru diminuarea sau atenuarea impactului atacurilor cibernetice [28]. Cerințele de securitate pentru CE nu sunt fenomene izolate, ci necesită a fi abordate ca și caracteristici esențiale și critice ale tehnologiilor comunicaționale [21]. Tehnologiile comunicaționale se referă la orice dispozitiv sau produs program care asigură comunicarea între elementele separate ale sistemelor informaționale [40]. Securitatea CE nu poate fi abordată ca un fenomen izolat, deoarece CE sunt parte constituentă esențială și critică, deopotrivă cu Tehnologia Informației a Societății Informaționale [21]. Pentru a înțelege provocările de securitate ale CE, este necesar mai întâi a identifica care sunt totuși activele la care se referă. În acest sens, în recomandările ITU-T X.1057 [41] se conține clasificarea activelor bazate pe CE, după categoriile reflectate în figura 1.2.

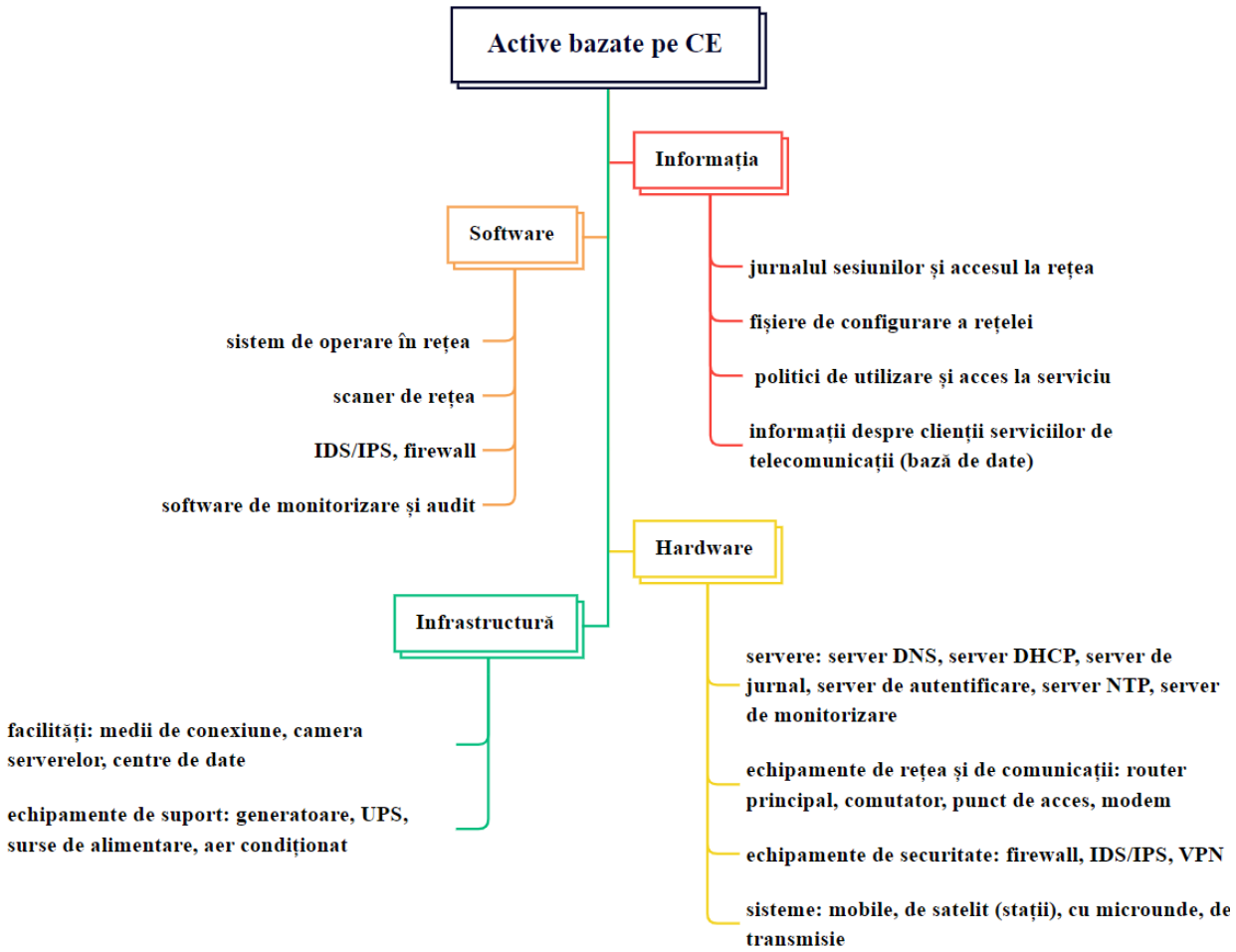

Fig. 1.2. Active bazate pe CE [41]

Dispozitivele de rețea, așa ca ruter, switch, modem, punct de acces, sunt responsabile de asigurarea securității comunicațiilor, deoarece problemele specifice de securitate se atestă anume în nodurile rețelei [25].

Arhitecturile de securitate propuse pentru sistemele de CE au evoluat din anii ’80 până în prezent, de la o abordare a securității bazată pe nivelurile modelului OSI (Open Systems Interconnection), confirmare fiind documentul X.800 [42], emis de ITU, până la arhitecturile de securitate a comunicațiilor end-to-end, bazate pe aplicații, reflectate în documentul X.805 [43], emis de ITU. Argumente relevante pentru migrarea spre sistemele de comunicații end-to-end au fost publicate încă din 1984 [44]. În lucrare au fost abordate problemele de securitate a sistemelor de comunicații și au fost prezentate argumente prin care s-a demonstrat că securizarea dispozitivelor intermediare din RCE nu este suficientă, fără a aborda și securitatea dispozitivelor terminale și a aplicațiilor care rulează pe acestea, deoarece este vorba nu de fenomene izolate, ci de întregul sistem de comunicații [44]. Astfel, arhitectura de securitate end-to-end este bazată pe 3 straturi (niveluri) [27]:

- ***Stratul de infrastructură*** care se referă la elementele esențiale ale RCE și la serviciile și aplicațiile acestora. Drept exemple pot servi dispozitivele terminale și intermediare de rețea și mediile de comunicații.
- ***Stratul de servicii*** care se referă la serviciile de CE prestate consumatorului final, ce pot varia de la serviciile de bază, așa ca conectarea la rețeaua globală, până la servicii cu valoare adăugată, așa ca stocarea în cloud.
- ***Stratul de aplicații*** care se referă la aplicațiile bazate pe rețea, utilizate de către consumatori, care pot varia de la aplicații simple, cum este poșta electronică, până la aplicații de vizualizare colaborativă, ce permit contribuția în comun a mai multor utilizatori pentru dezvoltarea anumitor proiecte, ca de exemplu în domeniul cercetării [45].

1.2. Amenințări de securitate ale comunicațiilor electronice

Practic, toate organizațiile contemporane utilizează comunicațiile electronice pentru transferul de date, ceea ce le face extrem de atractive pentru infractorii cibernetici [23].

Sursa amenințărilor de securitate ale RCE bazate pe protocolul Internet variază de la amenințările pe care le prezintă utilizatorii, sistemele informaționale, dispozitivele terminale până la producătorii tehnologiilor de CE [27]. Deși există tendința de a dezvolta sisteme de securitate a CE în jurul tehnologiilor, cea mai mare vulnerabilitate o prezintă totuși utilizatorul [21]. Amenințările de securitate ce provin din afara RCE sunt specifice spațiului cibernetic, deci, și riscurile sunt cibernetice. Sursa amenințărilor de securitate externe sunt utilizatorii și dispozitivele terminale, producătorii de echipamente de CE, sistemele informaționale, părțile terțe, care pot influența asupra securității CE prin 5 tipuri de amenințări de securitate, după ITU-T X.800 și ITU-T X.805, ce constau în *deteriorarea informației și a tehnologiilor de comunicații, coruperea sau*

modificarea informației, furtul, ștergerea sau pierderea informației și a tehnologiilor de CE, întreruperea serviciilor și divulgarea informației [27]. Atacurile cibernetice care au drept țintă tehnologiile de CE au fost clasificate în *atacuri de întrerupere a serviciilor de CE*, *compromiterea activelor importante*, *atacuri de deturnare a dispozitivelor intermediare de rețea* și *preluarea controlului asupra acestora*, *atacurile de impersonare*, *atacurile cu programe malițioase*. Exemple relevante în acest sens pot fi analizate în figura 1.3.

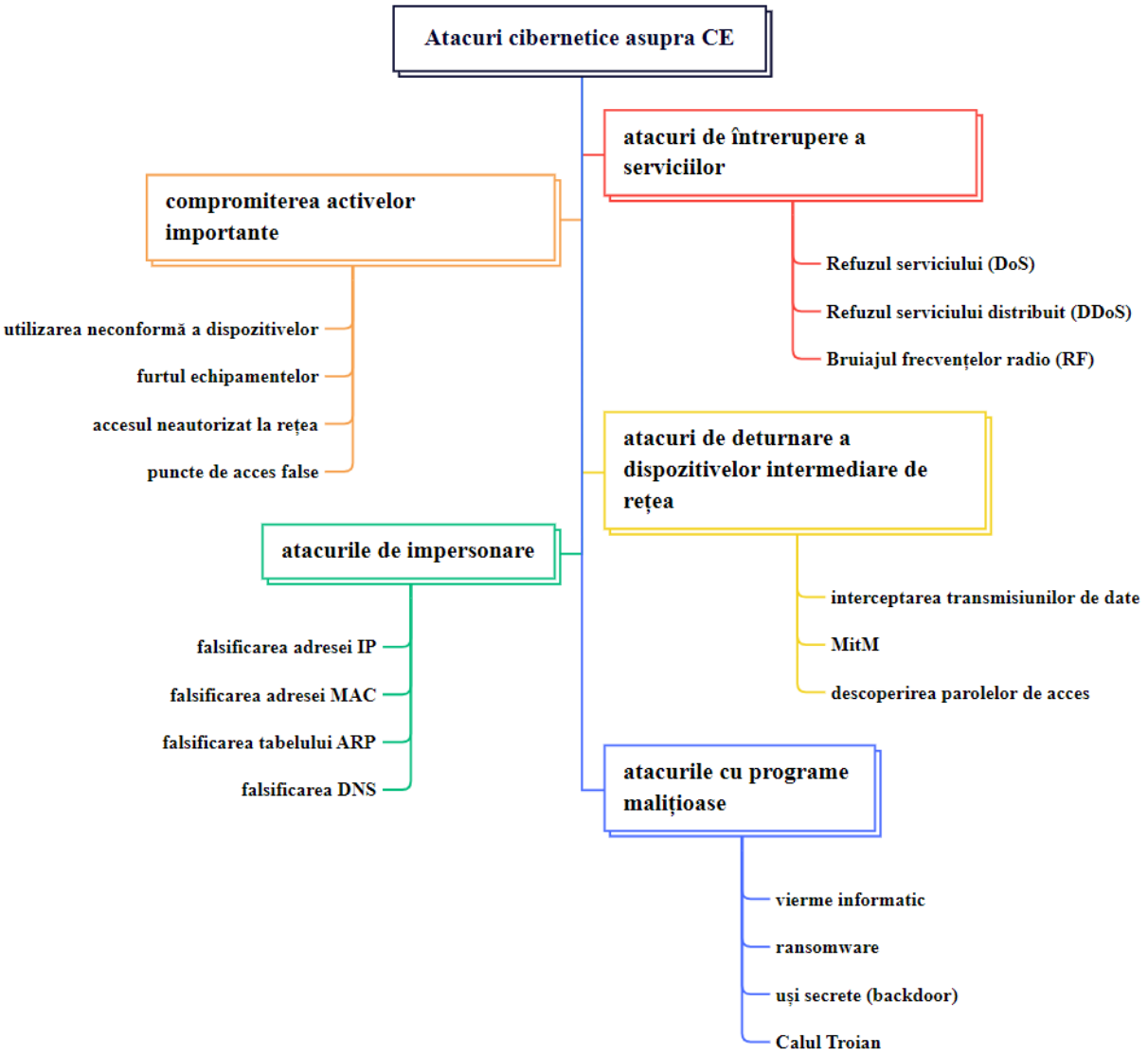

Fig. 1.3. Atacuri cibernetice asupra CE

Cel mai des întâlnit atac cibernetic de inundare este atacul de refuz al serviciului DoS sau DDoS. Ținta atacurilor DoS/DDoS sunt dispozitivele de rețea așa ca ruterele și comutatoarele, serverele și dispozitivele terminale. Atacurile de tip DoS/DDoS au loc prin inundarea cu pachete ale RCE sau prin transmiterea de pachete formatate incorect [46, 47, 48]. Inundarea cu pachete are loc prin transmiterea pachetelor TCP SYN, ICMP sau UDP la nivelul 4 OSI [49]. Creșterea

capacității de transfer a datelor prin rețeaua globală Internet a facilitat și creșterea volumului de trafic pentru atacurile DDoS de inundare, astfel încât dacă în 2002 cel mai mare atac înregistrat a fost de aproximativ 1 Gbps, în 2018, cel mai mare atac înregistrat de către sistemul de date ATLAS privind traficul global a fost de 1.7 Tbps, intentat asupra unui furnizor de servicii din SUA. Așadar, se înregistrează o creștere majoră a capacității pentru atacurile DDoS pe parcursul ultimilor 18 ani.

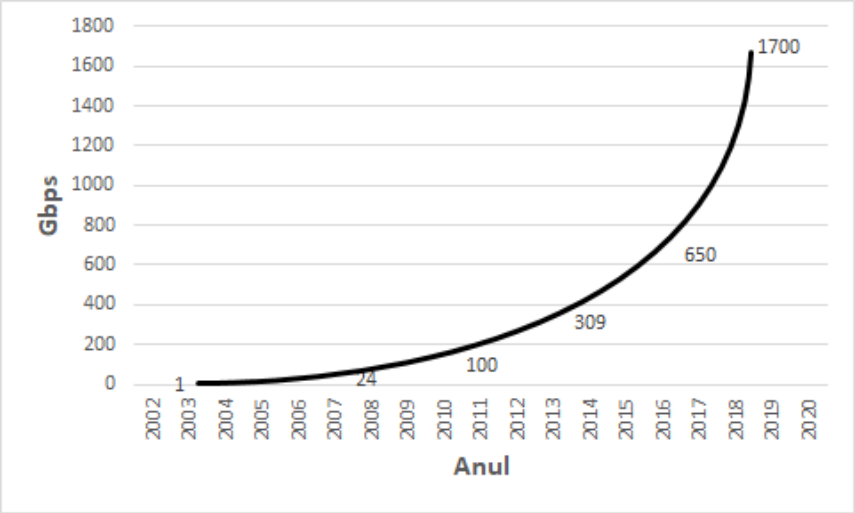

Fig. 1.4. Consumul de bandă în urma atacurilor de tip DoS/DDoS din ultimii 18 ani (sursa datelor NETSCOUT Arbor [50]**)**

De asemenea, a fost înregistrată o creștere semnificativă, începând cu anul 2021, a atacurilor de tip DDoS ce consumă mai mult de 50 Gbps, ceea ce poate duce la indisponibilitatea RCE a majorității organizațiilor.

Interceptarea transmisiunilor de date reprezintă atacuri pasive în RCE a căror scop este preluarea tuturor pachetelor, cu scopul descoperirii informațiilor sensibile, așa ca datele de autentificare ale utilizatorilor, conținutul email-urilor, numărul cardurilor de credit etc. Vulnerabile la astfel de atacuri sunt protocoalele serviciilor Internet de bază care transmit datele în mod clar, necriptat, așa ca HTTP, SMTP, POP, FTP, IMAP, Telnet. Pentru atacurile de interceptare se utilizează una dintre cele trei metode enumerate mai jos [51]:

- Interceptarea datelor bazată pe adresa IP a dispozitivului;
- Interceptarea datelor bazată pe adresa MAC a dispozitivului;
- Interceptarea datelor bazată pe protocolul ARP prin falsificarea adreselor de rețea.

De asemenea, atacurile de interceptare pot fi clasificate după nivelul modelului OSI la care funcționează, așa ca interceptarea sesiunilor TCP și UDP, de la nivelul 4 OSI, interceptarea după adresa IP sau port logic la nivelul 3 OSI, sau interceptarea după adresa MAC sau falsificarea ARP pentru preluarea pachetelor de date la nivelul 2 OSI [51].

Similare cu atacurile de interceptare sunt atacurile MitM (man in the middle), care sunt atacuri active, și pe lângă faptul că interceptează datele în tranzit, pot modifica conținutul pachetelor de date și modifica/șterge anumite date. La atacurile MitM sunt susceptibile diverse tehnologii, cu precădere cele bazate pe tehnologiile wireless. În literatura de specialitate [52] se disting 4 tipuri de atacuri MitM:

- MitM bazat pe falsificare prin care atacatorul interceptează pachetele de date prin falsificarea adreselor de rețea și controlează tot traficul de date transmis între 2 utilizatori; prin falsificarea DNS și a dispozitivelor intermediare de rețea sau prin compromiterea dispozitivelor terminale și falsificarea ARP.
- MitM bazat pe atacurile asupra protocoalelor TLS sau SSL prin care atacatorul intervine în comunicarea dintre 2 dispozitive terminale, pentru a intercepta și modifica transmisiunile de date.
- MitM bazat pe protocolul BGP prin care are loc preluarea neautorizată de către atacator a mai multor adrese IP, prin coruperea tabelelor de rutare și interceptarea comunicațiilor.
- MitM bazat pe crearea unor stații false și interceptarea datelor în tranzit; unul dintre cele mai comune astfel de atacuri sunt crearea punctelor de acces necinstite și a rețelelor ad-hoc.

Atacurile de impersonare reprezintă, de asemenea, mari provocări pentru securitatea rețelelor, după cum a fost expus mai sus, și pot să fie parte a altor atacuri sau să fie inițiate ca atacuri separate. Falsificarea adreselor logice de rețea reprezintă o tehnică comună utilizată împreună cu atacurile de tip DoS/DDoS și MitM, prin care atacatorul identifică victima, obține o IP adresă de încredere, dezactivează comunicarea cu una dintre sursele legitime prin lansarea unui atac de inundare cu pachete, modifică antetul pachetelor și încearcă conectarea la un serviciu sau port specific. În cazul când conexiunea a reușit, creează o ușă secretă (backdoor) [53]. Falsificarea adresei MAC este similară cu falsificarea adresei IP a dispozitivului. Falsificarea tabelei ARP, de asemenea, este o tehnică des întâlnită. Protocolul ARP potrivește adresa IP cu adresa MAC a dispozitivului dintr-o rețea locală pentru a cunoaște către care dispozitiv să fie direcționat traficul, iar prin falsificarea tabelului ARP, atacatorul se identifică în rețeaua locală ca fiind un dispozitiv legitim și primește traficul destinat dispozitivului autorizat din rețea. Falsificarea DNS utilizează diverse tehnici de inginerie socială și tehnici specifice atacurilor MitM [53] pentru a redirecționa traficul legitim spre un anumit server web fals prin modificarea informației despre rezoluția numelor de domeniu.

După cum se poate observa, majoritatea atacurilor în RCE au loc începând cu nivelul 2 OSI, însă sunt și câteva atacuri la nivelul 1 OSI, după cum este bruiajul frecvențelor radio (RF) în

rețelele fără fir, care utilizează undele radio pentru transmisiunile de date prin care are loc întreruperea transmisiunii semnalului între dispozitivele legitime [54].

De asemenea, un impact mare asupra RCE îl au tehnicile de inginerie socială [55], deoarece utilizatorul reprezintă una dintre principalele surse de amenințare pentru comunicațiile electronice. De nivelul de educație și informare a utilizatorului va depinde securitatea comunicațiilor electronice, deoarece una dintre cele mai mari provocări o reprezintă atacurile de phishing, prin email, care ca rezultat pot avea descărcarea de programe malițioase, așa ca ransomware, care pot cripta dispozitivele terminale, ceea ce poate duce la indisponibilitatea serviciilor RCE. Un exemplu notoriu de ransomware este viermele WannaCry, care în mai 2017, în doar câteva zile a infectat peste 200000 de computere în 150 de țări, blocând RCE ale spitalelor din Marea Britanie, sistemelor guvernamentale, rețelelor feroviare și a mai multor companii private [56]. Viermii sunt programe malițioase care se autoreplică în RCE. Alte programe malițioase capabile să modifice configurările dispozitivelor intermediare de rețea, de exemplu a ruterelor wireless, reprezintă de asemenea o mare provocare pentru securitatea CE. Un exemplu concludent este programul malițios VPNFilter, care, începând cu anul 2016, a infectat mai mult de jumătate de milion de rutere și dispozitive de stocare în rețea în 54 de țări [57]. Argumente relevante ale migrării programelor malițioase de la dispozitivele terminale și aplicații spre dispozitivele de CE sunt [58]:

- ruterele și punctele de acces sunt dispozitive mereu în funcțiune și conectate la Internet, astfel atacurile pot fi inițiate oricând;
- de cele mai dese ori, ruterele nu au capabilități de combatere și prevenire a infectării cu programe malițioase, spre deosebire de dispozitivele terminale;
- dispozitivele de rețea gestionează un număr mare de dispozitive terminale, astfel are loc infectarea mult mai rapidă a mai multor dispozitive simultan și cresc exponențial opțiunile de infectare;
- din păcate, utilizatorii cunosc mult mai puține informații despre securitatea dispozitivelor intermediare de rețea, utilizează parolele predefinite sau parole slabe, care nu sunt capabile să protejeze corespunzător;
- rețelele wireless extinse, utilizate actualmente din ce în ce mai mult, permit programelor malițioase să infecteze simultan mai multe rețele.

Tehnologizarea societății duce inevitabil la un interes sporit din partea atacatorilor, astfel încât numărul amenințărilor de securitate este în creștere cu fiecare zi. În datele din raportul cu privire la securitatea CE, pentru anul 2021, prezentate de ENISA, se specifică că cele mai afectate dispozitive ale RCE sunt ruterele, comutatoarele și serverele de adresare [59].

1.3. Dispozitive de securitate ale rețelelor de comunicații electronice

Componente esențiale ale sistemelor de securitate ale RCE sunt soluțiile tehnice implementate și configurate corespunzător, ghidate de politicile de securitate [29]. Inițierea procesului de stabilire a conexiunii între două dispozitive de comunicații trebuie să fie susținută cu cerințe specifice de securitate [25] încă de la început, prin implementarea cerințelor de securitate la fiecare nivel al modelului OSI, la care funcționează RCE.

Nivelul 1 al modelului OSI se referă cu precădere la asigurarea protecției fizice a dispozitivelor de rețea și a mediilor de conexiune, care trebuie fortificată încă în etapa de instalare a dispozitivelor de comunicații [32]. Dispozitivele electronice utilizate la acest nivel sunt: sursele neîntreruptibile de curent (UPS) și generatoarele, care ar asigura alimentarea continuă a dispozitivelor de comunicații; precum și alarmele sau încuietorile inteligente care ar limita accesul neautorizat la dispozitivele de comunicații.

La nivelul 2, legătura de date a modelului OSI, la care are loc adresarea fizică și configurarea dispozitivelor de rețea, precum sunt switch-urile, pot fi instalate dispozitive ca sistemele de detecție a intruziunilor (IDS) [32]. IDS constau din soluții pasive de analiză, clasificare și raportare a evenimentelor de rețea nedorite [25]. IDS analizează traficul de date cu scopul de a identifica anomalii și tentative de modificare a semnăturilor aplicațiilor și sunt eficiente în atenuarea atacurilor de tip DoS/DDoS, alertând sistemul de securitate sau administratorul, însă incapabil să oprească atacurile cibernetice. Alertele pot fi sunete specifice, semnale luminoase sau avertismente pe email [29]. Toate aceste capabilități pot fi gestionate cu precădere în RCE de dimensiuni mici, însă când este vorba despre organizații mari, care gestionează mii de dispozitive de CE, procesul de soluționare a riscurilor de securitate trebuie să fie automatizat [25]. În acest sens, o extensie a IDS sunt sistemele de detecție și prevenire a intruziunilor (IDPS), care sunt soluții active, capabile să prevină intruziunea neautorizată în RCE prin intermediul unui răspuns activ [29]. IDPS funcționează atât la nivel de rețea, cât și la nivel de gazdă. IDPS bazate pe rețea examinează traficul de comunicații. Există două tipuri de IDPS la nivel de rețea: wireless IDPS, utilizat pentru rețelele wireless și NBA (network behavior analysis) IDPS care analizează traficul pentru a recunoaște evenimentele anormale cum ar fi atacurile DDoS, programele malware, violarea politicilor de securitate [29]. IDPS bazate pe gazdă protejează dispozitivele terminale de rețea prin monitorizarea utilizatorilor conectați și a fișierelor stocate în sistem.

Nivelul rețea stabilește cum are loc rutarea pachetelor de date, fiind nivelul la care operează ruterele și adresarea logică. Astfel, la acest nivel, configurarea ruterelor prin implementarea listelor de acces al controlului (ACL) și filtrarea pachetelor de date [32] este esențială pentru un sistem de securitate robust.

La nivelul Transport, al modelului OSI, continuă să funcționeze regulile de configurare setate pe rutere, dar și capabilitățile dispozitivelor electronice, precum sunt firewall-urile [32], care controlează procesul de comunicație dintre rețeaua internă și externă, implementând politicile de securitate a rețelei securizate [25]. Firewall pot fi dispozitive electronice, servicii de securitate integrate pe rutere sau aplicații instalate pe sistemul de operare al dispozitivelor terminale. După modul de procesare, firewall pot fi clasificate în firewall de filtrare a pachetelor, firewall proxy de nivel aplicație, firewall de nivel control al accesului media și hibrizi [29]. Utilizați în practică sunt firewall hibride, deoarece sunt utilizate multiple abordări în procesul de implementare [29].

Alte dispozitive de securitate utilizate pentru protecția RCE sunt UTM (Unified Threat Management), considerate a fi firewall de generația următoare și dispozitive multifuncționale, care includ: funcționalul IDPS și a firewall de filtrare a pachetelor, protecție ziua-zero, filtrarea proxy a aplicațiilor, filtrarea emailurilor, controlul accesului la RCE și servicii prin VPN; și serverele de gestionare a dispozitivelor terminale, responsabile de monitorizarea tuturor dispozitivelor terminale din rețea, capabile să restricționeze accesul dispozitivelor la rețea, dacă acestea nu îndeplinesc cerințele prestabilite, ca de exemplu sisteme de operare și programe antivirus actualizate.

1.4. Cadrul normativ național și european cu privire la securitatea CE

Securitatea CE este tot mai importantă pentru Republica Moldova, ceea ce poate fi demonstrat prin mai multe inițiative legislative adoptate în ultimii 5 ani, justificate de nivelul înalt de dezvoltare a RCE [60]. Astfel, au fost aduse modificări Legii nr. 241 cu privire la CE, din 15-11-2007 [24], care au intrat în vigoare începând cu 17.11.2017, după publicarea în Monitorul Oficial al Republicii Moldova nr. 399-410, prin care a fost completată prezenta lege cu art. 21 și art. 22, care se referă la securitatea RCE și SCE, modificări aduse pentru armonizarea legislației Republicii Moldova la prevederile directivelor-cadru ale Uniunii Europene [24. 61]. Așadar, art. 21, punctul 1(a) se referă la totalitatea măsurilor tehnice și organizatorice pentru managementul riscului informațional, care poate afecta securitatea RCE și asigurarea unui nivel optim de securitate pentru a preveni sau diminua incidentele de securitate.

De asemenea, Hotărârea Guvernului nr.201 (HG.201) [62], din 28-03-2017, privind aprobarea Cerințelor minime obligatorii de securitate cibernetică (Cerințe Minime) care se aplică în cadrul Cancelariei de Stat, ministerelor, altor centre subordonate, autorităţi administrative ale Guvernului, inclusiv structurile organizatorice din sfera lor de competenţă (autorităţi administrative subordonate, servicii publice descentralizate şi subordonate, instituţii publice în care Cancelaria de Stat, minister sau altă autoritate administrativă centrală are statutul de fondator),

autorităţi administrative autonome şi unităţi autonome financiar; unde 22 din 28 de cerințe minime obligatorii se referă anume la securitatea RCE și a transmisiunilor de date. În HG. 201 este stipulată instituirea sistemelor de management al securității, desemnarea obligatorie a persoanei responsabile și atribuțiile persoanei desemnate din cadrul instituției, pct. 7 și 8.

De asemenea, problema securității CE este emergentă și la nivel european, astfel încât Codul european al CE a fost modificat prin Directiva 2018/1972 a Parlamentului European și a Consiliului Europei, din 11.12.2018 [33], deoarece noile condiții sunt impuse de progresul tehnologic. Punctele 94–98 din prezenta Directivă se referă în mod special la asigurarea securității rețelelor și serviciilor de CE pentru a reduce impactul evenimentelor de securitate prin luarea în calcul a riscului cibernetic. Drept condiție minimă, cerințele de securitate pentru RCE trebuie să ia în calcul următoarele elemente [33]: securitatea fizică și a mediului, securitatea aprovizionării, controlul accesului la rețele, integritatea rețelelor.

În mod direct este vizat factorul uman, deoarece trebuie să fie asigurate instruiri și informări cu privire la incidentele de securitate și măsuri pentru protecția utilizatorilor finali, acesta fiind elementul-cheie pentru asigurarea și menținerea nivelului optim de securitate în RCE.

Scopul 2(a) al Directivei 2018/1972 îl constituie securitatea rețelelor și serviciilor de CE [33], articolele 40 ”Securitatea rețelelor și a serviciilor” și 41 ”Punerea în aplicare și asigurarea respectării”. Se impun măsuri tehnice și organizaționale corespunzătoare și direct proporționale riscurilor cibernetice la adresa securității rețelelor și serviciilor de CE.

Directiva privind securitatea RCE și a informațiilor (Directiva NIS) reprezintă primul document adoptat de Parlamentul European și de Consiliul Uniunii Europene, la 6 iulie 2016. Directiva NIS prevede că toate statele-membre ale UE trebuie să atingă un nivel comun de securitate cibernetică, pentru a îmbunătăți securitatea CE, și acoperă următoarele domenii: asistență medicală, infrastructură digitală, transport, alimentare cu apă, furnizori de servicii digitale, infrastructură bancară și piața financiară, sectorul energetic [63].

Cu toate acestea, numărul amenințărilor de securitate a crescut considerabil în ultimii ani, astfel încât în strategia UE de securitate cibernetică, pentru anii 2020-2025, s-a propus revizuirea Directivei NIS prin actualizarea și extinderea acesteia la alte sectoare, dar și prin introducerea unor cerințe mai stricte de securitate, inclusiv sancțiuni la nivel european. Se dorește extinderea domeniului de aplicare prin obligarea mai multor sectoare de a implementa cerințe de securitate comune, care în rezultat ar duce la creșterea nivelului de securitate cibernetică în Uniunea Europeană. Astfel, în octombrie 2021, Parlamentul European a inițiat acest proces. Noul document valid pentru toate țările ce fac parte din Uniunea Europeană se numește NIS_2. Domeniile pe care le acoperă noua directivă NIS_2 sunt: CE, rețele sau servicii, gestionarea apelor și a

deșeurilor, fabricarea anumitor produse critice (cum ar fi produse farmaceutice, dispozitive medicale, produse chimice), alimente, servicii digitale, precum platforme de servicii de rețele sociale și servicii de centre de date, spațiu, servicii poștale și de curierat, administrație publică.

În raportul emis de ENISA, una dintre concluziile esențiale a fost că societatea modernă are în față o cale foarte lungă și anevoioasă până va atinge un nivel acceptabil al securității în mediul electronic [64]. Problemele de cercetare în domeniul securității cibernetice în general și a securității CE în particular sunt parte a priorităților Uniunii Europene [65].

1.5. Esența și particularitățile CE ale IÎS

RCE universitare sunt parțial deschise prin design [46, 66], descentralizate, multiutilizator și prezintă platforme importante pentru studiu, cercetare și inovare. IÎS utilizează comunicațiile electronice pentru a presta servicii educaționale, așa ca predarea, evaluarea, cercetarea, managementul, bibliotecile electronice, publicarea rezultatelor cercetărilor și conexiunea cu utilizatorii externi [67, 68, 69].

1.5.1. Specificul CE universitare

Rețelele de comunicații universitare reprezintă rețele IP autonome, gestionate de obicei de către IÎS, care pot fi amplasate în aceeași locație geografică, fiind rețele de comunicații ale LAN sau WLAN, sau în cazul când IÎS sunt dispersate pe campusuri, să includă și rețele ale CAN și MAN, sau chiar ale WAN [67]. Pentru managementul centralizat al rețelelor de CE universitare sunt utilizate conexiuni LAN și WAN [67].

Designul RCE diferă de la IÎS la IÎS [70], de la designul în cascadă (figura 1.5) la modelul ierarhic de organizare a RCE.

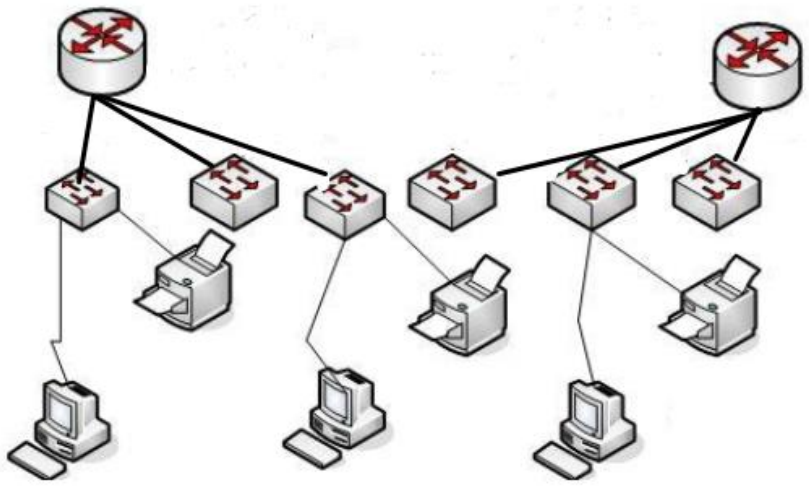

Fig. 1.5. Modelul cascadă

Configurarea RCE în cascadă devine totuși o problemă destul de dificilă, odată cu creșterea numărului de utilizatori ai Internetului, deoarece conectarea dispozitivelor de comutare direct la ruterele de bază poate avea impact negativ asupra performanței și disponibilității prin crearea multiplelor puncte unice de eșec, care ca efect pot avea pierderea conexiunii la Internet în cazul deconectării unui singur comutator [70].

Modelul ierarhic de configurare a RCE oferă o topologie modulară și scalabilă, care permite rețelelor să evolueze [67] (figura 1.6) și este divizat pe 3 straturi: acces, distribuție și de bază.

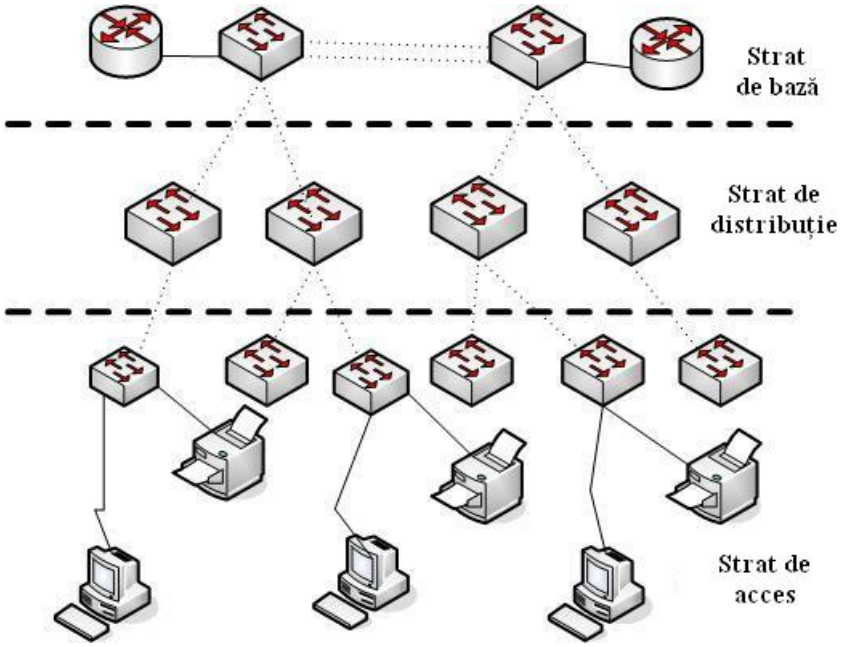

Fig. 1.6. Modelul ierarhic [67]

Stratul de acces permite dispozitivelor terminale să se conecteze la RCE prin dispozitive de rețea, așa ca: rutere cu fir și wireless, puncte de acces, switch-uri de Nivel 2 OSI. Obiectivul principal al acestui strat este de a oferi un mijloc de conectare a dispozitivelor terminale și de a gestiona drepturile de acces ale acestora [67]. Rolul stratului de distribuție este de a agrega informațiile primite de la stratul aplicație și de a gestiona traficul din rețea înainte ca să fie transmis către stratul de bază. Dispozitivele utilizate pentru stratul distribuție sunt switch-uri de nivel 3 OSI. Accesibilitatea sporită și redundanța sunt caracteristici esențiale pentru acest strat. Stratul de bază reprezintă resursa principală a RCE de mare viteză, care este esențial pentru interconectivitatea dintre dispozitivele stratului de distribuție, cât și servicii de interconectare cu alte rețele, ca de exemplu accesul la Internet.

Atât timp cât IÎS diseminează cunoștințe, un sistem tehnologizat devine un instrument indispensabil pentru a realiza activități de învățare și cercetare, atât pentru studenții care urmează

educația tradițională, cât și pentru a oferi oportunitatea de studii la distanță, pentru care se utilizează rețelele WAN, pentru a facilita accesul dispozitivelor terminale de la distanță. Rețelele de comunicații și sistemele informatice universitare contribuie la creșterea productivității, eficienței, calității, predării, administrării și a procesului de învățare [71] prin managementul electronic. Managementul electronic a fost definit anterior ca fiind executarea tuturor procedurilor și tranzacțiilor care pot avea loc între 2 sau mai multe entități, indiferent dacă sunt organizații sau persoane fizice, prin RCE [69]. Există mai multe servicii electronice pe care RCE le furnizează instituțiilor sau organizațiilor [72]. Unele exemple relevante pentru IÎS sunt [69]:

- SE pentru studenți, care includ admiterea la studii, atribuirea studenților la departamentele academice și gestionarea reușitei academice, diverse plăți și alte servicii aferente;
- SE pentru personal, așa ca stocarea/organizarea/procesarea dosarelor personale, furnizarea diverselor programe și facilități necesare personalului;
- SE pentru administrarea IÎS, care se referă la aplicații utilizate pentru comunicarea internă/externă, aplicații pentru prelucrarea documentelor; pregătirea orarului semestrial, achiziții și planificarea bugetelor universitare, biblioteci electronice.

E-managementul are un rol clar și eficient în realizarea excelenței organizaționale prin îmbunătățirea calității performanței muncii la universitate și utilizarea unor instrumente eficiente, ce pot avea impact direct asupra ridicării nivelului de excelență organizațională atât la nivel de administrare, cât și personal uman, și servicii furnizate [69]. Managementul RCE este necesar pentru a păstra fiabilitatea, validitatea și stabilitatea RCE și SCE a transmisiunilor de date [68].

1.5.2. Provocări de securitate a domeniului

Datorită modelelor de rețea utilizate și a erorilor în configurația dispozitivelor intermediare de rețea apar mai multe probleme, exploatate ulterior de atacurile cibernetice [73].

Potrivit cercetărilor realizate de Institutul Ponemon [74], care efectuează cercetări în domeniul securității cibernetice, în 2020, domeniul educației a înregistrat pierderi financiare, la nivel global, de 3,90 mln $ aferente încălcării securității datelor în RCE. Dovezile ce servesc drept exemple de pierderi financiare impunătoare în universități sunt [47]: Universitatea Newcastle din Marea Britanie; University California din San Francisco SUA ce a trebuit să achite $ 1.14 mln pentru a recupera datele; Universitatea din Utah, SUA care a plătit $ 40 mln pentru a debloca sistemele TIC etc. Raportul Microsoft Security Intelligence, din iunie 2020, a arătat că 61% din 7,7 mln atacuri malițioase înregistrate în acea lună se refereau la domeniul educației, fiind cel mai afectat sector al industriei [75].

Cea de-a doua dimensiune, indisponibilitatea serviciilor educaționale în IÎS, a devenit cu adevărat critică odată cu trecerea în mediul online, impusă de pandemia Covid-19. Astfel, securitatea CE devenind tot mai importantă, pentru a se asigura continuitatea procesului academic educațional. Drept dovezi confirmatoare sunt universitățile din Turcia și din nord-estul Statelor Unite, a căror RCE au fost indisponibile o anumită perioadă de timp, care corespundea cu perioada examenelor organizate online [47].

Ultima dimensiune, furtul proprietății intelectuale, a reprezentat un risc major și până la pandemia Covid-19, îndeosebi pentru instituțiile ce realizează cercetări strategice și economice importante. Un exemplu elocvent este atacul din partea Iranului asupra a 144 de universități din SUA și 176 universități din întreaga lume, care s-a soldat cu furtul a 31 de TB de date importante de cercetare, inclusiv proprietate intelectuală [9]. Mult mai ușor poate fi obținut accesul la rezultatele cercetărilor economice și strategice cu proprietate intelectuală de mare valoare în RCE universitare, față de organizațiile din domeniul critic național, așa ca cel militar sau financiar-bancar. Odată cu pandemia Covid-19, universitățile ce realizau studii științifice pentru a identifica formule de vaccinare sau tratamente anti-Covid 19, au fost țintite de atacatorii cibernetici pentru a li se fura rezultatele cercetărilor. Astfel, au fost înregistrate atentate din partea Chinei de a tergiversa eforturile de răspuns la pandemie, cât și din partea spionilor ruși care încercau să fure rezultatele cercetărilor Covid-19 din mai multe universități atât din Europa, cât și din SUA [9].

Deși IÎS sunt supuse unui număr mare de incidente de securitate, se poate menționa că cercetările în ceea ce privește implementarea politicilor de securitate și a sistemelor de securitate holistice în IÎS sunt limitate [8, 9].

Probabil, din cauza specificului domeniului educațional, care nu face parte din infrastructura națională critică, așa ca sectorul bancar și financiar [76], domeniul medical [77], sau mediul industrial [78], atenția autorităților și managementului IÎS asupra problemelor de securitate este limitată. Este evident că nici una dintre cele trei dimensiuni cu impact social major, descrise anterior, nu afectează nici un criteriu de existențialitate [9], deoarece nu sunt puse în pericol viețile oamenilor.

O dovadă în plus pentru abordarea cuprinzătoare a securității CE universitare este raportul publicat de Check Point Software Technologies, care a avut ca perioadă de estimare ianuarie 2021–decembrie 2021, ce a reflectat că cel mai vizat, de către atacatori, sector din industrie a fost cel al educației și cercetării, cu o creștere anuală față de anul 2020 cu 75%, înregistrând aproximativ 1605 atacuri cibernetice per instituție săptămânal [7]. Atacurile la nivel de organizații din alte industrii, de asemenea, au crescut substanțial, cu aproximativ 50% față de 2020.

Reieșind din cele expuse, provocările în domeniu sunt tot mai mari, astfel securitatea CE academice este tot mai importantă.

1.5.3. Amenințări de securitate ale RCE universitare

Practic, toate atacurile cibernetice ce pot afecta securitatea RCE sunt actuale și frecvent întâlnite în mediul universitar. Totuși, conform datelor publicate anterior, care s-au bazat pe analiza rapoartelor de securitate internaționale, cele mai mari amenințări la adresa RCE universitare revin atacurilor cu programe malițioase, atacurilor care vizează dispozitivele de rețea și atacurilor de inginerie socială prin care infractorii cibernetici obțin acces la datele transportate prin RCE universitare [46, 47].

Rețelele universitare sunt parțial deschise pentru a presta servicii educaționale electronice, aceasta reprezentând o vulnerabilitate importantă pentru atacatorii cibernetici care le permite ușor să obțină acces în rețea. Cele mai comune atacuri malițioase în mediile universitare sunt cele realizate prin programele ransomware. Ransomware reprezintă programe malițioase care permit atacatorilor să restricționeze accesul utilizatorilor autorizați, așa ca angajații sau studenții, prin criptarea unităților de stocare permanente din centrele de date universitare, laboratoare de cercetare [79], afectând astfel disponibilitatea RCE și perturbând accesul la serviciile electronice universitare. Alte programe malițioase comune sunt viermii informatici și virușii care vizează dispozitivele de rețea [57], așa cum sunt ruterele și comutatoarele. Impactul acestor atacuri duc la ștergerea configurațiilor de rețea, furtul informațiilor, blocarea accesului la serviciile de rețea, interceptarea comunicațiilor etc.

Scopul atacurilor de tip DoS/DDoS în mediul academic este indisponibilitatea activităților educaționale prestate prin RCE, mai ales în timpul examenelor sau a evaluărilor intermediare. Interceptarea comunicațiilor de date, de asemenea, prezintă un interes sporit, deoarece astfel pot fi capturate așa date ca datele de autentificare, datele despre cardul de credit și alte informații sensibile. Atacurile MitM sunt destul de frecvente în mediul academic [55].

Atacurile de inginerie socială sunt considerate a fi cele mai mari amenințări la adresa securității serviciilor și rețelelor de CE [47], deoarece utilizatorul reprezintă cea mai mare vulnerabilitate [55]. Atacurile de inginerie socială includ: phishing-ul, spear-phishingul. Phishing-ul care reprezintă transmiterea de mesaje electronice nesolicitate ce conțin fișiere sau legături către alte resurse electronice. Odată ce utilizatorul accesează aceste link-uri, diverse programe malițioase descrise mai sus pot afecta securitatea RCE.

Principalii vectori ai amenințărilor de securitate a CE în mediile universitare sunt [47]:

- epuizarea lățimii de bandă prin inundarea cu pachete [80];

- epuizarea resurselor prin exploatarea protocoalelor, utilizând pachete formatate incorect [80];
- controlul accesului la RCE universitare;
- utilizarea protocoalelor nesigure pentru comunicațiile de date;
- lipsa actualizărilor de firmware/software pe dispozitivele de rețea și dispozitivele terminale [55];
- lipsa sistemelor de management centralizat ale rețelelor și serviciilor de CE;
- lipsa educației în ceea ce privește amenințările de securitate a studenților și angajaților IÎS.

Digitalizarea IÎS este valoroasă, pe de o parte, pentru dezvoltarea mediilor de învățare moderne, iar pe de altă parte, sporește vulnerabilitatea rețelelor de comunicații și a numărului de amenințări de securitate. Multitudinea tehnologiilor utilizate creează foarte multe vulnerabilități datorită rețelelor de comunicații ale MAN (rețea metropolitană) și CAN (rețea de campus). Studierea și analiza insuficientă a securității CE reprezintă o problemă importantă pentru domeniul educațional [9], luând în considerare că cercetările în acest domeniu se află într-o fază incipientă. Adevărata amploare pe care o pot avea atacurile cibernetice în IÎS a fost demonstrată cu precădere în ultimii ani, odată cu pandemia Covid-19 și migrarea studiilor în mediul online.

În primăvara anului 2020, domeniul educației a fost puternic afectat de pandemia Covid-19. Studiul online a devenit principala modalitate de desfășurare a activităților educaționale la nivel internațional.

Amenințările de securitate care au vizat rețelele și serviciile de CE universitare, în 2020, au crescut dramatic față de aceeași perioadă din 2019. Kaspersky a raportat o creștere cu aproximativ 350% a atacurilor DoS/DDoS asupra resurselor educaționale electronice [75] (figura 1.7).

Fig. 1.7. Procentajul atacurilor DoS/DDoS asupra resurselor educaționale: Q1 2019 vs Q1 2020 [46]

1.5.4. Stadiul cercetărilor în domeniul securității CE în IÎS

Au fost analizate strategiile de securitate care se referă la standardele în domeniu și seturile de bune practici utilizate la nivel internațional. Standardele de securitate implementate la nivel internațional sunt standardul european ISO 27001 [17] și standardul american NIST [81]. Pe lângă standardele internaționale, există și standarde la nivel național, așa ca familia standardelor BSI, implementate în Germania [82], sau standardul MCSS, dezvoltat de Guvernul Marii Britanii. De asemenea, există mai multe cadre de securitate, ghiduri de bune practici, așa ca COBIT [83] sau ITIL [84]. Din multitudinea cadrelor enumerate mai sus, IÎS din Uniunea Europeană și Asia implementează preponderent standardul ISO 27001, numărul IÎS certificate crescând constant, astfel încât, dacă în 2018, la nivel internațional, erau certificate 137 de instituții, în 2020 numărul lor a fost de 187 de instituții, conform rapoartelor anuale realizate de ISO [85]. Cele mai multe IÎS certificate ISO 27001 sunt în Japonia (26), Grecia (30), Italia (11), Polonia (12), Cehia (11) [86]. Nici o IÎS din Republica Moldova nu este certificată cu ISO 27001 [85]. IÎS din SUA preponderent utilizează cadrul național NIST pentru a securiza RCE și serviciile electronice pe care le prestează.

Analizând resursele disponibile online, s-a constatat că o bună parte din IÎS din România au publicate politici de securitate [87, 88], care includ securitatea RCE și a SCE, așa ca controlul accesului la RCE; securizarea serverelor și a dispozitivelor de rețea; dispoziții pentru conectarea dispozitivelor terminale proprii la RCE universitare; indicații de utilizare a SCE universitare care se referă atâta la Internet/Intranet, cât și la SCE cu valoare adăugată menite să stabilească clar responsabilitățile utilizatorilor CE universitare.

La nivel național a fost analizat Instrumentul Bibliometric Național (IBN) [89], care reprezintă cea mai mari bibliotecă electronică cu acces deschis din Republica Moldova, ce indexează mai multe reviste științifice, dar și conferințe naționale și internaționale. S-a constatat că în domeniul securității cibernetice până în anul 2022 au fost publicate 82 de lucrări științifice, prevalând lucrările prezentate în cadrul conferințelor științifice, publicate în limba română. Un studiu care s-a bazat pe IBN, publicat de doi cercetători din Republica Moldova [90], în anul 2019, a constatat că dintre țările Europei de Est, Republica Moldova are cea mai mică contribuție în ceea ce privește publicațiile internaționale de cercetare aferente domeniului de securitate cibernetică, în două dintre cele mai mari baze de date internaționale: Scopus și Web of Science. De asemenea, o concluzie importantă a aceluiași studiu a fost că ”la nivel național, productivitatea în acest domeniu este destul de scăzută, publicațiile fiind distribuite neuniform în perioada de studiu, scrise preponderent în limba română și majoritatea fiind lucrări ale conferințelor. Deficitul informațiilor

referitoare la cercetarea în domeniul securității cibernetice a dovedit clar necesitatea explorării sistemice" [90].

Abordarea securității cibernetice și a CE specifice mediului universitar este reflectată în lucrările științifice publicate de autorul prezentei teze de doctor, alte lucrări științifice analizează această problemă deopotrivă cu alte organizații la nivel național [91, 92] sau din perspectiva educației în acest domeniu [30, 93]. De asemenea, un anumit număr de lucrări științifice se orientează pe problemele de securitate ale infrastructurilor critice de stat [94] și pe domeniul medical. O lucrare națională importantă, în care a fost tratată problema securității informației în sistemele informaționale automatizate, se referă la asigurarea securității ca la un proces sistemic și iterativ de abordare a problemelor de securitate din cadrul organizațiilor, care implică aspecte legale, organizatorice, economice și tehnice [95].

Atât la nivel internațional, cât și național, studiile științifice relevante problemelor de securitate a CE în mediul universitar/academic sunt limitate, domeniul științific fiind în curs de dezvoltare, ipoteză susținută în diferite perioade de timp de diferiți cercetători [8, 9, 96]. Deși cercetările anterioare au reflectat diferențele dintre abordarea securității CE în mediul universitar față de alte medii, ceea ce justifică necesitatea cercetărilor în acest domeniu foarte important, aflat în curs de dezvoltare, majoritatea lucrărilor științifice sunt publicate începând cu anul 2014 [86]. Mai mulți cercetători au specificat ca scop pentru lucrările viitoare realizarea cadrelor de securitate de referință, care să susțină IÎS în efortul de implementare a cadrelor sistemice de securitate [8, 9, 97] și optează pentru crearea unei noi direcții de cercetare științifică, orientată pe dezvoltarea cadrelor de securitate a CE adaptate mediului universitar [96]. O altă problemă științifică foarte importantă rezidă în faptul că standardele și cadrele de securitate existente conțin recomandări generice [98], iar pentru a le pune în practică urmează a fi identificată modalitatea de operaționalizare a acestora în cadrul IÎS.

Deci, sunt necesare mai multe cercetări în acest domeniu, ipoteză susținută atât de autorul prezentei teze de doctor [86], cât și de alți cercetători la nivel internațional [9, 96, 97, 99] și național care afirmă că " severitatea tot mai mare a criminalității cibernetice și complexitatea tot mai mare a atacurilor cibernetice accentuează importanța cercetării/dezvoltării în securitatea informației" [92].

1.6. Studiul empiric al situației actuale în IÎS din Republica Moldova

Studiul empiric reprezintă o fază foarte importantă a procesului de securizare a organizațiilor, deoarece permite evaluarea stării actuale în domeniul cercetat [92]. Metoda utilizată

pentru a identifica provocările și abordarea securității CE în instituțiile de învățământ superior din Moldova a fost sondajul bazat pe chestionar.

Pentru realizarea acestui sondaj au fost contactați 9 specialiști din cele mai mari 9 instituții de învățământ superior din Moldova. Universitățile care au participat la acest studiu sunt: Universitatea de Stat din Moldova, Universitatea Tehnică a Moldovei, Universitatea de Stat „Alecu Russo", Academia de Studii Economice din Moldova, Universitatea de Stat „Bogdan Petriceicu Hasdeu", Universitatea Pedagogică de Stat „Ion Creangă" din Chișinău, Universitatea de Stat de Educație Fizică și Sport, Universitatea de Stat de Medicină și Farmacie „Nicolae Testemițanu" din Republica Moldova, Universitatea Agrară de Stat din Moldova (actualmente parte a Universității Tehnice a Moldovei). Designul cercetării este reflectat în figura 1.8.

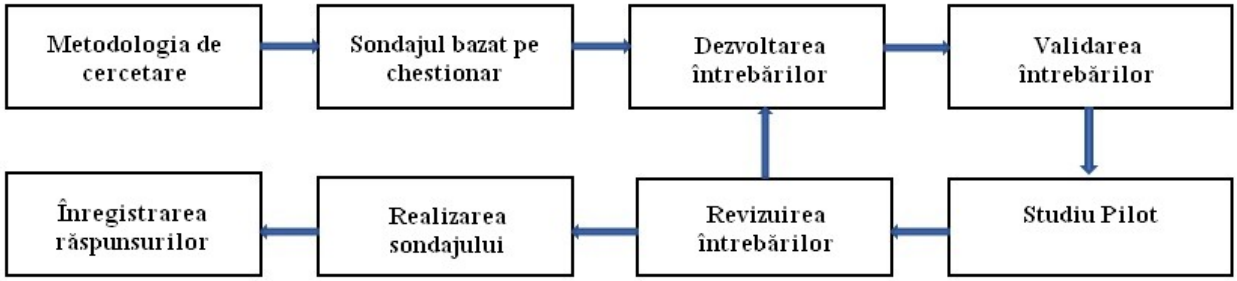

Fig. 1.8. Procedura realizată pentru investigație (elaborată de autor)

Întrebările sondajului s-au referit la problemele și preocupările legate de amenințările de securitate din mediul academic, abordarea riscului cibernetic, răspunsul la incidentele de securitate și cum are loc managementul securității CE.

Analiza amenințărilor de securitate cibernetică

Conform rezultatelor sondajului, aferente amenințărilor de securitate în mediul electronic, care au vizat IÎS din Republica Moldova în anul 2020, s-a constatat că 80% din respondenți au răspuns că instituțiile pe care le reprezintă au fost ținta atacurilor cibernetice din acea perioadă. Distribuția amenințărilor cibernetice cu care s-au confruntat IÎS naționale sunt reflectate în figura 1.9.

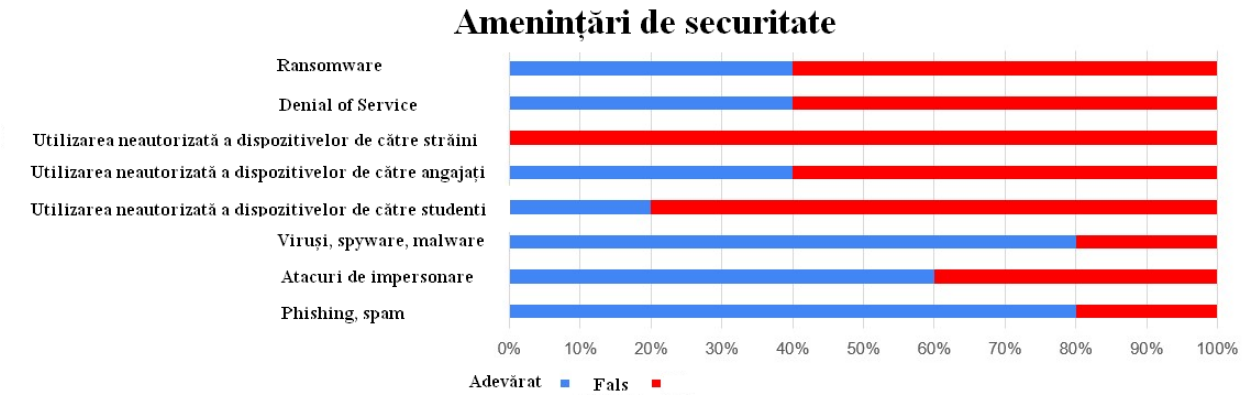

Fig. 1.9. Amenințări de securitate ale IÎS din RM în anul 2020 (elaborată de autor)

Astfel, se poate observa că cele mai mari provocări de securitate a CE, în 2020, au fost atacurile spam sau phishing (80%) și atacurile cu programe malițioase: viruși, viermi sau Cal Troian (80%). Atacuri ransomware și DoS au fost înregistrate de 40% dintre respondenți. Amenințările de securitate care vizează utilizarea neautorizată a dispozitivelor universitare de către personal, cum ar fi computere, servere sau dispozitive de rețea, au fost înregistrate de 40% dintre IÎS. Utilizarea neautorizată a dispozitivelor de către studenți sau persoane din exterior nu a reprezentat o amenințare, probabil motivul principal fiind că procesul educațional s-a desfășurat în mare parte online, astfel că vizitele studenților sau a persoanelor din exterior nu au fost frecvente.

La întrebarea *Care sunt cele mai comune 3 amenințări la adresa instituției dvs.*, respondenții au selectat dintr-o listă de 10 opțiuni următoarele: atacuri DoS sau DDoS (40%), phishing și inginerie socială (20%), ransomware (20%) și atacuri MitM (20%); rezultatele sunt prezentate grafic în figura 1.10.

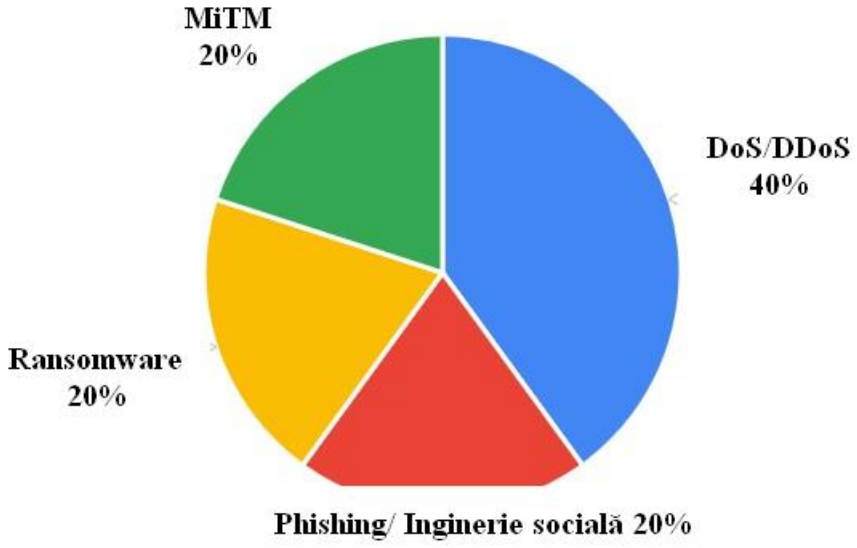

Fig. 1.10. Amenințări de securitate frecvente (elaborată de autor)

Rezultatele sondajului au reflectat o rată sporită a atacurilor cibernetice care au loc în instituțiile de învățământ superior din Moldova: 80% dintre respondenți au declarat că în 2020, instituția pe care o reprezintă a fost ținta atacurilor cibernetice [100]. Deși instituțiile academice din Moldova nu sunt la fel de cunoscute pe arena internațională, se confruntă cu provocări destul de mari în acest domeniu, iar asigurarea securității CE este importantă.

Analiza gestiunii riscului cibernetic și răspunsul la incidente

Reieșind din rezultatele colectate și reflectate în figura 1.11, putem afirma că acțiunile generale pentru abordarea riscurilor informaționale și răspunsul la incidente se realizează în cel mai bun caz de doar 66% din instituțiile respondente.

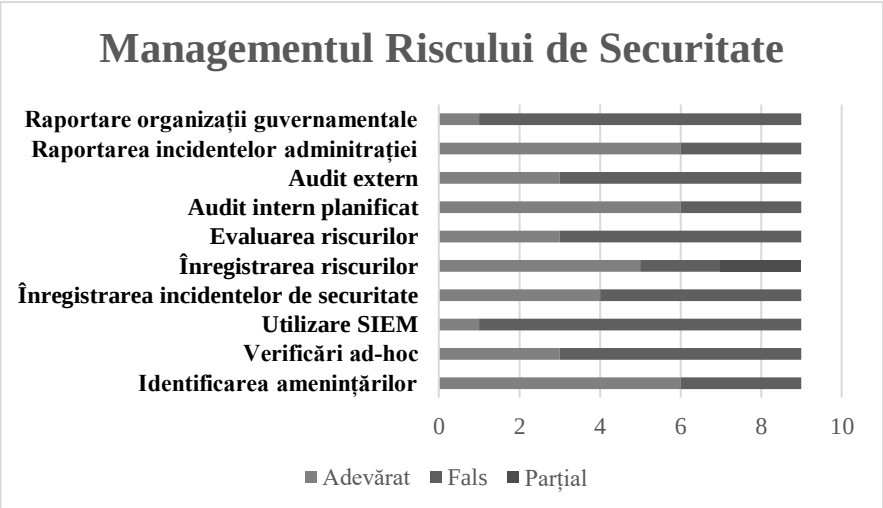

Fig. 1.11. Acțiuni pentru gestiunea riscului de securitate și răspunsul la incidente (elaborată de autor)

Punctele-cheie identificate asupra cărora trebuie să se reflecte se referă la următoarele:

- evaluarea riscurilor cibernetice care a înregistrat un scor scăzut (30% din respondenți au răspuns afirmativ), deși managementul riscurilor reprezintă calea spre un sistem de securitate mai robust și permite a identifica activele informaționale care urmează a fi protejate;
- verificările ad-hoc din care fac parte testele de penetrare și utilizarea scanerelor de vulnerabilități sunt realizate de un număr mic de instituții, deși permit ajustarea cerințelor de securitate la necesitățile reale;
- lipsa sistemelor de monitorizare a rețelelor, precum este utilizarea produsului program SIEM (Security Information and Event Management), constituie o lacună importantă, deoarece SIEM este util pentru monitorizarea, detectarea și reacția la atacurile cibernetice (doar un răspuns afirmativ a fost înregistrat) [101]; tot aici pot fi menționate și programele de detecție a intruziunilor [102], pentru a identifica comportamente necorespunzătoare;
- raportarea către organizațiile guvernamentale a incidentelor de securitate a înregistrat un singur răspuns afirmativ (11%), deși această practică este recomandată la nivel internațional pentru a evalua anual indicele de securitate cibernetică națională, a identifica amenințările cibernetice cu impact ridicat și pentru a introduce vulnerabilitatea identificată în baza de date națională a amenințărilor la securitatea cibernetică, care urmează a fi creată.

Abordarea riscurilor cibernetice în cadrul organizațiilor ce prestează servicii electronice și gestionează un număr mare de date personale, precum și modul în care este organizat procesul de răspuns la incidente influențează reziliența sistemului de securitate [100].

Analiza managementului securității CE

Managementul securității CE permite o abordare holistică a problemelor legate de securitatea cibernetică, ce influențează competitivitatea și supraviețuirea organizației pe piața globală [103]. Standardul ISO 27001 reprezintă un bun ghid pentru evaluarea managementului securității. Întrebările aferente acestei secțiuni au fost formulate, luând în considerație prevederile standardului pe anumite dimensiuni.

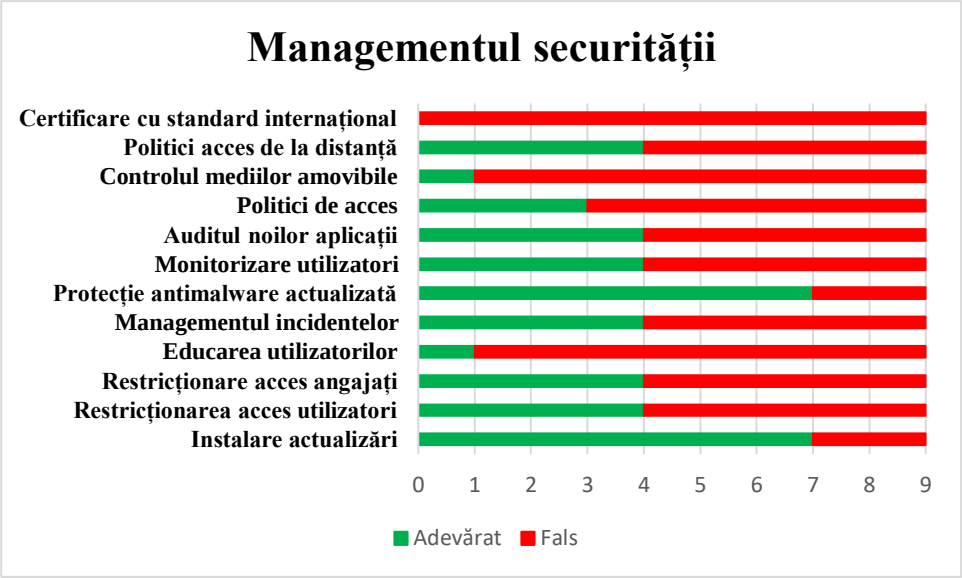

Fig. 1.12. Realizarea managementului securității (elaborată de autor)

Rezultatele arată că acțiunile operaționale, așa ca instalarea actualizărilor și protecția malware actualizată, sunt implementate de 7 instituții respondente, ceea ce este un bun indicator.

În schimb, acțiunile specifice managementului, așa ca politicile de acces, educarea utilizatorilor, controlul mediilor amovibile, monitorizarea utilizatorilor, managementul incidentelor, sunt aplicate de o mică parte din IÎS [100]. Datele sondajului arată că nicio IÎS națională nu este certificată cu un standard internațional [100], deși importanța implementării politicilor de securitate este majoră [104], iar investițiile în educarea utilizatorilor sunt considerate a fi cele mai eficiente în acest domeniu [93]. Doar așa, printr-o abordare holistică a managementului securității CE, poate crește rezistența organizației la atacurile cibernetice.

Analiza site-urilor oficiale ale IÎS din Republica Moldova a elucidat faptul că instituțiile academice nu au implementat, în mare parte, politici de securitate, în afară de *Politica de securitate privind protecția datelor cu caracter personal*, fapt confirmat și de rezultatele sondajului: doar 22,2% au afirmat că au implementat politici interne de securitate, 44,4% că sunt în curs de implementare, iar 33,3% că nu au politici de securitate.

1.7. Definirea problemei de cercetare

Securitatea CE devine o prioritate la nivel național și european, demonstrată prin completarea Legii CE nr. 241 cu articolele 21 și 22, iar la nivel european prin punctele 94-98 și articolele 40 și 41 din Codul European al CE modificate prin Directiva 2018/1972. Atât cadrul normativ național, cât și cel european impun măsuri organizatorice și tehnice pentru asigurarea securității CE. Astfel, dezvoltarea unui cadru de securitate, care să se refere la managementul organizației, sistemele tehnice, educația și formarea utilizatorilor [105], care au acces la RCE și

la serviciile electronice, va permite abordarea holistică a securității și implementarea cerințelor de securitate comune.

CE sunt extrem de susceptibile la atacuri cibernetice, deoarece anume de securitatea acestora depinde siguranța online a utilizatorilor și capacitatea organizațiilor de a funcționa. Spectrul amenințărilor de securitate ale CE este unul vast, care include pe lângă amenințări de securitate specifice dispozitivelor de rețea și mediilor de conexiune, alte amenințări de securitate care au migrat de la amenințări de securitate specifice dispozitivelor terminale la dispozitivele de rețea, datorită impactului mult mai mare pe care îl pot avea în acest caz. Protocoalele utilizate pentru CE, de asemenea, prezintă riscuri sporite de securitate, precum sunt interceptarea comunicațiilor, accesul și controlul dispozitivelor de la distanță, impersonarea, refuzul serviciului, care pot perturba funcționarea întregului sistem de CE.

Modalitățile de abordare a securității CE variază de la abordarea de jos în sus, în care administratorii de RCE implementează cerințe de securitate pe dispozitivele și mediile de rețea, avantajele acestei abordări fiind expertiza tehnică pe care o dețin, gestionând RCE zilnic și cunoscând amenințările de securitate reale. Însă această abordare în practică deseori eșuează, deoarece îi lipsesc ”caracteristicile critice, cum ar fi suportul colectiv și puterea de rezistență organizațională” [29]. Cu o probabilitatea mai înaltă de succes este considerată abordarea de sus în jos, deoarece în acest caz proiectul este inițiat de managementul superior, care setează obiectivele și verifică rezultatele obținute după implementarea centralizată a politicilor, cerințelor și controalelor de securitate, alocă resurse, planifică și gestionează procesul de implementare cu scopul de a influența cultura organizațională [29] și abordarea cuprinzătoare a procesului de securizare a CE.

Directivele europene NIS și NIS_2 obligă implementarea cerințelor de securitate comune pentru sectoare specifice, promovând o abordare de sus în jos, însă domeniul educației nu este acoperit de nici unul dintre aceste documente.

IÎS sunt specifice prin rețelele parțial deschise la care au acces un număr impunător de utilizatori, ceea ce le face deosebit de vulnerabile, fapt demonstrat prin rezultatul analizei rapoartelor de securitate anuale realizate de companii specializate și studiul empiric la care au participat 9 IÎS naționale, ce reflectă provocările reale cu care se confruntă IÎS naționale și internaționale, în ceea ce privește incidentele de securitate. Nu mai puțin de 80% din IÎS naționale au confirmat că pe parcursul anului 2020 au fost ținta atacurilor cibernetice.

La capitolul managementul securității și a riscurilor de securitate au fost identificate mai multe lacune, care se referă la următoarele:

- acțiunile generale privind riscurile informaționale și răspunsul la incidentele de securitate (evaluarea riscurilor cibernetice, scanarea vulnerabilităților, folosirea sistemelor de monitorizare a rețelelor etc.) se realizează în cel mai bun caz de doar 66% dintre IÎS;
- politicile de acces, educarea utilizatorilor, controlul mediilor amovibile, monitorizarea utilizatorilor, managementul incidentelor sunt aplicate de o mică parte din IÎS;
- politicile de securitate nu sunt implementate în cea mai mare parte de către IÎS naționale, doar 22,2% au confirmat implementarea acestora;
- nici o IÎS nu este certificată cu un standard internațional.

Astfel, **problema de cercetare a lucrării constă în elaborarea unui cadru sistemic național de securitate a comunicațiilor electronice pentru instituțiile de învățământ superior din Republica Moldova, care ar asigura abordarea holistică a problemelor ce se referă la securitatea CE, prioritate la nivel internațional în ultimii ani**.

În acest scop sunt necesare astfel de cercetări:

- identificarea metodelor științifice potrivite pentru dezvoltarea unui cadru sistemic al securității CE, care să includă aspecte organizatorice și tehnice, cerințe de securitate comune pentru IÎS;
- dezvoltarea cadrului sistemic de securitate a CE pentru IÎS prin analiza specificului mediului universitar;
- evaluarea CSSCE prin sondaj în baza criteriilor de valoare și validarea CSSCE prin simularea implementării în cadrul unei facultăți.

O parte esențială a oricărei lucrări de cercetare este metoda științifică selectată pentru a realiza studiul și instrumentele care facilitează obținerea rezultatelor științifice relevante. Această premisă a stat la baza identificării metodei științifice Cercetarea în Știința Proiectării DSR (din engleză: Design Science Research). Metoda DSR (Design Science Research) a fost apreciată ca fiind una dintre metodele principale de cercetare pentru domeniul ingineresc [106].

Finalitatea implementării metodei DSR reprezintă un model, concept sau cadru [13, 107, 108]. Astfel, rezultatul poate fi definit ca „sistem, în care întregul (cadrul) este mai mare decât suma părților sale, în care elementele constitutive nu sunt separate, ci interactive, la fel ca orice subsisteme care formează un sistem complex” [109, 110].

1.8. Concluzii la capitolul 1

Rețelele și serviciile de CE universitare, și nu numai, se confruntă cu un număr sporit de incidente de securitate, care afectează disponibilitatea, integritatea și confidențialitatea datelor. Analiza cadrelor normative naționale și europene care se referă la securitatea CE a permis

identificarea tendințelor actuale în acest domeniu, pentru a se asigura conformitatea IÎS, pe această dimensiune, și pentru a se accentua necesitatea realizării cercetărilor în domeniu.

Analiza problemelor securității CE a permis identificarea dimensiunilor sensibile ale IÎS în acest domeniu la nivel internațional.

Studiul empiric a contribuit la conturarea necesităților și lacunelor existente în procesul de asigurare a securității CE în IÎS naționale, dintre cele mai importante fiind: lipsa politicilor de securitate, a activităților specifice managementului riscului, a educării utilizatorilor și lipsa cadrelor sistemice de securitate, care ar permite abordarea tuturor problemelor de securitate în mod sistemic și cuprinzător.

Astfel, pentru o abordare holistică a fenomenului, se impune dezvoltarea unui cadru sistemic de securitate a CE orientat spre serviciile și rețelele de comunicații electronice universitare, care să permită implementarea cerințelor de securitate comune, într-un mod scalabil și modular, în dependență de dimensiunea și nivelul de dezvoltare digitală a IÎS, respectând prevederile standardului internațional ISO 27001 pe dimensiunile acoperite.

2. METODOLOGIA DE DEZVOLTARE A CADRULUI SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE

Proiectele DSR trebuie să aibă valoare intelectuală, creativă, dar și impact extins în domeniul aplicativ prin soluții originale ale problemei de cercetare [107, 108]. Aceasta este considerată oportunitate de a demonstra rigoarea și relevanța cadrelor sistemice ca domeniu academic [110, 111], iar cercetarea cadrelor sistemice ar trebui să contribuie la soluționarea provocărilor din lumea reală [112].

Cercetările vizează soluțiile care necesită a fi investigate empiric și discutate cu specialiștii din organizațiile ce utilizează tehnologia specifică [13]. Adesea, analiza mediului de afaceri și derivarea nevoilor specifice care trebuie rezolvate constituie punctul de plecare al unui proiect DSR. În orice caz, există, de asemenea, situații în care nevoile au fost deja studiate și pot fi preluate din cercetările existente [13].

Metoda DSR propune crearea unei soluții inovatoare la problemă, care, în majoritatea cazurilor, se bazează pe componentele existente ale altei soluții și combină, revizuiește și extinde cunoștințele de proiectare existente [13]. Herbert Simon afirma că ”rezolvarea unei probleme înseamnă prezentarea acesteia, astfel încât soluția să devină transparentă” [113].

În literatura de specialitate se identifică 6 etape tipice ale proiectului DSR [13, 109, 114]:

- identificarea problemelor și motivația;
- definirea obiectivelor pentru soluția dezvoltată;
- design și dezvoltare cadru;
- demonstrația cadrului;
- evaluarea cadrului;
- comunicarea rezultatelor.

Metoda DSR se pretează cel mai bine pentru dezvoltarea CSSCE, care trebuie să aibă o valoare aplicativă mare, să permită abordarea holistică și identificarea cerințelor de securitate comune pentru CE gestionate de IÎS naționale, să aducă inovație.

CSSCE ca și construct abstract reprezintă un cadru conceptual, iar ca rezultat al operaționalizării sale în mediul academic este o instanțiere [115]. Termenul *instanțiere* a fost definit în literatura științifică ca un cadru destinat unui anumit mediu [116], sau ca un sistem real ce poate fi implementat în practică [117]. De asemenea, instanțierile pot fi clasificate ca fiind produse sau procese [118]. Deoarece securitatea CE reprezintă un proces iterativ [28], CSSCE reprezintă un cadru de tip proces, care include metode și proceduri organizatorice și tehnice, pentru a aborda problemele aferente securității CE în IÎS din Moldova. O altă abordare pentru instanțieri, le clasifică ca fiind constructe tehnice sau sociotehnice, iar din acest aspect CSSCE este

sociotehnic, deoarece stabilește o interacțiune directă între factorul uman implicat în aplicarea metodelor și procedurilor pe care le prevede, de care depinde succesul implementării.

Cele 6 etape tipice ale metodei DSR au fost utilizate pentru a înțelege, conceptual, cum a fost dezvoltat CSSCE, iar rezultatul studiului științific să fie reproductibil. Figura 2.1 reprezintă designul cercetării conform etapelor metodei DSR.

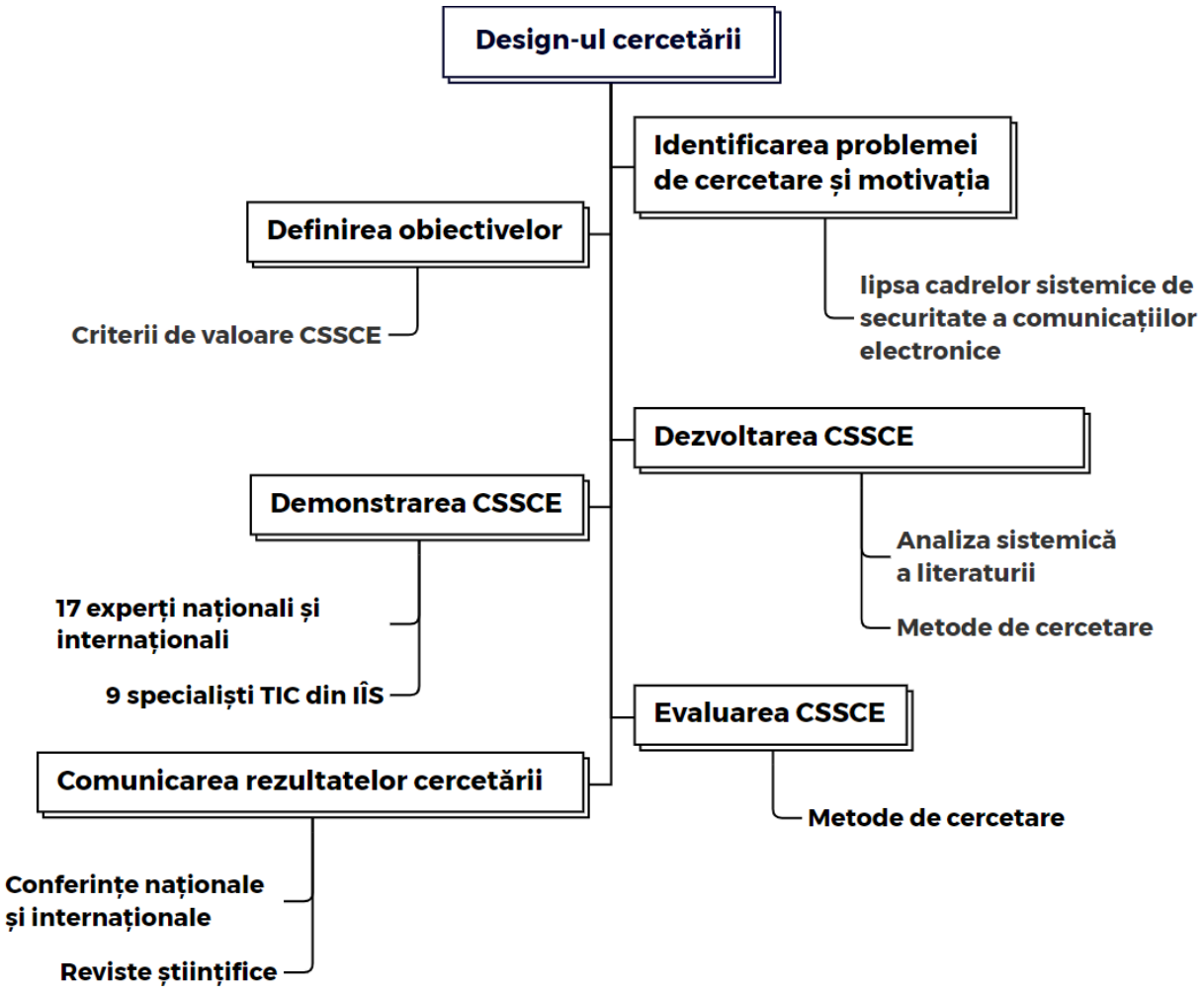

Fig. 2.1. Designul cercetării conform etapelor DSR (elaborat de autor)

2.1. Identificarea problemei și motivația

Cauzele care au generat problema de cercetare (din perspectiva autorului) sunt:

- lipsa cadrelor de referință specifice care pot fi utilizate pentru implementarea sistemelor de securitate în IÎS, care să abordeze holistic securitatea CE, să specifice clar cum poate fi operaționalizat întreg procesul orientat spre protecția serviciilor și rețelelor de CE academice;
- complexitatea procesului de implementare a standardelor, deoarece standardele nu sunt orientate spre domeniul educației, ci sunt mai degrabă generice, precum este standardul ISO 27001, adică acoperă controalele de securitate ce ar trebui să fie implementate obligatoriu,

însă nu specifică instrumentele operaționale, deși pentru orice organizație este foarte important ca instrucțiunile de implementare să se potrivească cu specificul activităților pe care le desfășoară;

- lipsa personalului specializat; IÎS din Republica Moldova nu au prevăzut în organigrama instituției postul de Ofițer al securității informației, responsabil inclusiv de securitatea RCE și a serviciilor electronice, care să gestioneze acest proces în mod sistemic și cuprinzător;
- lipsa bugetelor prevăzute în planurile financiare universitare pentru implementarea sistemelor de management al securității, acest proces fiind costisitor [91];
- imaturitatea domeniului de securitate cibernetică și respectiv a securității CE, Republica Moldova fiind o țară în curs de dezvoltare, iar legea privind securitatea cibernetică urmează încă a fi implementată.

Motivația respectivei teze de doctor rezidă în faptul de a dezvolta un cadru sistemic de securitate orientat spre procesul academic al IÎS din Republica Moldova, care să poată fi utilizat ca ghid de implementare a sistemelor de securitate holistice, ce prevede atât măsuri organizatorice, cât și tehnice pentru abordarea problemelor de securitate a CE universitare.

2.2. Definirea obiectivelor CSSCE

Obiectivul principal este dezvoltarea unui cadru sistemic de securitate a CE pentru instituțiile de învățământ superior, luându-se în calcul cerințele și limitările standardelor internaționale de securitate, specificul și amenințările de securitate ale RCE universitare [119].

Provocarea a fost de a identifica criterii de valoare după care va fi evaluat și confirmat CSSCE. Astfel, au fost studiate lucrările științifice [120, 121, 122] pentru a identifica criteriile de valoare după care pot fi evaluate cadrele, în baza dovezilor științifice. Criteriile de valoare permit evaluarea obiectivă a cadrelor, modelelor, conceptelor rezultate în urma aplicării unei metode științifice calitative, astfel sporind calitatea acestora, iar cunoștințele prescriptive produse în DSR pot fi considerate ca având o valoare asemănătoare adevărului [116].

Criteriile de valoare propuse pentru evaluarea CSSCE și argumentele relevante pot fi analizate în tabelul 2.1.

Tabelul 2.1. Criteriile de valoare ale CSSCE

Nr.d/o	Criteriul	Argumentarea
1	Aplicabil în grupul-țintă	Să conțină cerințe de securitate pentru SCE și RCE academice.
2	Fazele de implementare	Cadrul trebuie să determine pașii principali după care poate fi implementat CSSCE în cadrul IÎS.
3	Roluri predefinite	Rolurile personalului implicat în implementarea cadrului de securitate a CE în IÎS trebuie să fie clar definite, pentru a cunoaște

		Continuarea tabelului 2.1
		responsabilitățile aferente postului și a desemna proprietarii activelor bazate pe CE universitare.
4	Managementul riscului	Pentru a spori eficacitatea sistemului de securitate, este necesar a identifica riscurile reale raportate la activele bazate pe CE și amenințările ce le pot afecta. A evalua impactul riscurilor.
5	Eficient	Eficiența cadrului depinde în mod direct de nivelul de a-l înțeleg de către specialiștii din IÎS, care urmează să-l implementeze, cât de clar vor fi definite obiectivele, scopul și fazele de implementare.
6	Scalabil	Să poată fi implementat în orice instituție, indiferent de dimensiunea acesteia și de complexitatea serviciilor academice electronice pe care le prestează; să fie modular.
7	Importanță internațională	IÎS din RM se conformează procesului de la Bologna, care definește importanța implementării cadrelor recunoscute internațional [119] drept un proces extrem de important. Astfel, cadrul de securitate pentru IÎS trebuie să se conformeze standardelor internaționale din acest domeniu, iar certificarea ulterioară a instituțiilor reprezintă un obiectiv apreciabil.

Evaluarea CSSCE va fi realizată prin prisma a 7 criterii de valoare stabilite prin care se va confirma utilitatea acestuia.

2.3. Design și dezvoltare CSSCE

Dezvoltarea prototipului este instanțierea inițială, parte a procesului de dezvoltare a unui concept [123]. De asemenea, dezvoltarea prototipului trebuie să se bazeze pe studiul aprofundat al soluțiilor propuse de alți cercetători și componentele funcționale ale sistemului, precum și relațiile predefinite dintre acestea [124].

2.3.1. Standarde/cadre de securitate utilizate în IÎS

Ca parte importantă a cercetărilor a fost realizat studiul literaturii, conform metodei propusă de Kitchenham [12], cu scopul de a identifica, interpreta și evalua cercetările relevante domeniului de securitate a CE în instituțiile de învățământ superior [86] (figura 2.2).

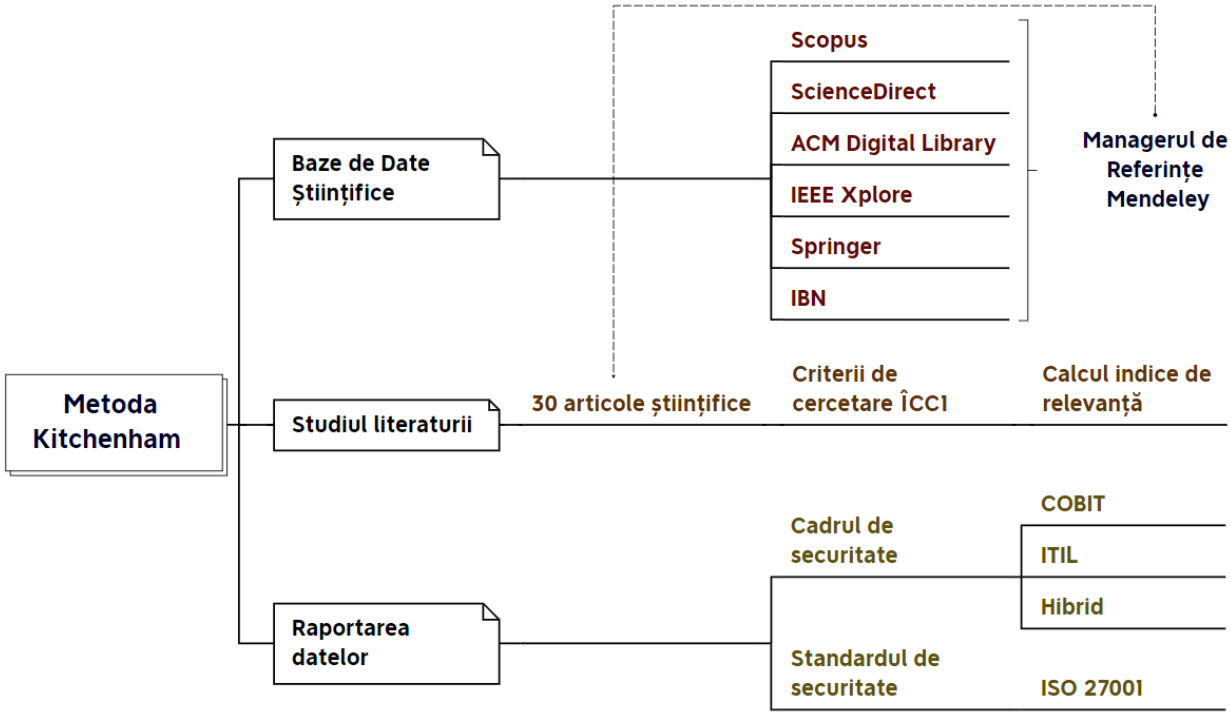

Fig. 2.2. Studiul literaturii în baza metodei lui Kitchenham (elaborat de autor)

Studiile primare sunt realizate în baza criteriilor de incluziune și excluziune [12]. Criteriile de incluziune care au stat la baza identificării articolelor relevante cercetării sunt:

- CI1: Studii care includ cercetarea cadrelor și standardelor de securitate;
- CI2: Studii care prezintă controale, instrumente sau politici relevante pentru implementarea cadrului/standardului de securitate în IÎS;
- CI3: Studii publicate începând cu anul 2012 (pentru analiza literaturii din ultimii 10 ani).

Criteriile de excluziune în baza cărora au fost excluse anumite studii din cercetare sunt:

- CE1: Este disponibil doar rezumatul articolului;
- CE2: Studiul nu reprezintă un articol de cercetare sau lucrare de conferință;
- CE3: Studii ce reflectă importanța programelor de studii (specializărilor) în domeniul securității CE în cadrul IÎS.

În bazele de date științifice au fost identificate 73 de lucrări științifice. Cu toate acestea, o mare parte au fost excluse, deoarece nu erau relevante, conform criteriilor de incluziune/excluziune. În cele din urmă, 30 de articole științifice au fost introduse în Managerul de Referințe Mendeley [125] pentru analiză. Pentru realizarea unei evaluări a calității, au fost stabilite criteriile de cercetare reflectate în tabelul 2.2.

Tabelul 2.2. Criterii de cercetare

Nr. d/o	Întrebări de cercetare	Criterii de cercetare
1	Care este cadrul / standardul de securitate recomandat de cercetători pentru securizarea CE din instituțiile de învățământ superior?	Cadrul sau standardul de securitate
2	Care este cadrul/standardul pentru abordarea managementului riscului CE în IÎS?	Cadrul/standardul de management al riscului

Indicele de relevanță a fost calculat conform formulei 2.1. Fiecare răspuns x_i poate lua valorile 1, dacă articolul a răspuns la toate criteriile de cercetare, și 0 în caz contrar:

$$\boldsymbol{R}_i = \frac{\sum_{i=1}^{n} x_i}{n} * 100\%, \quad (2.1)$$

unde:

n = numărul de itemi selectați, $i = \{1,\ldots, n\}$

$x_i \in \{0,1\}$

$\boldsymbol{R}_i$ - poate lua valori cuprinse între 0 și 1.

Folosind metoda propusă de Kitchenham [12], în baza formulei (2.1), a fost calculat indicele de relevanță ($\mathbf{R}_i$) al lucrărilor științifice. Lista lucrărilor științifice pentru analiza sistemică a securității poate fi analizată în tabelul 2.3.

Tabelul 2.3. Relevanța lucrărilor științifice

Referință	Articol științific	Anul publicării	R_i
[8]	Information Security Management in academic institutes of Pakistan	2013	0,89
[126]	An analysis of Indonesia's information security index: a case study in a public university	2018	0,89
[127]	Information security risks management framework – A step towards mitigating security risks in university network	2017	0,89
[128]	Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study	2014	0,89
[129]	Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization	2017	0,89
[130]	Today's Action is Better than Tomorrow's Cure - Evaluating Information Security at a Premier Indian Business School	2013	0,89
[131]	Emergence of Robust Information Security Management Structure around the world wide Higher Education Structure around the world wide Higher Education Institutions: Institutions: a Multifaceted Security Solution	2012	0,89
[132]	IT Governance, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education	2016	0,89

Continuarea tabelului 2.3			
[133]	A study on integrating penetration testing into the information security framework for Malaysian higher education institutions	2015	0,83
[134]	Defense-through-Deception Network Security Model: Securing University Campus Network from DOS/DDOS Attack	2018	0,77
[83]	Cobit Framework as a Guideline of Effective it Governance in Higher Education: A Review	2013	0,72
[99]	Assessment of Information System Risk Management with Octave Allegro at Education Institution	2018	0,72
[135]	A generic framework for information security policy development	2017	0,72
[136]	Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education	2018	0,72
[137]	An Analysis of IT Assessment Security Maturity in Higher Education Institution	2016	0,68
[138]	Information Security Management for Higher Education Institutions	2014	0,61
[139]	Information system and management for campus safety	2019	0,22
[140]	Towards an Unified Information Systems Reference Model for Higher Education Institutions	2017	0,61
[141]	Web vulnerability assessment and maturity model analysis on Indonesia higher education	2019	0,61
[142]	Implementing IT Security Penetration Testing in Higher Education Institute	2014	0,55
[143]	IT Governance Mechanisms in Higher Education	2016	0,50
[144]	Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world	2019	0,50
[145]	Missing Values Prediction for Cyber Vulnerability Analysis in Academic Institutions	2018	0,44
[146]	Implications, Risks And Challenges Of Cloud Computing In Academic Field – A State-Of-Art	2019	0,44
[147]	Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions	2020	0,44
[148]	Sixware Cybersecurity Framework Development To Protect Defense Critical Infrastructure And Military Information Systems	2021	0,39
[149]	The Design of Information Security Management System in College	2016	0,39
[150]	Analysis And Implementation Of Operational Security Management On Computer Center At The University X	2014	0,33
[151]	An IT value management capability model for Portuguese universities: A Delphi study	2018	0,22
[152]	Cloud Computing: Empirical Studies in Higher Education A Literature Review	2017	0,22

Pentru sinteză, urmează a fi utilizată analiza descriptivă. Informația extrasă din lucrările științifice va fi prezentată grafic, utilizându-se diagrama circulară, care va genera grafice pentru abstractizarea vizuală a datelor și va permite vizualizarea distribuției datelor cercetate.

Astfel, s-a determinat că standardele și cadrele de securitate recomandate pentru implementare în IÎS, atunci când scopul rezidă în crearea cadrelor sistemice de securitate, sunt: ISO 27001, COBIT, ITIL sau soluția hibridă. Majoritatea cercetătorilor însă recomandă propriile

cadre de securitate cibernetică și a RCE, bazându-se pe ipoteza că standardele/cadrele enumerate mai sus nu sunt orientate spre implementare în instituțiile de învățământ superior.

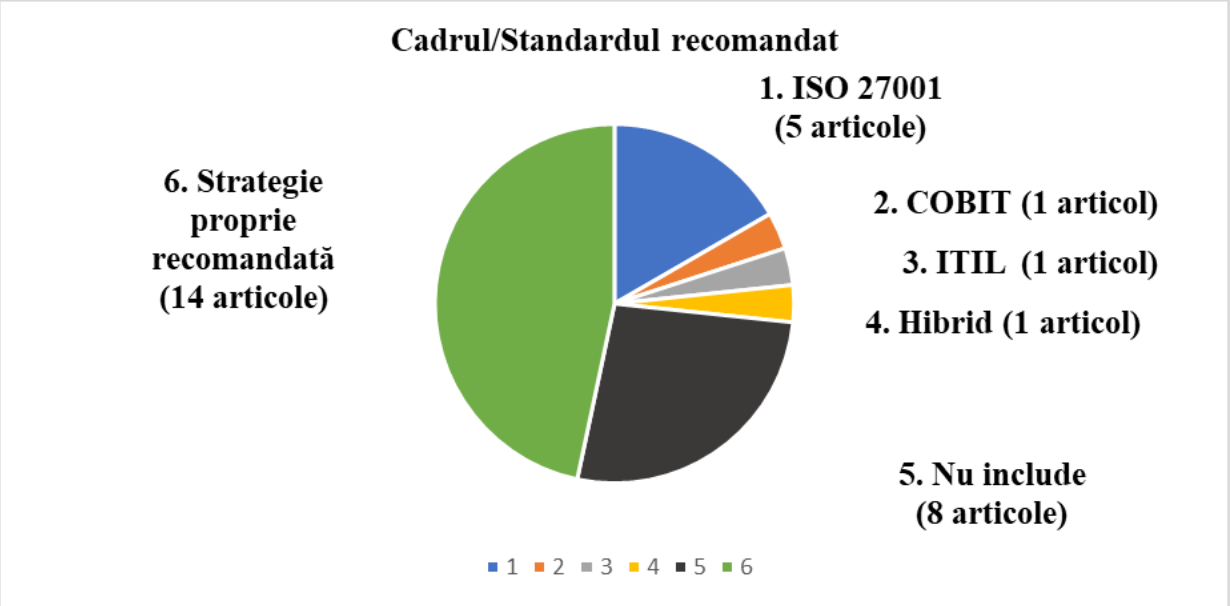

Fig. 2.3. Cadrul/standardul recomandat pentru implementare în IÎS (elaborat de autor)

Standardul ISO 27001 [17] este cel mai des utilizat standard de asigurare a securității informației la nivel internațional [8, 98, 128]. Conform rapoartelor anuale prezentate de ISO [85], certificarea cu ISO 27001 este în continuă creștere. Dacă în 2018 numărul organizațiilor certificate a fost de 31910, în 2020 numărul acestora a fost de 44 486 organizații certificate, cu o creștere procentuală de aproximativ 28%. Republica Moldova nu este o excepție, astfel că numărul organizațiilor certificate în 2020 a crescut față de 2018 de la 3 la 8 organizații.

Cercetările empirice realizate de Școala de Management din Rotterdam, Universitatea Erasmus, realizate în baza a 645 de răspunsuri din partea companiilor, la nivel internațional, au constatat că certificarea cu standardul ISO 27001 a avut un efect pozitiv semnificativ asupra îmbunătățirii securității informației și respectiv a RCE, apreciat de 85% din respondenți [153].

Standardul ISO 27001 recomandă crearea unui sistem de management al securității informațiilor (SMSI) în cadrul organizațiilor [17], și anume, sub acest aspect este o resursă ce trebuie să fie preluată drept referință conceptuală când se dezvoltă cadrele sistemice, care susțin abordarea procesului de securitate de sus în jos. Modelul PDCA (Planificare, Realizare, Verificare, Acțiune) [98, 128, 154] recomandat de ISO 27001, numit ciclul lui Deming, reflectat în figura 2.4, conține un ciclu închis de acțiuni, care asistă procesele sistemice ale cadrelor de securitate.

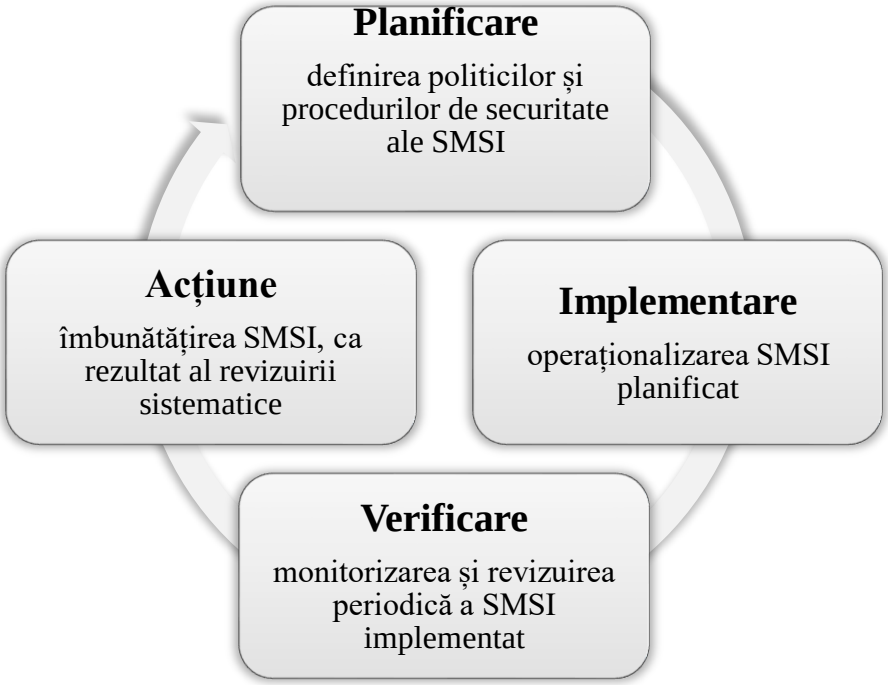

Fig. 2.4. Modelul PDCA (adaptat după [98, 154]**)**

Ciclul lui Deming poate fi utilizat pentru a implementa un sistem de securitate a informației cuprinzător, sau poate fi implementat pentru cadre sistemice pentru profiluri mai înguste, așa cum este cel al CE, orientat exclusiv pe protecția RCE și a serviciilor electronice.

Indiferent de domeniul de aplicare, protecția activelor importante bazate pe CE este realizată prin implementarea SMSI, care are la bază evaluarea riscurilor de securitate și se axează pe triada CIA [98, 126, 128, 155, 156, 27, 41] și, după cum a fost specificat și în capitolul 1 al tezei, reprezintă principiile fundamentale ale securității CE. Sub acest aspect, triada CIA se referă la confidențialitatea transmisiunilor de date și controlul accesului la RCE, integritatea datelor aflate în tranzit și a RCE și disponibilitatea SCE și RCE [27, 156].

Standardul ISO 27001 prevede controale de securitate divizate în 4 secțiuni: control organizațional, controlul personalului, control fizic și tehnologic, care recomandă în total 93 de controale de securitate [17]. Nu toate secțiunile standardului sunt aplicabile în IÎS. Decizia se ia prin elaborarea Declarației de aplicabilitate în care se stabilesc controalele de securitate implementate și se prezintă justificări privind excluderea anumitor controale de securitate, considerate irelevante pentru organizație.

Standardul ISO 27001 este generic și necesită adaptări substanțiale pentru a fi implementat în organizații de anumit profil. Controalele de securitate care se regăsesc în anexa A [17] nu dețin

instrumente operaționale, dar este important ca sistemul de securitate să se bazeze pe acesta [105]. De aceea, este imperativ ca înainte de implementarea unui cadru de securitate, IÎS să determine clar domeniul de aplicare [27] al cadrului sistemic de securitate.

COBIT oferă practici eficiente și stabilește activitățile specifice securității CE într-o structură organizată și flexibilă. Cadrul implementează cele mai bune practici din domeniu și se orientează în special pe crearea politicilor de securitate [83]. COBIT se axează pe generarea unui set structurat de principii, așa ca cerințele organizației, resursele IT și CE, procesele IT și furnizarea informației [83]. Strategia propusă de COBIT nu este altceva decât un set de documente și bune practici care oferă suport unui specialist, auditor sau utilizator să evalueze riscurile cibernetice, controalele implementate și problemele tehnice cu care se confruntă organizația [137].

COBIT este orientat spre managementul riscului, la fel ca și ISO 27001, însă este o strategie care se aplică pentru guvernanța sistemelor de securitate și include următoarele domenii: Planificare și organizare, Achiziționare și implementare, Livrare și suport, Monitorizare și evaluare [157].

După COBIT, obiectivele de control se referă la politici, proceduri, practici și structuri organizaționale, care să asigure obiectivele organizației, astfel încât orice incident de securitate să fie prevenit sau detectat [83]. COBIT include 34 de procese și 13 obiective de control. Fiecare proces conține o diagramă RACI [83], care prezintă rolul fiecărui proces într-o activitate managerială. Activitățile sunt identificate din obiectivele de control și au o structură detailată.

Deoarece controalele COBIT se orientează spre realizarea obiectivelor organizaționale, pentru a operaționaliza un cadru de securitate este necesar suplimentar a potrivi controalele COBIT cu controalele standardului ISO 27001, pentru a se asigura un nivel optim de securitate a CE [86]. În cadrul IÎS se recomandă a utiliza COBIT pentru verificarea nivelului de maturitate a cadrului implementat [126], însă este foarte dificil a operaționaliza acest cadru de securitate.

Cadrul de securitate ITIL reprezintă o asociere între diferite practici și servicii ale tehnologiei informației și comunicațiilor pentru o mai bună gestionare a serviciilor TIC [137], la care se referă și tehnologiile comunicaționale. Serviciile sunt caracterizate ca un mijloc de a oferi valoare clienților fără a crește riscurile de securitate sau costul. ITIL este o librărie care conține un set de 5 cărți și 26 procese ce descriu diferite faze ale implementării și oferă o abordare sistematică a guvernării TIC, managementului operațiunilor și controlul serviciilor electronice [84].

Ca și în cazul COBIT, se recomandă a utiliza cadrul ITIL, combinat cu standardul ISO 27001, pentru a integra controalele de securitate recomandate de standardul ISO 27001 în prestarea celor mai bune servicii de management al proceselor, recomandate de ITIL. Cadrul ITIL necesită investiții financiare considerabile, ceea ce reprezintă un factor nefavorabil pentru IÎS.

Pentru un sistem eficient de gestionare a securității CE este obligatoriu să se realizeze managementul riscurilor, care se referă la confidențialitatea, integritatea și disponibilitatea SCE și RCE ale IÎS [129]. Managementul riscurilor poate reduce riscurile aferente anumitor procese importante, pierderi financiare sau deteriorarea reputației instituțiilor de învățământ superior [99] și poate sprijini crearea politicilor de securitate [129]. Aceste argumente au servit drept motiv pentru a analiza standardele de management a riscurilor recomandate deopotrivă cu identificarea cadrelor de securitate recomandate de cercetători, ca parte integrantă a procesului de implementare a sistemului de securitate, prevăzut de standardul ISO 27001 [17], în IÎS și sporirea securității CE.

Odată cu creșterea necesității de implementare și utilizare a tehnologiilor comunicaționale în activitatea IÎS, managementul riscului a devenit un proces obligatoriu, integrat în sistemul de management al securității informației [150] în general și al securității CE, ca parte esențială și critică de protecție a datelor în tranzit. Managementul riscului include 3 procese [150]: estimarea riscului, atenuarea riscului și evaluarea riscului.

Există mai multe modele disponibile pentru managementul riscului atât calitative, cât și cantitative [127, 155]. Scopul aplicării unui cadru de management al riscului în IÎS este evaluarea nivelului de risc al activelor bazate pe CE universitare [127].

Cadrul selectat trebuie să includă controale de securitate, care se bazează pe riscurile reale ale activelor și operațiunilor din cadrul organizației [127]. În urma studiului realizat s-a identificat că principalele cadre pentru abordarea riscului cibernetic în IÎS sunt standardul ISO 27005, cadrul OCTAVE și cadrul OCTAVE Allegro. De asemenea, în unele lucrări științifice se recomandă utilizarea strategiilor propuse de cercetători orientate pe securitatea proactivă, prin realizarea la anumite intervale de timp a testelor de penetrare, pentru identificarea riscurilor de securitate [133, 142], însă aceste strategii nu sunt cuprinzătoare, deoarece identifică riscul prezent și nu se ia în considerație riscul potențial. Deși managementul riscului reprezintă un proces obligatoriu pentru asigurarea securității CE în IÎS, o mare parte din lucrările științifice nu au inclus un mecanism recomandat pentru abordarea acestora.

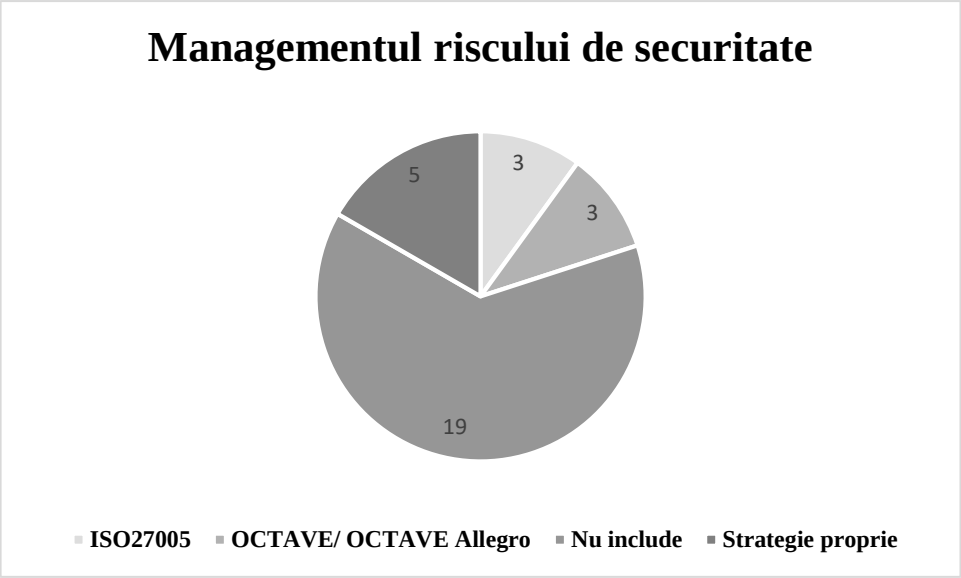

Fig. 2.5. Cadre recomandate pentru managementul riscului (elaborată de autor)

Standardul ISO 27005 conține recomandări privind realizarea managementului riscului și este recomandat de mai mulți cercetători [8, 126, 128, 155]. Activele organizației sunt clasificate în active primare și active de suport [158]. Activele primare sunt totalitatea proceselor și activităților specifice organizației, iar activele de suport sunt echipamente terminale, software, rețea și comunicații, personal și infrastructură [158]. Un pas important pentru managementul riscului, conform standardului ISO 27005, este identificarea și clasificarea vulnerabilităților și amenințărilor de securitate, după categoria activelor la care se referă, reflectate în figura 2.6.

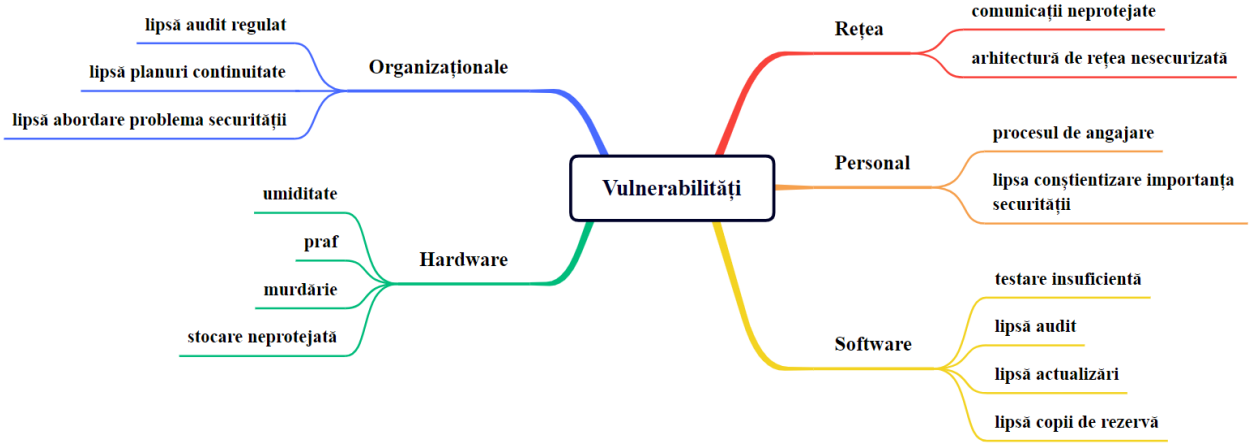

Fig. 2.6. Clasificarea vulnerabilităților conform standardului ISO 27005 (adaptare după [158]**)**

Conform figurii 2.6, există o serie de vulnerabilități care trebuie analizate în cadrul procesului de management al riscului:

- *Echipamentele terminale* pot fi afectate de umiditate, praf, murdărie și stocare neprotejată, vulnerabilitățile sunt ușor de depistat, iar impactul pe care îl pot avea este foarte mare și poate cauza daune financiare importante;

- *Componentele software* pot fi ușor exploatate de către persoane neautorizate din cauza lipsei de audit, care ar fi putut elucida vulnerabilitățile existente sau din cauza că nu au fost testate suficient înainte să fie exploatate. Testarea produselor software în etapa de proiectare și implementare ar putea minimiza riscul de securitate [133, 142, 150, 159]. De asemenea, o vulnerabilitate importantă o reprezintă lipsa actualizărilor, care este primul pas spre un sistem securizat, lipsa copiilor de rezervă realizate periodic, pentru ca în cazul unor incidente de securitate, datele să poată fi recuperate, precum și testarea încercărilor de backup și de recuperare a datelor;
- Una dintre cele mai vulnerabile componente rămâne a fi totuși *securitatea rețelelor de comunicații* [134, 160, 161, 162]; arhitecturile de rețea non-redundante și non-fiabile, dispozitivele de rețea configurate fără a se lua în calcul asigurarea cu liste de control al accesului, firewall, protocoale sigure, utilizarea dispozitivelor de securitate specializate reprezintă cea mai mare vulnerabilitate a CE universitare;
- *Personalul* reprezintă cea mai abstractă categorie de vulnerabilități; atacurile ce se bazează pe comportamentul oamenilor reprezintă 90% din toate atacurile cibernetice [46]. Astfel, procesul imatur de selectare a angajaților sau lipsa de educație în domeniul securității cibernetice provoacă vulnerabilități importante RCE universitare;
- *Infrastructura* universitară este foarte importantă pentru a proteja activele primare și de suport. Accesul la locație, mediile de conexiune utilizate, sistemele de acces automatizat susțin implementarea unui sistem de securitate eficient.

Lipsa de audit și monitorizare continuă a activelor informaționale cauzează vulnerabilități organizaționale importante.

Modelul OCTAVE este unul foarte des utilizat pentru managementul riscului și este implementat în sistemele de securitate universitare pentru a reduce riscul amenințărilor cibernetice prin identificarea cauzelor ce fac sistemul universitar vulnerabil [127]. Aceasta se face prin identificarea activelor universitare și evaluarea vulnerabilităților și amenințărilor specifice activelor [130].

Una dintre variantele modelului OCTAVE este OCTAVE Allegro, care a fost recomandat de cercetători, deoarece permite o evaluare mai cuprinzătoare a mediului de risc operațional, are rezultate mai bune și nu necesită cunoștințe extinse în ceea ce privește evaluarea riscurilor de securitate [99]. Această abordare diferă de abordarea OCTAVE [99], se concentrează în principal pe activele informaționale în contextul modului în care sunt utilizate, unde sunt stocate, procesate și transferate, precum și extinse la amenințări, vulnerabilități și orice fel de perturbări [129], poate fi util în cazul serviciilor Cloud utilizate de IÎS.

Din numărul total de 30 de lucrări științifice publicate, care au avut ca problemă științifică securitatea CE din cadrul IÎS, publicate între 2012-2021, în bazele de date științifice internaționale (figura 2.2), s-a constatat că 46% din lucrări recomandă un cadru propriu de securitate, un mare neajuns însă îl reprezintă lipsa conformității la standardele internaționale, cât și caracterul generic și secvențial al acestor studii, deși problema de cercetare identificată în capitolul 1 accentuează anume caracterul sistemic, iterativ al cadrelor de securitate, care ar permite abordarea securității în mod cuprinzător.

În lucrările științifice care s-au referit la standardul ISO 27001 s-a accentuat caracterul generic pentru a putea fi aplicat în orice sector al industriei, însă această constatare este motiv de incertitudine, deoarece este dificil a transforma controalele de securitate generice în controale clar definite, pentru a fi implementate în medii specifice, așa ca IÎS, deoarece lipsesc instrumentele de operaționalizare. Cadrele de securitate COBIT și ITIL pot fi utilizate ca și cadre de nivel superior, însă sunt dificil de implementat în mediile universitare compuse din mai multe tipuri de rețele parțial deschise. Cu toate acestea, IÎS din Republica Moldova se conformează procesului de la Bologna, care pune un accent deosebit pe implementarea standardelor recunoscute internațional, ceea ce semnifică că standardul ISO 27001 poate fi utilizat ca o strategie de nivel superior pentru dezvoltarea CSSCE. În acest caz, managementul riscului de securitate devine obligatoriu. Cu toate acestea, 63% din lucrările analizate nu abordau problemele legate de realizarea managementului riscului în mediul universitar. Cadrele propuse după cum sunt Octave și Octave Allegro sunt dificil de implementat în medii complexe. Standardul ISO 27005 poate fi utilizat pentru a se asigura conformitatea, însă este necesar a modifica abordarea, datorită diversității activelor informaționale universitare.

Concluzia finală constă în faptul că până în acest moment nu există un cadru de referință, ce poate fi utilizat pentru dezvoltarea cadrelor sistemice de securitate a CE, care să îndeplinească obiectivele universităților la nivel operațional. Standardele internaționale, după cum sunt familia standardelor 27000, nu au emis standarde pentru mediul academic ca pentru alte medii așa ca ISO 27011 pentru organizațiile din domeniul telecomunicațiilor; ISO 27015 pentru serviciile financiare sau ISO 27019 pentru industria energetică. Cu toate acestea, importanța internațională și calitatea demonstrată în timp au constituit premise obiective pentru utilizarea standardului ISO 27001 și respectiv a ciclului lui Deming, pentru asistență de nivel superior la dezvoltarea CSSCE atât pe dimensiunile organizaționale, cât și pe cele tehnice. Pentru abordarea problemelor de management al riscului cibernetic, specific activelor bazate pe CE, va fi analizat și implementat standardul ISO 27005. Categoriile delimitate de către standardul ISO 27005 urmează a fi potrivite cu categoriile de active propuse de ITU [27, 41].

Conform HG 201 [62], IÎS sunt obligate să implementeze cerințe minime de securitate cibernetică, în care problema securității CE se conține în următoarele:

- *Articolul 15:* se referă la controlul accesului la infrastructura dispozitivelor RCE și la sistemele informaționale: gestiunea conturilor de utilizator, condiții de utilizare a parolelor, monitorizarea evenimentelor din sistem și prevederi pentru accesul de la distanță la activele bazate pe CE;
- *Articolul 16:* conține instrucțiuni privind securitatea fizică: identificarea infrastructurii necesare pentru protecția echipamentelor critice, asigurarea cu condiții de mediu adecvate, controlul accesului în spațiile unde se amplasează active bazate pe CE, tehnici de mentenanță a dispozitivelor și controlul accesului în spațiile protejate;
- *Articolul 17:* vizează securitatea operațională: protecția dispozitivelor pentru a se asigura disponibilitatea sistemelor și a RCE, actualizări periodice planificate, controale tehnice realizate la intervale prestabilite de timp, securizarea serverelor și acțiuni pentru identificarea cerințelor de securitate pentru a se asigura funcționarea continuă a RCE organizaționale, clarificarea acțiunilor necesare pentru continuitatea serviciilor, în cazul când a avut loc un incident de securitate, distrugerea echipamentelor scoase din uz și politici clar definite pentru conectarea de pe dispozitivele terminale proprii;
- *Articolul 18:* prevede recomandări privind schimbul securizat de date și de comunicări: stabilirea acțiunilor interzise cu referință la accesarea sau manipularea cu diferit conținut și identificarea metodelor de limitare a accesului.

Cu toate acestea, într-o lucrare științifică publicată de autor [98] au fost identificate lacune între cerințele minime ale HG 201 și controalele de securitate din anexa A a standardului ISO 27001 [17], deși cerințele lipsă vizează aspecte importante pentru IÎS. Pentru identificarea lacunelor a fost utilizată analiza decalajului, iar în continuare vom prezenta câteva concluzii relevante domeniului academic:

- Este necesar a fi prevăzute proceduri clare pentru eliminarea conturilor înregistrate în sistemele universitare a studenților care au absolvit IÎS și a angajaților demiși, implementate politici de securitate cu referire la controlul de securitate *A.8.2. Drepturi de acces privilegiate* și *A.8.3 Restricții de acces la informații*; condiție obligatorie pentru a diminua vulnerabilitățile de securitate aferente utilizării neautorizate a resurselor universitare, după încetarea raporturilor de serviciu, sau a utilizării neautorizate a conturilor inactive de către atacatorii cibernetici pentru inițierea atacurilor ce vizează RCE.
- Este necesar a realiza restricționarea instalării de către utilizatori a produselor program, pentru a minimiza riscurile aferente suprascrierii drepturilor de acces la RCE, prin diferite programe

specializate, cu referire la controlul *A.8.18. Utilizarea programelor utilitare privilegiate,* dar și pentru a limita descărcarea programelor malițioase și a altor amenințări de securitate, care ar crește vulnerabilitatea RCE, cu referire la controlul *A.8.19. Instalarea software-ului pe sistemele de operare.*

- Identificarea capacității necesare pentru stocarea, procesarea și transmiterea datelor prin RCE; este un aspect important, deoarece permite universităților să identifice necesarul de capacitate pentru a se asigura continuitatea procesului academic prin alocarea resurselor necesare și pentru a proteja integritatea RCE; cu referire la controlul *A.8.6. Managementul capacității*.
- Sincronizarea ceasului de sistem pentru toate dispozitivele ce prelucrează sau transmit date este un alt aspect important, deoarece permite, în cazul incidentelor de securitate, a identifica momentul când a avut loc un incident de securitate, cine era autentificat în sistem la acel moment și ce acțiuni realiza pentru luarea deciziilor corecte; aceasta se referă la controlul *A.8.17. Sincronizarea ceasului;*
- Este necesar a evalua riscurile cibernetice și dependența procesului academic de activele bazate pe CE care susțin realizarea acestuia cu referire la controlul *A.8.21. Securitatea serviciilor de reţea;* prin aceasta se recomandă implementarea controalelor în RCE relevante serviciilor academice electronice ce sunt prestate de către IÎS.

Concluziile enumerate au drept scop completarea lacunelor cerințelor minime pentru mediul universitar, dar, pe lângă acestea, pentru a susține abordarea holistică a securității CE în IÎS este necesar a identifica multe alte aspecte atât organizaționale, cât și operaționale, neprevăzute de HG 201, pentru a avea o abordare sistemică și nu una segmentată, iar în acest sens, vor fi utilizate standardele ISO 27001 și ISO 27005.

2.3.2. Metode și materiale pentru dezvoltarea CSSCE

Ciclul lui Deming [163] va fi utilizat pentru a reflecta etapele de implementare a CSSCE în concordanță cu prevederile standardului ISO 27001. Astfel, pentru suport generic, informativ și ca trasare a cerințelor pentru cadrul sistemic de securitate a CE a fost utilizat standardul ISO 27001 [17]. Ca ghid de implementare a controalelor din anexa A a standardului ISO 27001 relevante CE a fost utilizat standardul ISO 27002. Standardul ISO 27005 [158] a fost utilizat pentru suport relevant managementului riscului, iar pentru suportul tehnic și crearea interdependențelor a fost utilizat IT Grundschutz Kompendium, elaborat de Oficiul Federal pentru Securitate în Tehnologia Informației din Germania [164], care este un ghid tehnic ce conține diferite instrumente, recomandări și alte materiale importante pentru îmbunătățirea securității CE în organizații [82].

Factorul decisiv în selectarea IT Grundschutz Kompendium pentru designul și dezvoltarea CSSCE a fost completitudinea informațiilor tehnice pe care le conține, dar și faptul că este actualizat anual, or, cerințele pentru securitatea CE reprezintă un proces continuu și iterativ [82, 165].

O acțiune-cheie în această etapă a fost contactarea responsabililor din IÎS pentru a identifica serviciile academice electronice pe care le prestează instituția și activele de suport pentru prestarea acestora. Ca rezultat au fost identificate și centralizate într-o listă comună toate serviciile academice electronice prestate de către IÎS din RM. A fost întocmită de către autor o listă de verificare a activelor de suport bazate pe CE, conform următoarelor categorii: echipamente terminale, software, rețea și comunicații, personal și infrastructură, ce poate fi consultată în anexa 2 a prezentei teze de doctor. Astfel, cerințele de securitate recomandate sunt orientate pe active de suport reale. Calitatea CSSCE, ca și instanțiere, este înaltă, deoarece se bazează pe contextul real și nu pe date abstracte.

De asemenea, au fost selectate din anexa standardului ISO 27005 [158] lista de amenințări generice la adresa activelor bazate CE. Amenințările de securitate, conform standardului ISO 27005, sunt clasificate conform originii: accidentale, intenționate sau de mediu. Autorul a extins acest concept prin determinarea principiului de securitate pe care îl încalcă o anumită amenințare de securitate. De asemenea, în baza listei de verificare a activelor bazate pe CE a fost generată o listă cu amenințări specifice, în baza rapoartelor anuale de securitate, analizei realizate în capitolul 1, standardelor de securitate. Ambele liste de verificare a amenințărilor de securitate pot fi consultate în anexa 3.

Ciclul lui Deming permite analiza CSSCE la nivel macro, însă marea problemă în acest domeniu este lipsa instrumentelor pentru operaționalizarea cadrelor de securitate [10]. Au fost realizate cercetări extinse pentru a identifica un algoritm potrivit prin care va fi operaționalizat CSSCE, pentru a aduce contribuții aplicative importante. Astfel, a fost identificată metoda științifică, Ingineria Cerințelor de Securitate SRE, care anterior era utilizată doar în procesul de dezvoltare a produselor software, având impact major în elaborarea sistemelor software securizate [14]. Așadar, în studiile științifice recente s-a demonstrat efectivitatea aplicării metodelor SRE și i-a fost recunoscută aplicabilitatea și pentru alte contexte ale ingineriei de securitate [166], precum sunt sistemele cyber-fizice securizate [167, 168] și sistemele de management al securității informației [166]. În prezenta teză de doctor este explicată utilizarea acestei metode științifice pentru dezvoltarea aspectelor operaționale a unui cadru sistemic de securitate orientat pe IÎS.

Metodele SRE permit o abordare structurată în analiza cerințelor de securitate prin care este posibilă dezvoltarea și documentarea cadrelor sistemice de securitate a CE [166], precum este

CSSCE. Aplicarea metodelor SRE, pentru dezvoltarea sistemelor de securitate, reprezintă un proces mult mai complex decât procesul de dezvoltare a software-ului, deoarece trebuie luate în calcul nu doar activele software, ci și alte tipuri de active, precum sunt echipamentele terminale, rețelele și comunicațiile, personalul și infrastructura, respectiv, varietatea amenințărilor de securitate este mai mare, sistemele fiind eterogene.

Ingineria Cerințelor de Securitate se concentrează pe determinarea specificațiilor sistemului și identificarea cerințelor de securitate relevante [10]. Procesul este unul continuu, deoarece amenințările de securitate nu sunt statice, căci noi amenințări și căi de acces la sistemele inginerești apar zilnic. Abordând sistemele de securitate perpetuu, pentru identificarea noilor amenințări de securitate, poate fi creat un set definit de cerințe de securitate, care ulterior pot fi reutilizate. Verificarea cerințelor de securitate se face prin crearea listelor de verificare, care determină completitudinea soluțiilor de securitate [168].

Astfel, a fost selectată pentru implementare metoda propusă de Mellado [14], deoarece este potrivită pentru abordarea sistemică a cerințelor de securitate în mediile eterogene. Metoda se numește Procesul de Inginerie a Cerințelor de Securitate (SREP - security requirements engineering process) și în varianta clasică recomandă 9 etape [14]:

1. *Definirea termenelor și politicilor de securitate;*
2. *Identificarea activelor vulnerabile și/sau critice;*
3. *Identificarea obiectivelor de securitate și dependența lor de sistem;*
4. *Identificarea amenințărilor generice și specifice de securitate;*
5. *Evaluarea riscului cibernetic;*
6. *Identificarea cerințelor de securitate;*
7. *Clasificarea și prioritizarea cerințelor de securitate;*
8. *Analiza cerințelor de securitate identificate;*
9. *Actualizarea depozitului de securitate.*

Pentru operaționalizarea CSSCE vor fi utilizate 7 etape, deoarece etapele 6, 7 și 8 urmează a fi combinate într-o singură etapă. Întreg procesul este reflectat în figura 2.7.

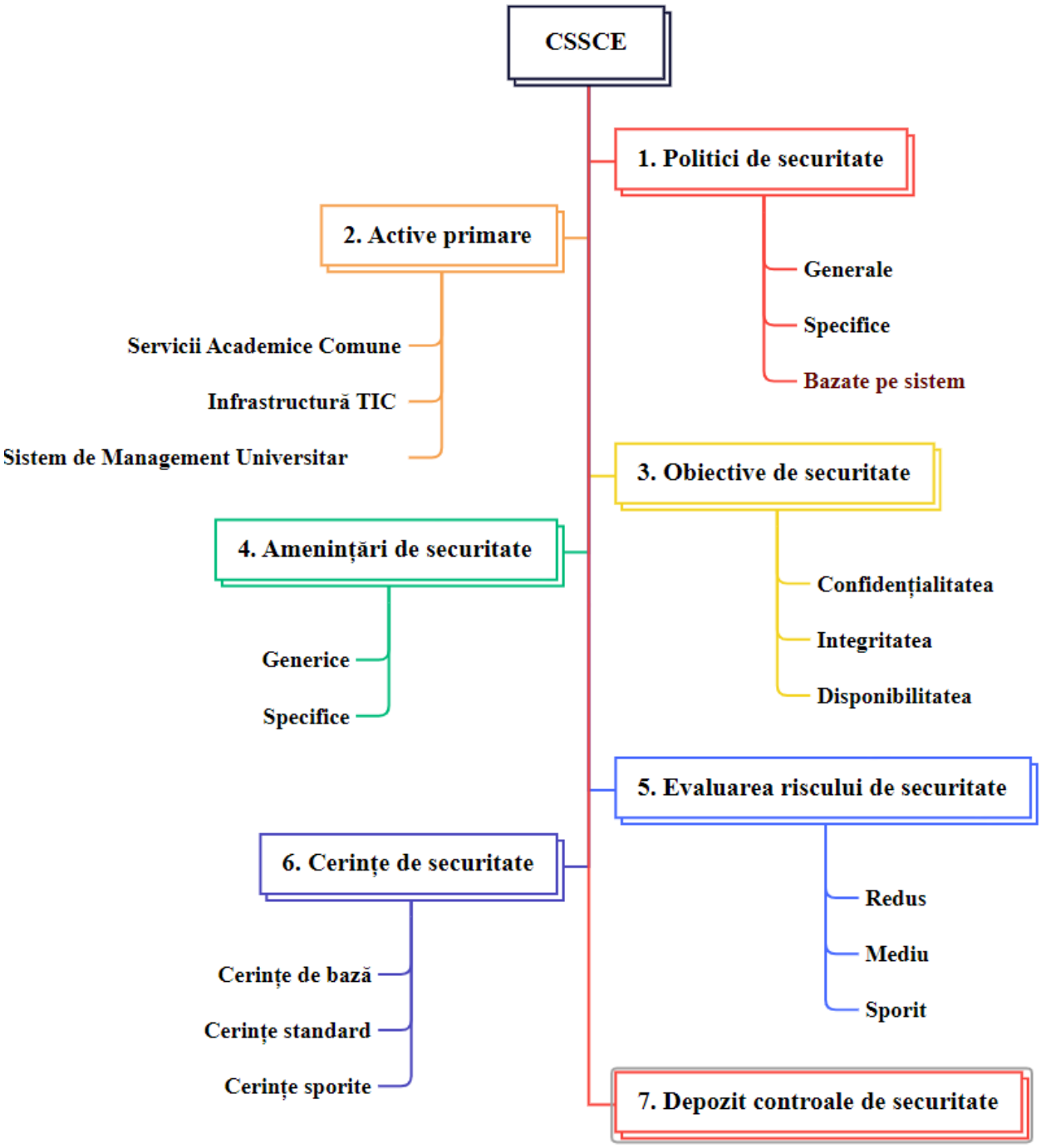

Fig. 2.7. Operaționalizare CSSCE

2.4. Demonstrarea CSSCE

Scopul etapei este de a prezenta cum anume cadrul de securitate dezvoltat rezolvă problema de cercetare [13, 114, 119]. Toate rezultatele științifice obținute au fost prezentate grupului de 15 experți naționali și internaționali, selectați pentru evaluarea CSSCE, și 9 specialiști ai departamentelor TIC din IÎS. Experții au fost selectați din mediul industrial, guvernamental și academic cu vastă experiență în domeniul gestionării CE.

Astfel, au fost prezentate raționamentele care au stat la baza conceptualizării CSSCE în urma căreia a fost obținut cadrul conceptual preliminar, ce abordează sistemic securitatea CE în IÎS și conține acțiuni concrete, ordonate care produc rezultate.

Dezvoltarea CSSCE a permis prezentarea rezultatelor științifice clasificate pe două dimensiuni, organizaționale și tehnice, deoarece securitatea este un proces interdisciplinar. Aspectele organizaționale ale CSSCE au fost dezvoltate, utilizând prevederile standardului ISO 27001, dezvoltarea aspectelor tehnice prin operaționalizarea CSSCE, utilizând metoda științifică SRE.

Pentru a valida rezultatele obținute, a fost creat instrumentul i-CSSCE, care a permis a simula implementarea CSSCE în cadrul unei facultăți, cu scopul vizualizării per ansamblu a întregului proces de implementare și care poate fi utilizat ca aplicație prototip, ce necesită dezvoltare pe dimensiunile propuse, pentru a evalua implementarea cadrelor de securitate.

2.5. Evaluarea CSSCE

Evaluarea ar trebui să determine cât de bine CSSCE suportă rezolvarea problemei de cercetare [13]. Acest lucru este posibil prin prisma criteriilor de valoare sau utilitate [114], stabilite în subcapitolul 2.3.2, comparate cu rezultatul reflectat în subcapitolul 2.3.4.

Evaluarea poate fi făcută în diferite moduri [13], dezvoltarea metricilor având un rol foarte important, deoarece metricile prezintă obiectivele soluției propuse și permit evaluarea performanței cadrelor [116]. Identificarea criteriilor de valoare sunt considerate metrici, care vor evalua măsura în care CSSCE îndeplinește scopul lucrării de cercetare [10].

Reieșind din rezultatele științifice relevante domeniului de securitate a CE pe care ar trebui să le furnizeze și care vor aduce contribuții importante în mediul real, a fost selectată metoda Delphi, deoarece se potrivește pentru obținerea recomandărilor experților când se proiectează un sistem informațional nou [169] sau un cadru de securitate. Observația lui Powell, *”metoda ... este foarte utilă în cazul în care judecățile indivizilor sunt necesare pentru a soluționa lipsa de acord sau starea incompletă a cunoștințelor ...”* [170], descrie foarte bine ceea ce a stat la baza selectării acestei metode pentru a evalua CSSCE, care să fie unul ce implică contribuția specialiștilor în domeniu, dovezi empirice și nu teoretice. Metoda Delphi s-a bazat pe sondajul online care poate fi consultat în anexa 4, bazat pe chestionar și scara Likert [119], pentru a evalua cât de bine CSSCE satisface criteriile de valoare. Această abordare a fost recomandată de mai mulți cercetători la nivel internațional, așa ca C. Sonnenberg and J. vom Brocke [122], J. Venable, J. Pries-Heje, and R. Baskerville [171], R. J. Wieringa [172], realizând studii ce descriu implementarea metodei DSR. De asemenea, studiul aprofundat realizat în subcapitolul 2.3.1 a arătat că în 15 lucrări

științifice, din totalul de 30 analizate, erau propuse studiile de caz, iar în 11 lucrări științifice sondajele și tehnica Delphi [68] bazată pe tehnica chestionarelor și interviului [86] pentru evaluarea cadrelor propuse de cercetători. Datorită complexității cadrelor de securitate, pentru evaluare se utilizează metode calitative, deoarece este dificil a fi evaluat cantitativ.

Evaluarea calitativă facilitează o mai bună înțelegere a percepțiilor, credințelor și atitudinilor participanților la studiul filosofic interpretativ a sistemelor informaționale și de comunicații electronice [173]. Anume metoda calitativă permite a înțelege contextul unei soluții inclusiv în baza comentariilor făcute de specialiștii din IÎS.

Calificativele și recomandările exprimate în rundele metodei Delphi au fost analizate de către autor. Astfel, au fost obținute dovezi empirice (feedback-ul experților și specialiștilor în domeniu), ca mai apoi, prin indicatori statistici descriptivi și inferențiali, să fie interpretate științific calificativele înregistrate.

Indicatorii statistici descriptivi utilizați sunt media, pentru a reflecta tendința centrală a calificativelor date de experți și specialiști din IÎS, și deviația standard pentru a calcula variația grupului de valori [174]. Indicatorii statistici inferențiali au fost utilizați pentru a calcula coeficientul de concordanță W al lui Kendall [16], a măsura acordul dintre evaluatorii sondajului.

În secțiunea de recomandări, experții care au considerat relevant să propună recomandări de îmbunătățire pentru CSSCE, au avut posibilitatea să o facă. Recomandările experților au fost luate în calcul, fiind efectuate modificări relevante în teză. De asemenea, pentru evaluarea calitativă, rezultatele obținute au fost transmise spre examinare către doi profesori din Germania, care au prezentat recenzii pozitive rezultatelor obținute.

2.6. Comunicarea rezultatelor cercetării

Ultima etapă a metodologiei utilizate presupune comunicarea rezultatelor [119], care au fost reflectate prin publicarea articolelor științifice și participarea la conferințe naționale și internaționale cu comunicate. Astfel, au fost descrise detaliat metodele științifice utilizate la dezvoltarea CSSCE, noutatea produsului și în ce mod acesta va avea impact asupra îmbunătățirii securității CE în IÎS.

Rezultatele aplicării științei de proiectare trebuie prezentate atât publicului orientat spre tehnologie, precum și celui orientat spre management [107]. Acest lucru va permite practicienilor să profite de beneficiile oferite de rezultatele aplicative ale tezei de doctor, iar cercetătorilor a construi o bază de cunoștințe cumulativă pentru ulterioara extindere și evaluare a cadrului [107]. Pentru a prezenta rezultatele cercetărilor prezentei teze de doctor au fost publicate 11 lucrări

științifice dintre care 5 articole științifice la conferințe internaționale și 6 lucrări științifice în reviste de profil indexate în bazele de date internaționale.

2.7. Resursele utilizate

Pentru a aplica metoda DSR și a identifica soluții privind problema de cercetare, în studiul literaturii care reprezintă baza teoretică a cercetării aplicative, au fost utilizate bazele de date științifice internaționale și naționale, sondajele pentru care au fost folosite formularele Google și care au fost utilizate pentru a identifica contextul actual al securității CE în IÎS din Republica Moldova, cât și pentru a evalua CSSCE. Pentru a comunica cu părțile interesate din IÎS și experții selectați spre evaluarea CSSCE a fost utilizată poșta electronică, dar și interviurile aprofundate pentru a înțelege contextul domeniului cercetat.

Au fost realizate simulări de implementare a controalelor și politicilor de securitate bazate pe sistem, iar pentru aceasta a fost utilizat Packet Tracer v.8.2. La dezvoltarea prototipului aplicației de implementare a CSSCE a fost folosit PHP, Java Script, HTML5 și CCS3, iar pentru generarea bazei de date MySQL.

Pentru procesarea statistică a rezultatelor sondajului a fost utilizat instrumentul SPSS produs de IBM [175].

2.8. Concluzii la capitolul 2

Fără o componentă puternică care să permită obținerea soluțiilor de cercetare aplicabile în mod explicit, cercetarea în domeniul securității CE se confruntă cu posibilitatea de a pierde influența asupra fluxurilor de cercetare pentru care este esențială aplicabilitatea [114]. Anume din aceste considerente a fost selectată metoda calitativă **Cercetarea în Știința Proiectării DSR.**

Existența multiplelor studii în domeniul ingineresc, care au aplicat metoda DSR pentru a obține rezultate științifice relevante, a contribuit la corectitudinea implementării acesteia. Astfel, efectuând fiecare etapă de cercetare, conform metodei DSR, a fost dezvoltat și perfectat CSSCE.

În acest capitol au fost descrise succint acțiunile privind realizarea scopului cercetării pentru a oferi soluții valide, care ar rezolva problema de cercetare nominalizată. Utilizarea metodei DSR a permis a obține o soluție viabilă pentru o problemă reală.

Așadar, pot fi trasate următoarele concluzii:

1. Cercetarea în domeniul securității CE trebuie să finalizeze cu soluții aplicative care au la bază dovezi științifice.

2. Valaorea studiului empiric poate fi demonstrată prin elaborarea unor soluții aplicabile mediilor specifice după cum sunt domeniile de educație, medicină, financiar etc.

3. CSSCE reprezintă un cadru conceptual prin abordarea sa teoretică și o instanțiere datorită aplicabilității sale în mediile universitare și astfel poate fi definit ca fiind un sistem sociotehnic de tip proces.

4. Pentru a distinge clar cum a fost obținută soluția privind problema de cercetare, ce va contribui esențial la dezvoltarea bazei metodologice, au fost identificate acțiunile relevante fiecărei etape a metodei DSR.

5. Identificarea cauzelor esențiale ale problemei de cercetare privind implementarea cadrelor sistemice de securitate, după cum sunt lipsa în bugetele financiare universitare a compartimentului privind asigurarea securității CE, complexitatea implementării standardelor și a bunelor practici în domeniu, lipsa personalului calificat și imaturitatea domeniului de securitate cibernetică în general și de securitate a CE în particular în Republica Moldova, permite a înțelege contextul și a propune soluții.

6. În baza studiilor privind implementarea metodei DSR și a rezultatelor obținute au fost stabilite următoarele criterii de valoare cu privire la aplicabilitatea CSSCE în IÎS, la fazele de implementare ale CSSCE, la rolurile predefinite ale personalului care va implementa cadrul, la metodele de management al riscului, la eficiența și scalabilitatea CSSCE, care trebuie să se bazeze pe standardele din domeniu pentru a avea importanță internațională; după care poate fi validată soluția obținută.

7. Standardele de securitate ISO 27001 și ISO 27005 au fost selectate drept cadre de referință de nivel superior, iar metoda științifică SRE a fost selectată pentru dezvoltarea aspectelor operaționale ale CSSCE.

3. CADRUL SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE UNIVERSITARE

3.1. Fundamentarea teoretică a cadrului sistemic de securitate a CE

Metodologia de cercetare a fost determinată de direcția propusă de cercetare, iar în acest sens, fundamentarea teoretică a fost realizată prin analiza problemelor în acest domeniu care s-a bazat pe securitatea CE în IÎS, cadrele normative naționale și europene, rapoartele anuale publicate de organizațiile specializate. S-a determinat că una dintre problemele principalele, când se analizează securitatea CE în cadrul IÎS, este lipsa unei abordări sistemice, care să ia în calcul buna funcționare a serviciilor electronice ale IÎS ca sistem interdependent. Astfel, pentru a completa fundamentarea teoretică urmează a fi formulată o nouă definiție a securității CE, bazată pe elementele-cheie ale conceptului; a fi utilizat modelul de securitate Clements–Hoffman [176], considerat baza descrierii formale a sistemelor de securitate [177] pentru argumentarea necesității unei abordări sistemice a procesului de securizare a rețelelor și serviciilor de CE universitare.

Abordarea sistemică poate fi realizată prin implementarea cadrelor de securitate, ce reprezintă sinergia bunelor practici, standarde și recomandări care pot fi implementate de către organizații pentru a-și îmbunătăți măsurile de securitate ale rețelelor și serviciilor de CE [178]. O altă interpretare vine să completeze înțelegerea termenului în limitele utilizării sale în prezenta lucrare științifică: ”Cadrul sistemic de securitate reprezintă o structură fundamentală, pentru organizații și guvern, ce poate fi luată în considerație când se dezvoltă sisteme de securitate cuprinzătoare” [179]. Cadrele de securitate oferă suport pentru implementarea unui sistem de management al securității, pentru o soluție completă și o experiență mai bună de securizare a tehnologiilor de CE, oferind politicile, instrumentele și procedurile necesare pentru îmbunătățirea și menținerea unui sistem de CE securizat [128]. O altă abordare, dar care susține aceeași idee, se referă la cadrul de securitate ca la o soluție completă care conține politici, instrumente și proceduri pentru consolidarea securității rețelelor și serviciilor de CE și mentenanța sistemelor informaționale” [180, 181, 182, 183]. În limitele acestei teze, cadrul sistemic de securitate poate fi definit ca un construct derivat din sinergia standardelor în domeniu și a celor mai bune practici recomandate de organizațiile specializate și cercetători, rezultat din implementarea metodelor științifice relevante, care conține instrucțiuni clare pentru a reduce riscul cibernetic în RCE universitare.

3.1.1. Conceptul de securitate a CE

Conceptul de securitate a CE poate fi descris prin elementele-cheie identificate în definițiile la care s-au referit alți cercetători și organizații specializate expuse în subcapitolul 1.1. Totalitatea elementelor-cheie este reprezentată prin harta conceptuală din figura 3.1.

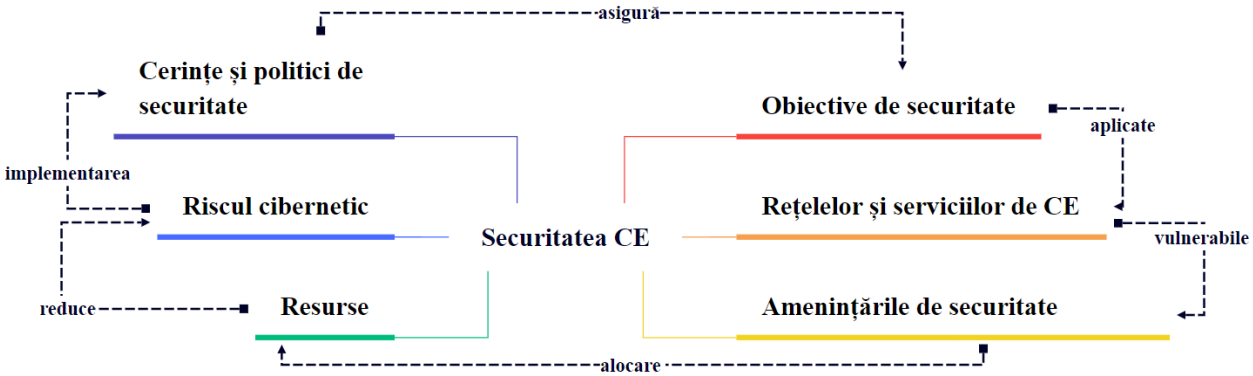

Fig. 3.1. Conceptul de securitate a CE

Astfel, ***securitatea CE poate fi definită ca realizarea obiectivelor de securitate, cum ar fi confidențialitatea, integritatea și disponibilitatea, cu scopul de a se asigura un nivel acceptabil de securitate a rețelelor și serviciilor de CE, a tuturor tehnologiilor comunicaționale, hardware sau software față de amenințările cibernetice, prin alocarea de resurse pentru a reduce riscul cibernetic prin cerințele și politicile de securitate implementate***.

Obiectivele securității CE au fost definite astfel:

- *Confidențialitatea,* care reprezintă limitarea accesului neautorizat la rețelele și serviciile de CE prin prisma modelului AAA, unde primul A reprezintă autentificarea, siguranța că doar persoanele care dețin acreditări pot obține acces la serviciile electronice; al doilea A reprezintă autorizarea, asigurarea că accesul va avea loc în funcție de acreditările utilizatorului, și ultimul A reprezintă auditarea, evidența acțiunilor utilizatorului în timp ce este conectat la RCE.
- *Integritatea,* ce asigură acuratețea cu care sunt manipulate informațiile stocate, procesate sau transmise prin rețelele și serviciile de CE, inclusiv prevenirea interferențelor electromagnetice între rețelele sau serviciile de CE.
- *Disponibilitatea,* care asigură accesul în momentul oportun al utilizatorului autorizat la rețelele sau serviciile de CE și siguranța că rețelele și serviciile de CE pot fi accesate la cerere, indiferent de circumstanțe.

Calitatea serviciilor (Quality of Services – QoS)

Rețelele și serviciile de CE sunt sensibile la diverse amenințări de securitate, de aceea, implementarea cerințelor și politicilor de securitate trebuie să aibă un impact semnificativ asupra

calității serviciilor de CE. Pentru ca utilizatorii să beneficieze de tehnologiile comunicaționale, aceste sisteme trebuie să fie de încredere [184]. Un sistem de CE care nu prevede mecanisme de securitate este considerat nesigur și nepotrivit pentru utilizare [184, 185]. Securitatea la nivel de sistem deseori este analizată ca fiind binară [0, 1]. La nivel macro- așa și poate fi considerată, însă sistemele de CE necesită diferite niveluri de securitate, în dependență de tipul serviciilor pe care le prestează și de mediul în care se află. La selectarea cerințelor de securitate trebuie să se ia în calcul calitatea serviciilor, astfel că securitatea devine unul dintre criteriile constituente ale QoS, deopotrivă cu viteza, utilizabilitatea, disponibilitatea, fiabilitatea etc. Așadar, securitatea și QoS sunt considerate servicii critice ale RCE [184], fiind interdependente și necesită a fi luate în calcul când se proiectează infrastructura de rețea. Cu toate acestea, atât securitatea, cât și calitatea serviciilor sunt dependente de resursele alocate: umane, financiare, informaționale etc., ceea ce poate provoca diverse probleme când se proiectează sistemele de CE, deoarece este dificil a identifica personal care să îmbine eficient cunoștințele pe ambele dimensiuni simultan, problemă ce poate fi soluționată prin implementarea politicilor de securitate ale RCE, în care să fie echilibrate ambele servicii, revizuite în comun de specialiști pentru a exclude cerințele conflictuale. Un exemplu relevant, care susține ideea implementării cerințelor de securitate echilibrate, care să nu aibă impact negativ asupra altor parametri ai QoS, este de exemplu politica de parole a unei organizații. O organizație care nu implementează politici pentru parolele utilizatorilor, din punct de vedere a QoS, va asigura acces rapid la serviciile de rețea, însă din punct de vedere al securității, aceste rețele vor fi nesecurizate. Pe de altă parte, dacă politicile organizației cu privire la parole vor dispune schimbarea frecventă a parolelor și lungimea maximă, acest lucru va avea un impact negativ asupra utilizării rețelelor, respectiv asupra QoS. Astfel, se poate deduce că QoS poate afecta, în etapa de implementare inițială, anume principiul de disponibilitate, care este critic atât pentru securitate, cât și pentru utilizabilitatea rețelelor.

3.1.2. Modelul formal pentru descrierea sistemelor de securitate

Modelul Clements–Hoffman se bazează pe teoria grafurilor, mulțimile fuzzy și teoria probabilității [176, 177]. Teoria mulțimilor fuzzy permite ca obiectele să aparțină unei mulțimi sau cuplurile de obiecte să aparțină unei relații, deținând un anumit grad de apartenență [186, 187] și sunt potrivite pentru evaluarea sistemelor de securitate complexe, în care există un anumit nivel de incertitudine [188]. Teoria mulțimilor fuzzy este aplicată în momentul când este necesar a exprima cantitativ anumite mărimi imprecise [189].

Modelul Clements–Hoffman descrie sistemele de securitate ca fiind compuse din următoarele seturi fuzzy: obiecte ce necesită protecție (O), amenințări de securitate (A), cerințe de

securitate (C) și relația dintre acestea [176]. Obiectele (O) expuse riscului sunt activele universitare bazate pe CE, care susțin realizarea serviciilor academice electronice. Amenințările de securitate sunt caracterizate prin probabilitatea de apariție, care în sistemele reale posedă un nivel limitat de precizie [176]. Cerințele de securitate (C) nu ar trebui să influențeze calitatea serviciilor. În acest sens este necesar a echilibra nivelul de securitate, astfel încât interoperabilitatea și calitatea serviciilor în RCE să nu fie limitată [190].

Este important a specifica că relația Amenințare–Cerință–Obiect, conform modelului Clements–Hoffman, nu este una 1-1-1 [95], deoarece orice obiect O_i poate fi atacat de una sau mai multe amenințări de securitate A_j pentru care pot fi implementate una sau mai multe cerințe de securitate C_m, după cum este reflectat în figura 3.2.

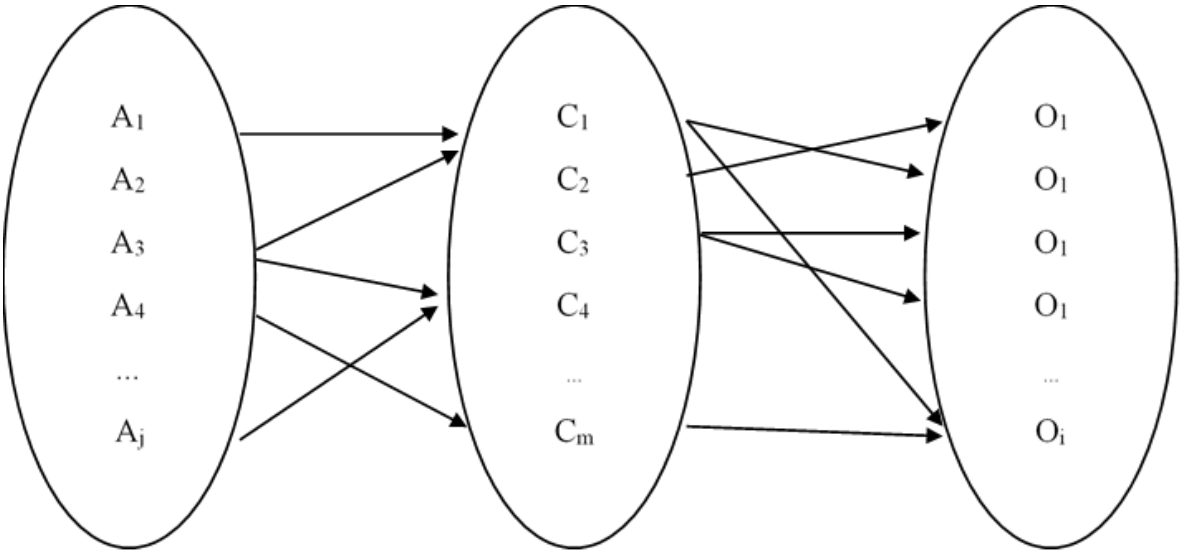

Fig. 3.2. Graful relației Amenințare-Cerință-Obiect (adaptat după [176]**)**

Prin utilizarea modelului Clements–Hoffman pot fi definite următoarele:

Definiția 1. Un sistem de securitate S poate fi definit prin mulțimea $\{O, A, C, V, P\}$:

$$S=\{O,A,C,V,P\}; \tag{3.1}$$

unde:

O – set de obiecte, $o_i \in O$;

A – set de amenințări de securitate, $a_j \in A$;

C – set cerințe și politici de securitate, $c_m \in C$;

V – set vulnerabilități sistem sau căi de penetrare, $v_l \in V$;

P – căi de penetrare protejate, $p_t \in P$.

Conceptele de care depinde sistemul de securitate sunt O,A,C,V,P, iar o_i,a_j,c_m,v_l,p_t sunt elementele acestor concepte.

Definiția 2. Un sistem de securitate S poate fi definit de conceptele O,A,C,V,P și de relațiile care există între aceste concepte, obținute prin produsul cartezian:

$$V=O\times A=\{v_l=(o_{i,}\ a_j),l=1,L\}; \tag{3.2}$$

$$P=C\times V=O\times A\times C=\{p_t=(o_i,a_j,c_m),t=1,T\}; \tag{3.3}$$

Un sistem poate fi deci considerat ca având un anumit nivel de securitate dacă pentru fiecare obiect este atribuită cel puțin o cerință de securitate. Într-un astfel de sistem, pentru fiecare pereche $\{o_i,a_j\}\in V$, există perechea $\{o_i,a_j,c_t\}\in P$. Reieșind din cele expuse, dacă nu există o astfel de corespondență, atunci obiectul o_i este neprotejat, iar sistemul poate fi considerat nesecurizat. Nivelul optim de securitate poate fi atins prin acțiuni periodice, de exemplu utilizând ciclul lui Deming, care va permite a evalua securitatea sistemului.

Definiția 3. Graful sistemului de securitate este format din noduri, nodurile sunt reprezentate prin mulțimea conceptelor de securitate, legătura dintre noduri reprezintă contextul formal (relația) dintre două concepte.

Graful care prezintă un sistem de securitate complet acoperit, compus din 5 seturi de variabile conform (3.1), poate fi analizat în figura 3.3.

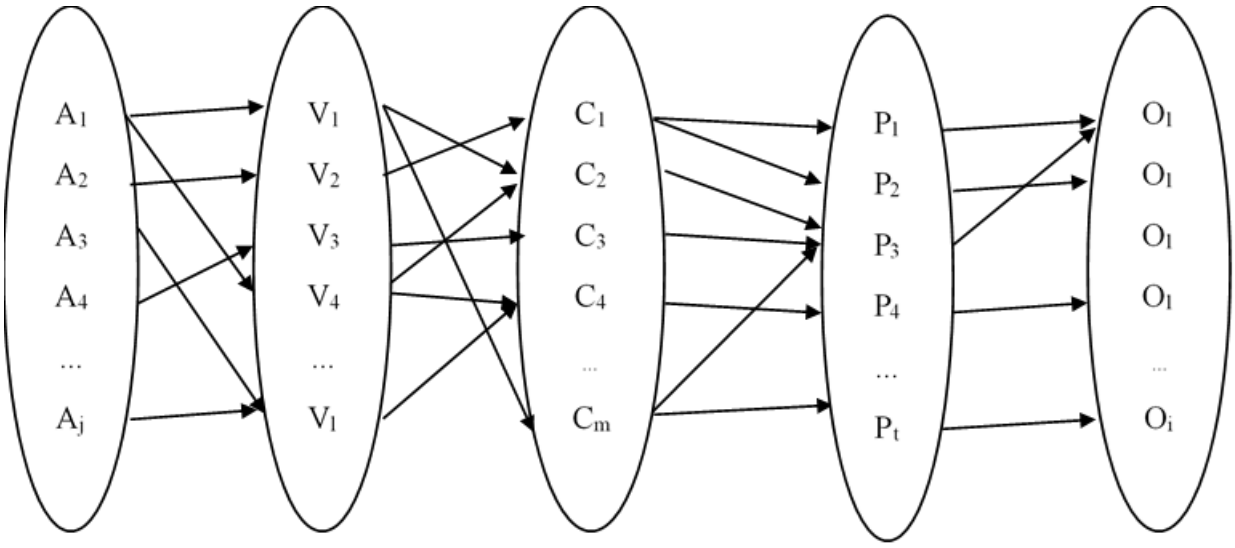

Fig. 3.3. Graful sistemului de securitate (adaptat după [176]**)**

Scenariul descris nu este tocmai realist, ci mai degrabă reprezintă un scenariu ideal, deoarece fiecare cerință de securitate implementată poate oferi o reziliență limitată la amenințările de securitate. De exemplu, politicile de securitate pot fi respectate doar parțial, controlul accesului

poate fi realizat prin parole de o lungime specifică, folosind algoritmi criptografici ușor de spart; amenințările de securitate au caracter dinamic, noi amenințări apar zilnic, astfel fiind imposibil a afirma că toate variabilele sunt cunoscute, iar sistemul are un nivel înalt de securitate. Pentru modelul sistemului de securitate complet protejat se va îndeplini următoarea condiție:

$$\forall(v_l)\in V\ \exists(p_t=\langle o_i, a_j, c_m\rangle)\in P \tag{3.4}$$

Securitatea absolută a activelor informaționale nu poate exista în sistemele reale, deoarece setul de variabile care se referă la amenințările de securitate este imprecis (set fuzzy). Cu toate acestea, identificarea amenințărilor de securitate reprezintă un factor-cheie, utilizat pentru identificarea cerințelor de securitate necesare. Reieșind din condiția (3.4), care indică un sistem complet securizat, se poate deduce că un sistem nu este securizat în cazul următoarei condiții:

$$(v_l)\in V\ \nexists(p_t=\langle o_i, a_j, c_m\rangle)\in P \tag{3.5}$$

Mai mult ca atât, orice p_t, poate să asigure doar o anumită reziliență (R_t), numită potențial defensiv [191] al obiectului (tehnologia comunicațională): $P(o)\geq 0,\ o\in O,$ față de amenințările de securitate a_j, caracterizată prin probabilitatea de a fi depășită [177, 192], care poate fi definită ca potențial ofensiv: $P(a)\geq 0,\ a\in A$. Reziliența sistemului este determinată de gradul de protecție reflectat într-o cerință de securitate pentru un set cunoscut de amenințări (non-fuzzy).

IÎS utilizează sisteme complexe de CE, care asigură funcționalitatea instituțiilor și permit prestarea serviciilor educaționale electronice, care trebuie să asigure cele 3 principii de securitate. Cadrul sistemic de securitate a CE va permite abordarea cuprinzătoare a securității și raționalizarea politicilor și cerințelor de securitate implementate. Importanța implementării cadrului poate fi explicată în raport cu următoarele:

- amenințările de securitate *A(t)* care posedă potențial ofensiv;
- reziliența sistemului *R(t)* care posedă caracter defensiv.

Un indicator de securitate pentru un sistem (IÎS) poate fi considerată probabilitatea ca amenințările de securitate *A(t)* să nu depășească nivelul acceptabil $a_0\geq 0$, pe când reziliența sistemului *R(t)* trebuie să fie mai mare de nivelul-limită b_0, fiind prezentat prin următoarea relație:

$$\beta(t)=P\{A(t)\leq 0,\ R(t)>b_0\} \tag{3.6}$$

Un alt indicator propus pentru utilizare poate fi riscul rezidual R_r, adică valoarea riscului rămasă după tratarea riscului prin implementarea cerințelor de securitate [158], care se determină prin formula (3.7):

$$Rr_t=P_tC_t(1\text{-}R_t), \tag{3.7}$$

unde:

P_t – probabilitatea de apariție a amenințării a_j pentru care a fost implementată cerința de securitate p_t;

C_t – pierderi financiare asociate o_i exploatate de a_j pentru care s-a implementat cerința de securitate p_t;

R_t – rezistența căii de penetrare protejate p_t.

Ca rezultat, poate fi determinat gradul de securitate al unui sistem (S), care este invers proporțional riscului rezidual Rr_t:

$$S = \frac{1}{\sum_{t=1}^{T} P_t C_t (1-R_t)} \tag{3.8}$$

Astfel, managementul securității CE constă în principal din optimizarea distribuției cerințelor de securitate în raport cu căile de penetrare, pentru a se asigura protecția sistemelor de CE universitare. Strategia de securitate, care urmează a fi adoptată de IÎS, trebuie să asigure o reziliență cât mai mare a căilor de penetrare protejate prin cerințe de securitate adecvate, iar costurile de implementare să nu depășească valoarea acceptată de IÎS, care depinde de dimensiunea instituției și de activele financiare ale acesteia. Cadrul de securitate a CE trebuie să îndeplinească următoarele două condiții:

- să minimizeze riscul cibernetic, păstrând funcționalitatea și calitatea serviciilor rețelelor de CE universitare;
- valoarea costurilor de implementare și mentenanță pentru reducerea riscului cibernetic să nu depășească valoarea maximă acceptată.

Acest model poate fi utilizat doar în mod teoretic, deoarece reprezintă un sistem complet securizat, ceea ce în practică este imposibil de atins. Pentru calcularea riscului cibernetic, în cadrul organizațiilor sunt cunoscute mai multe cadre, descrise în subcapitolul 2.3.1, ce pot fi utilizate de IÎS pentru managementul riscului.

Deci, a fost utilizat modelul Clements–Hoffman pentru următoarele:

- formalizarea prin utilizarea aparatului matematic al sistemului de securitate;
- reprezentarea prin grafuri a interacțiunii dintre elementele sistemului de securitate;
- argumentarea necesității de a implementa un cadru sistemic de securitate, ca un proces continuu, pentru reducerea riscului cibernetic pe care îl au tehnologiile comunicaționale, aceasta fiind o cale eficientă de abordare a securității de sus în jos descrisă în capitolul 1 al tezei de doctor.

3.2. Dezvoltarea CSSCE

Cadrul sistemic este format din mai multe componente distincte, eterogene, inseparabile ce îi definesc consistența [193]. Acesta poate fi definit ca o rețea sau un plan de concepte interconectate, care oferă o înțelegere cuprinzătoare a unui fenomen [193]. Cadrele conceptuale sunt create de către cercetători [194] și sunt cadre generative care reflectă gândirea întregului proces de cercetare [194]. Cercetătorii au libertatea de a adopta cadrele existente, dar trebuie să le modifice pentru a se potrivi cu natura contextului cercetării lor, precum și cu natura întrebărilor de cercetare [195].

Astfel, CSSCE reprezintă *sinergia standardelor în domeniu și a celor mai bune practici recomandate de organizațiile specializate și cercetători, abordate prin implementarea metodelor științifice relevante*.

În acest subcapitol urmează a fi dezvoltat CSSCE atât din punct de vedere organizațional, cât și operațional, care să poată fi utilizat ca ghid de implementare a propriului concept de securitate de către instituțiile de învățământ superior din Republica Moldova, fiind orientat spre specificul și serviciile electronice academice naționale.

3.2.1. Abordarea sistemică a securității CE în mediul universitar

În cazul abordării securității CE ca sistem, este necesară abordarea holistică, adică o privire de ansamblu și nu una segmentată [191], deoarece securitatea este interdisciplinară și nu se referă neapărat doar la sistemele de CE, ci implică legislația aplicabilă, structura organizațională și alte aspecte care pot influența acest proces. Securitatea activelor bazate pe CE reprezintă funcționalitatea de bază a unui sistem de securitate, iar după cum a fost demonstrat în subcapitolul 3.1, pentru fiecare activ trebuie identificate cerințe de securitate relevante care vor limita efectul amenințărilor de securitate. Cerințele de securitate pot fi implementate local și în mod sistemic [95]. Local sunt implementate când amenințarea este cunoscută, la fel, și efectul acesteia asupra unei anumite tehnologii ale sistemului de CE, fie dispozitiv intermediar de rețea sau dispozitiv terminal, adică afectează o parte din RCE [95], iar sistemic în cazul unor sisteme complexe, formate dintr-o multitudine de RCE interconectate, vulnerabile la un set fuzzy de amenințări de securitate.

Abordarea sistemică a securității CE în cadrul IÎS va utiliza modelul recomandat de standardele de securitate, modelul PDCA: planificare, realizare, verificare, acțiune; cunoscut ca ciclul lui Deming, pentru creșterea continuă a calității cadrului de securitate, ca urmare a caracterului dinamic al securității CE și caracterului iterativ obligatoriu pentru un sistem de securitate a CE.

Prin aplicarea ciclului Deming se subliniază necesitatea inițierii procesului, precum și integrarea planificării operațiunilor, realizării, verificării constante și acționării conforme cu planificarea [154]. Modelul PDCA a fost reflectat în majoritatea lucrărilor științifice analizate care au susținut implementarea strategiei de securitate bazată pe standardul ISO 27001.

Acțiunile recomandate pentru dezvoltarea CSSCE aplicabil în IÎS distribuite pe cele 4 dimensiuni ale modelului PDCA sunt:

- ***Planificare*** – se referă la procesele importante, organizaționale, așa ca: aprobarea documentată a implementării cadrului sistemic de securitate, stabilirea contextului, determinarea domeniului de aplicare, managementul riscului cibernetic și designul CSSCE. În această etapă sunt stabilite standardele relevante care acoperă realizarea proceselor identificate și documentația relevantă etapei de preimplementare;
- ***Realizare*** – se realizează prin dezvoltarea și implementarea CSSCE, identificarea proceselor secundare, identificarea activelor de suport, identificarea cerințelor de securitate, evaluarea riscului cibernetic, precum și educarea/informarea utilizatorilor;
- ***Verificare*** – se referă la monitorizarea și revizuirea conformității CSSCE de către părțile interesate din cadrul IÎS, cu strategia de securitate a CE abordată, conformă cu prevederile standardelor de securitate;
- ***Acțiune*** – măsurile corective care ar îmbunătăți calitatea CSSCE; include actualizarea controalelor și politicilor de securitate care s-au dovedit a fi ineficiente.

Întregul proces care reflectă ciclul de viață al CSSCE în baza modelului PDCA poate fi analizat în figura 3.4.

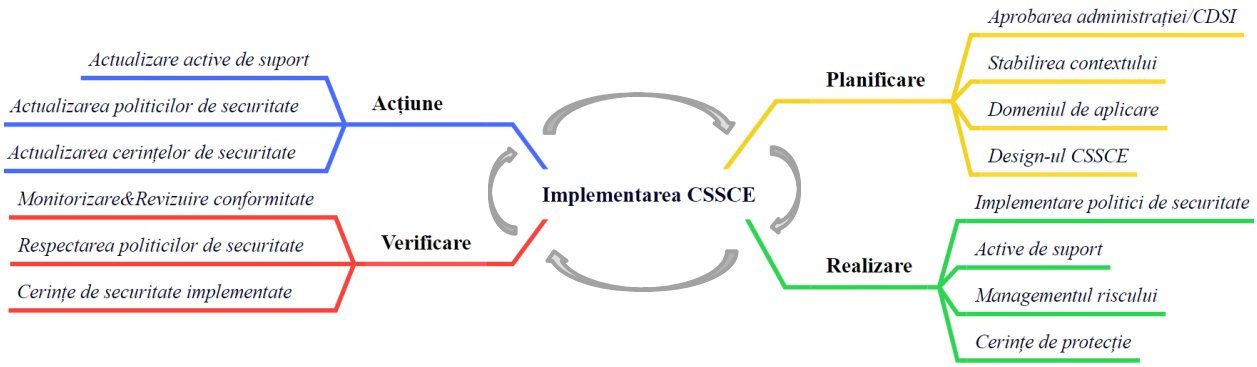

Fig. 3.4. Dezvoltarea CSSCE conform ciclului Deming (elaborat de autor)

Scopul CSSCE este de a aborda sistemic și holistic securitatea CE în mediul academic. CSSCE este un ghid detaliat ce poate fi utilizat de către cercetători și practicienii în domeniu, interesați de implementarea cadrelor sistemice de securitate și pentru identificarea cerințelor de securitate, cu precădere pentru domeniul educațional, însă cu posibilitatea de a fi adaptat la orice tip de organizație. Pentru fiecare activitate identificată se explică semnificația și cum poate fi

aplicată, abordând întreg procesul ca proiect, conform noii versiuni a standardului ISO 27001 [17]. Mai mult ca atât, pentru a susține implementarea corectă a CSSCE sunt recomandate modele ușor utilizabile, ca de exemplu modelul proiectului pentru inițierea procesului de implementare a cadrului de securitate, care poate fi consultat în anexa 5.

3.2.2. Dezvoltarea aspectelor organizaționale

Abordarea sistemică a securității CE, în orice organizație, începe cu procesele organizaționale [10, 196], cu angajamentul administrației de a implementa cadrul sistemic de securitate și cu alte aspecte ce țin de contextul organizației și angajarea personalului necesar, stabilirea domeniului de aplicare (figura 3.5).

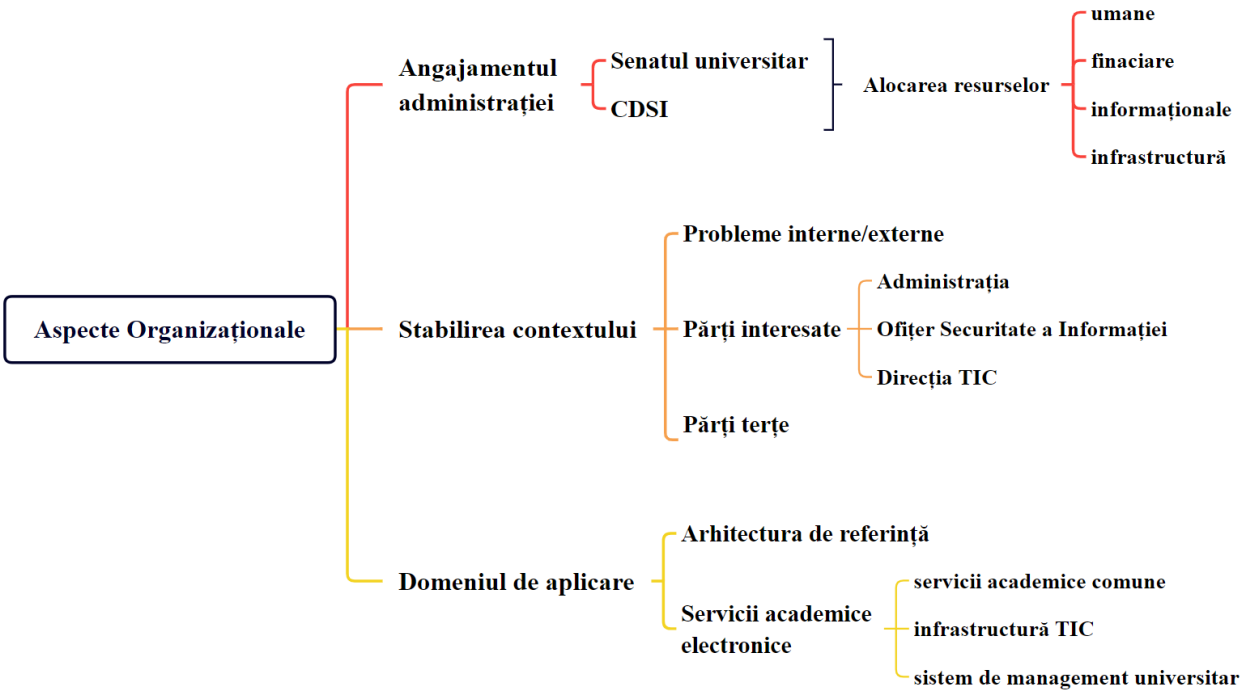

Fig. 3.5. Dezvoltarea aspectelor organizaționale

Aprobarea administrației

Implementarea unui cadru sistemic de securitate a CE trebuie să fie asumată și susținută de top managementul universitar, deoarece reprezintă un proces esențial pentru asigurarea conformității serviciilor de bază. În mediul universitar aceasta se referă la *Senatul instituției*, autoritatea supremă de conducere [197], care este format din președintele Senatului, secretar și senatori, sau la *Consiliul de dezvoltare strategică instituțională* (CDSI). Se stabilește scopul preliminar și prioritățile organizaționale [155], care constau în abordarea cuprinzătoare, sistemică a securității CE, reieșind din raționamentele existente, precum că este mai rentabil să protejezi decât să recuperezi în caz de dezastru, indiferent dacă este produs intenționat sau nu.

Un argument în plus sunt prevederile Strategiei Naționale de Securitate Informațională a RM pentru perioada 2019-2024, care identifică, ca problemă principală pentru asigurarea securității informației în RCE, lipsa sistemelor de securitate integrate la nivel național [198].

Conform standardului ISO 27001, organizația ce are ca scop implementarea unui sistem de securitate, sau, ca în cazul acestei lucrări de cercetare, a unui cadru sistemic de securitate a CE, trebuie în mod constant să aloce resurse ”pentru stabilirea, implementarea, menținerea și îmbunătățirea continuă” [17].

Alocarea resurselor necesare se referă la următoarele:

- *Resursele umane* – se nominalizează persoana responsabilă pentru elaborarea, implementarea și controlul implementării CSSCE, numit în literatura de specialitate Ofițer al securității informației. Pentru aceasta, la nivel superior sunt necesare modificări în organigramele universitare, deoarece Ofițerul de securitate nu face parte din direcția TIC, ci este o unitate de management separată.
- *Resursele financiare* – au un rol important în crearea, implementarea și mentenanța cadrului sistemic de securitate. Alocarea resurselor necesare pentru implementarea cadrului de securitate este o condiție obligatorie pentru inițierea și menținerea procesului.
- *Resurse informaționale* – pentru argumentarea strategiei propuse, validarea cerințelor de securitate propuse și informarea angajaților, studenților și tuturor părților interesate privitor la cerințele obligatorii ce urmează a fi implementate.
- *Infrastructura necesară* – componente hardware și software cu caracteristici potrivite pentru a putea implementa controale de securitate relevante.

Un rol important în acest sens l-ar putea avea Ministerul Educației și Cercetării, care reprezintă autoritatea superioară pentru IÎS din RM. Abordarea la nivel de Guvern a asigurării securității CE a procesului educațional academic ar permite gestionarea centralizată și alocarea resurselor necesare, prin includerea unui coeficient din suma alocată per student de la bugetul de stat.

Stabilirea contextului

Pentru implementarea unui cadru sistemic de securitate util, instituția academică trebuie să definească scopul implementării cadrului de securitate, să identifice elementele procesului educațional academic și activele de suport. Stabilirea scopului este esențială pentru implementarea unui cadru sistemic de securitate, fiindcă reprezintă baza implementării și completitudinea cerințelor de securitate.

Scopul unui cadru sistemic de securitate operațional este de a elimina sau minimiza riscul apariției amenințărilor de securitate, utilizând un set de activități de planificare, organizare, tehnice

și de control [191]. Este important a realiza evaluarea riscurilor de securitate în baza amenințărilor de securitate și vulnerabilităților, a calcula impactul asupra organizației [199]. Astfel, se identifică și se documentează domeniile de control, cerințele de securitate necesare pentru a minimiza riscurile, se documentează motivele pentru care au fost selectate controalele de securitate [199].

Conform prevederilor standardului ISO 27001, IÎS trebuie să identifice problemele externe şi interne, care sunt relevante scopului său [17].

Probleme interne și externe

Pentru a analiza problemele interne cu care se confruntă IÎS, este necesar a lua în calcul următoarele domenii:

- Strategia și obiectivele organizației;
- Standardele implementate la nivel de universitate;
- Procesele academice și activele de suport;
- Contractele/acordurile naționale/internaționale și relațiile derivate cu părți terțe;
- Proprietatea intelectuală și rezultatele cercetărilor;
- Infrastructura fizică și mediul de operare;
- Sistemele de CE;
- Rapoartele precedente de evaluare a riscurilor de securitate (dacă există).

Astfel, pot fi definite următoarele probleme interne, specifice IÎS: manipularea datelor personale; încălcarea confidențialității, accesul neautorizat la activele ce conțin date sensibile ale organizației; pierderi financiare; indisponibilitatea activităților de bază (cursuri, examene, imposibilitatea de a se înscrie la studii); indisponibilitatea serviciilor electronice academice; perturbarea operațiunilor interne; perturbarea operațiunilor cu organizațiile terță; atacul la viața privată a personalului; costuri financiare asociate pierderii personalului, înlocuirii echipamentului, valorii cercetărilor realizate de cercetătorii din universitate; pierderea activelor importante; pierderea avantajului competitiv; pierderea eficacității. Apariția acestor probleme depinde în mod direct de securitatea CE universitare.

Problemele externe nu pot fi controlate de IÎS, iar următoarele aspecte necesită atenție: legile, hotărârile de guvern și regulamentele de ordin superior; mediile socioculturale, naturale și geopolitice; financiare și la nivel micro- și macroeconomic; tehnologice; competitive, poziția unde se plasează instituția în raport cu alte instituții naționale.

Părțile interesate în implementarea cadrului sistemic de securitate

În dependență de structura și dimensiunea IÎS, pentru implementarea CSSCE este necesar, conform standardului ISO 27001, a forma o echipă responsabilă de implementarea și controlul

cadrului de securitate a CE, formată din Ofițerul securității informației și alți membri, angajați ai direcțiilor TIC universitare.

Obiectivul principal al Ofițerului securității informației este de a dezvolta strategii de securitate la nivel organizațional care să fie flexibile, adaptabile și ușor de modificat pe măsură ce mediul de risc este dinamic și volatil, aliniindu-se strategiei de afaceri [200]. Un strateg dezvoltă și conduce implementarea strategiilor care permit organizațiilor să-și atingă scopul și obiectivele [201]. Pe lângă responsabilitatea formală, Ofițerul securității informației comunică cu managementul IÎS, cu managementul și operațiunile serviciilor electronice, cu utilizatorii interni ai IÎS și grupurile de interese speciale interorganizaționale, precum și cu autoritățile publice pentru aplicarea legislației [129].

Ofițerul securității informației trebuie să înțeleagă specificul organizației și domeniul pentru a identifica amenințările de securitate și pentru a crea și a implementa o strategie de securitate bazată pe necesitățile reale, în baza proceselor de afaceri și a informației deținute de organizații. Astfel, cu un puternic accent pe obiectivele organizației, să se realizeze ajustarea și integrarea strategiei de securitate în procesele academice [202, 203]. Ofițerul securității informației trebuie să înțeleagă aspectele tehnice aferente rețelelor și serviciilor de CE, însă cel mai important este să aibă abilități analitice care să-i permită înțelegerea cuprinzătoare pentru întreaga organizație a personalului și studenților, activităților și proceselor adiacente, ce vizează securitatea CE, deoarece sistemele de securitate sunt sisteme sociotehnice. O persoană orientată doar pe aspectele tehnice nu este potrivită pentru această funcție unde comunicarea este aspectul-cheie, care ar asigura succesul implementării cadrului sistemic de securitate. În același timp, este important a menționa că Ofițerul securității informației nu poate impune cerințe de securitate, poate doar recomanda, iar decizia finală aparține top managementului universității.

Standardul ISO 27001 [17] impune calificări regulate și obligatorii ale Ofițerului securității informației, care poate fi recrutat atât din angajații IÎS, cât și din afară atât timp, cât există documente ce atestă calificarea necesară pentru a deține această funcție.

Dependența activităților universitare de părțile terțe

Pentru a determina cum anume părțile terțe externe pot influența domeniul de aplicare a securității CE în IÎS, este necesar a lua în calcul cerințele specifice și regulamentele acestora. De exemplu, care sunt politicele de securitate, regulamentele interne ale organizațiilor din industria națională, partenere cu instituția academică, pentru a putea colabora. În cazul instituțiilor guvernamentale, este necesar a lua în considerație hotărârile și legile implementate, deoarece s-ar putea să existe cerințe specifice (de exemplu, pentru a accesa proiecte guvernamentale), care vor influența conținutul și prevederile cadrului de securitate din mediul universitar.

Datorită caracterului dinamic pe care îl pot avea problemele interne și externe ale instituției, care se pot modifica, cât și interesele părților terțe ce se pot modifica între timp, includerea sau excluderea proceselor și cerințelor de securitate trebuie să fie justificată și documentată corespunzător.

Domeniul de aplicare

Domeniul de aplicare este definit de către administrația universitară. Domeniul de aplicare, conform standardului ISO 27001, se prezintă ca informație documentată, care conține:

- probleme interne și externe;
- părțile interesate pentru implementarea cadrului de securitate;
- dependența activităților universitare de părți terțe.

Domeniul de aplicare a cadrului de securitate poate include întreaga organizație sau secțiuni specifice ale organizației [155], așa cum sunt procesul educațional sau procesul de cercetare. CSSCE este orientat pe procesul educațional academic.

Arhitectura de referință

Necesitatea de a reflecta o arhitectură de referință generică specifică mediului universitar, pe de o parte, oferă o imagine de ansamblu asupra funcționalului tipic [204] activităților academice, iar pe de altă parte, susține crearea arhitecturilor pentru fiecare instituție [205] în parte.

Arhitectura de referință este necesară ca suport pentru a identifica cerințele de securitate pentru activele informaționale din mediul academic. Arhitectura de rețea de referință generică [196], specifică unei instituții academice din Republica Moldova, este reflectată în figura 3.6 în care este reprezentată schema de interconectare a RCE ale Universității Tehnice a Moldovei.

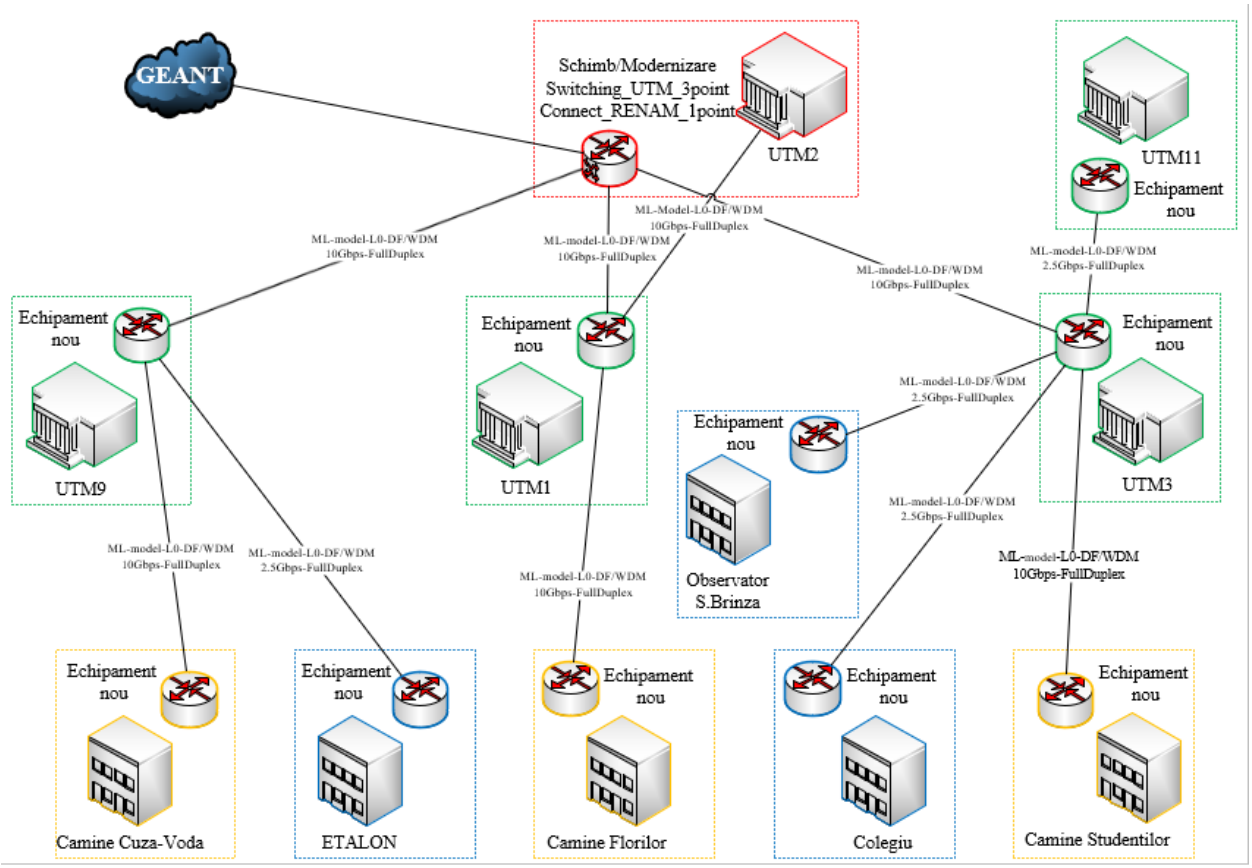

Fig. 3.6. Schema de interconectare a RCE, UTM

În figura 3.6 se poate observa conexiunea externă a unei universități din RM la rețeaua europeană a comunității de cercetare și educație, GEANT. GEANT oferă acces la resursele informaționale globale, inclusiv la Internet, pentru mediile academice. IÎS care participă la proiectul GEANT pentru moment sunt: Universitatea de Stat din Moldova, Universitatea Tehnică a Moldovei și Academia de Studii Economice a Moldovei. Rețeaua universitară de referință este distribuită în mai multe blocuri de studii și cămine studențești.

Fiecare IÎS trebuie să creeze propria arhitectură de referință, care ar permite identificarea necesităților reale, pentru acoperirea serviciilor electronice pe care le prestează, deoarece numărul și complexitatea diferă de la instituție la instituție.

În urma interviurilor semistructurate cu administratorii de sistem din cadrul IÎS din Republica Moldova s-a identificat că RCE utilizează preponderent modelul ierarhic.

Procesul educațional academic

Universitățile moderne sunt foarte complexe din punct de vedere tehnologic, deoarece dețin o infrastructură tehnică sofisticată [206], datorită multitudinii de platforme, aplicații și sisteme academice utilizate pentru realizarea proceselor academice. Acestea reprezintă, conform standardelor, procese de afaceri universitare.

Procesele de afaceri pot fi definite ca ”seturi de sarcini interconectate care conduc la crearea unui produs sau serviciu” [207]. Procesele de afaceri academice de bază sunt educația și cercetarea.

Standardul ISO 27005 abordează riscurile de securitate prin perspectiva activelor informaționale, în care se includ și activele bazate pe CE, definite ca și orice bun ce are valoare pentru organizație și necesită protecție [158]. Conform standardului ISO 27005 [158], toate activele informaționale trebuie să fie clasificate în active primare și active de suport. Activele primare sunt procesele de afaceri și informația, iar activele de suport susțin realizarea activelor primare [196].

CSSCE va lua în calcul doar procesele secundare ale procesului educațional academic, deși activele bazate pe CE și RCE universitare sunt aceleași și pentru procesul de cercetare, în cazul securizării activelor de suport bazate pe CE. Activul primar, Informația, nu este acoperit de CSSCE, deoarece acest domeniu este acoperit de legislația europeană prin Regulamentul general privind protecția datelor (GDPR), intrat în vigoare în mai 2018 [208]. În tabelul 3.1 sunt descrise procesele academice secundare care susțin realizarea procesului educațional academic.

Tabelul 3.1. Procesul educațional academic

Active primare		**Descriere active**
Proces educațional academic	Servicii academice comune	Infrastructura de rețea Stații de lucru fixe Stații de lucru mobile sau BYOD Lucrul la distanță (VPN, WLAN) Servicii centralizate: - servere virtuale - controlul centralizat al accesului, - identificarea și autentificarea utilizatorilor
	Infrastructura TIC	- laboratoare cu echipament specializat - platforme de învățare online - acces la rețelele wireless - acces de la distanță
	Sistemul de management universitar studenți/angajați	- administrarea întregului parcurs academic al studentului - rezultatele sesiunilor de examinare - sistem antiplagiat pentru studenți - taxe suplimentare - ordine de concediu - registrul electronic - fluturași salariali ai angajaților - ordine și regulamente, noutăți universitare etc.

Această listă nu este exhaustivă, aici pot fi incluse/excluse alte procese academice secundare, în dependență de spectrul serviciilor electronice pe care le prestează IÎS, astfel susținându-se criteriul de *scalabilitate* și criteriul *aplicabil în grupul-țintă* al CSSCE.

3.2.3. Dezvoltarea aspectelor operaționale ale CSSCE

În limitele acestei teze, pentru operaționalizarea CSSCE, vor fi parcurse următoarele 7 etape:

1. Elaborarea politicilor de securitate;
2. Identificarea activelor bazate pe CE importante;
3. Identificarea obiectivelor de securitate și dependența de sistem;
4. Identificarea amenințărilor de securitate;
5. Evaluarea riscului cibernetic;
6. Identificarea cerințelor de securitate;
7. Completarea depozitului cu controale de securitate relevante.

CSSCE operațional va putea fi evaluat prin prisma indicatorilor-cheie de performanță identificați, pentru fiecare din cele 7 etape, ceea ce va satisface criteriul de *efectivitate*. Indicatorii de performanță sunt utilizați pentru a măsura nivelul de securitate în cadrul organizațiilor [91], cu referire la un anumit punct de control, cu scopul de a oferi dovezi pentru administrarea eficientă: tehnică și managerială [10].

Sistemele de securitate sunt compuse din seturi de variabile fuzzy, după cum a fost demonstrat în secțiunea 3.1.2. Prin urmare, și securitatea unui sistem de CE este de asemenea fuzzy și nu poate fi măsurată ca și alte concepte, deoarece este mult prea complexă, dinamică și incertă [209]. Scopul securizării sistemelor de orice fel este subiectiv, deoarece nu poate fi măsurat cu exactitate. Comportamentul sistemelor de securitate are deseori caracter instabil, ca de exemplu în cazul amenințărilor de securitate nou apărute, pentru care încă nu au fost determinate cerințe de securitate relevante, iar scopul unui sistem de securitate este să asigure cel mai înalt nivel de securitate a CE într-un moment dat de timp. Astfel, indicatorii de performanță pot servi ca instrumente utilizate pentru luarea deciziilor [210] și pentru stabilirea obiectivelor măsurabile [91]. Indicatorii-cheie ai CSSCE au fost identificați conform etapelor de operaționalizare ale cadrului sistemic și reprezintă finalitatea fiecărei etape în parte. Fluxul de lucru, prin care activitățile vor fi procesate și obținuți indicatorii de performanță, este reflectat în tabelul 3.2.

Indicatorii de performanță au fost selectați conform prevederilor standardelor internaționale, după cum sunt ISO 27001 și ISO 27005, a cadrului normativ european, directiva NIS_2, având la bază modelul de securitate Clements-Hoffman.

Tabelul 3.2. Indicatori-cheie de performanță a CSSCE

Nr. d/o	Operaționalizarea cadrului sistemic de securitate	Intrare	Acțiuni realizate	Ieșire (indicatori cheie de performanță)
1	Elaborarea politicilor de securitate	- Cadrul generic pentru dezvoltarea politicilor de securitate - Structura politicii de securitate - Standardul ISO 27001 - Standardul ISO 27002	- Interviuri, - Sesiuni de brainstorming, - Analiză	- Politică de securitate generală - Politici de securitate specifice serviciilor electronice academice - Politici de securitate bazate pe sistem implementate în tehnologiile comunicaționale
2	Identificarea activelor bazate pe CE importante	- Lista de verificare a activelor de suport - Standardul ISO 27005	- Interviuri, - Chestionare, - Discuții cu părțile interesate, - Ședințe	- Lista activelor de suport pentru fiecare proces secundar
3	Identificarea obiectivelor de securitate și dependența de sistem	- Principiile fundamentale ale securității CE - Procesele secundare academice - Standardul ISO 27001	- Sesiuni de brainstorming, - Analiză	- Lista obiectivelor de securitate și dependența de tehnologiile comunicaționale
4	Identificarea amenințărilor de securitate	- Lista de verificare a amenințărilor generice - Lista de verificare a amenințărilor specifice - Standardul ISO 27005	- Interviuri, - Sesiuni de brainstorming, - Teste de penetrare, - Analiza jurnalelor sistem	- Lista amenințărilor generice și specifice pentru fiecare activ important
5	Evaluarea riscului cibernetic	- Lista activelor de suport pentru fiecare proces secundar - Lista amenințărilor generice și specifice pentru fiecare activ informațional important - Standardul ISO 27005	- Sesiuni de analiză și brainstorming	- Registrul riscurilor cibernetice - Plan de tratare a riscului de securitate - Declarația de aplicabilitate
6	Identificarea cerințelor de securitate	- Depozitul cerințelor de securitate - IT Grundschutz Kompendium - Declarația de aplicabilitate - Standardul ISO 27001	- Sesiuni de brainstorming, - Consultări externe, - Interviuri	- Lista cerințelor de securitate, pentru fiecare activ de suport al unui proces secundar academic - Responsabilii pentru implementare

				Continuarea tabelului 3.2
7	Completarea depozitului cu controale de securitate relevante	- Depozitul cerințelor de securitate - Lista amenințărilor generice și specifice pentru fiecare activ important	- Sesiuni de brainstorming, - Consultări externe, - Interviuri	- Depozit actualizat cu controale de securitate

Scopul securității este unul subiectiv, pe când indicatorii de performanță sunt obiectivi și permit evaluarea unui anumit cadru de securitate de către experți sau echipe de audit. Astfel, indicatorii ce se referă la politicile de securitate sunt importanți pentru a se asigura că utilizatorii respectă prevederile cadrului de securitate, încât intenția de a implementa un cadru de securitate trebuie să fie susținută prin documente specifice, politici de securitate administrative și politici bazate pe sistem (tehnice). În cazul politicilor de securitate administrative, informarea prin documente revizuite periodic, în dependență de modificările aduse în sistemele de CE universitare, poate asigura conformitatea acțiunilor utilizatorilor sistemului de CE cu cerințele de securitate ale cadrului. Politicile de securitate bazate pe sistem reprezintă configurările tehnologiilor de CE prin care să poată fi controlat accesul la CE universitare. Conform modelului Clements-Hoffman, activele reprezintă punctul de referință al sistemelor de securitate, astfel încât generarea listei activelor de suport va permite o imagine de ansamblu asupra elementelor sistemelor de CE ce necesită securizare. Obiectivele de securitate, după cum a mai fost relatat în prezenta teză, reprezintă principiile fundamentale ale securității CE, determinarea relației dintre obiectivul de securitate și activul primar universitar, contribuie la determinarea corectă și argumentată a cerințelor de securitate. Așadar, dacă pentru un anumit activ este critică disponibilitatea, atunci cerințele de securitate implementate trebuie în mod prioritar să prevină/corecteze problemele aferente disponibilității RCE sau SCE. Amenințările de securitate sunt seturi fuzzy de date, însă pentru a realiza un scenariu optim de securitate este necesar a determina un set definit de amenințări generice și specifice, ca parte esențială a sistemului de securitate, pentru a cunoaște spectrul amenințărilor existente, iar pe parcurs această listă trebuie actualizată periodic, pe măsură ce noi amenințări riscă să exploateze activele bazate pe CE universitare, ceea ce va permite implementarea controlului de securitate *5.7. Inteligența pentru amenințări*, al standardului ISO 27001 [17]. Conform standardului ISO 27005 [158], orice organizație care implementează sisteme de securitate trebuie să realizeze evaluarea riscului cibernetic, pentru a identifica riscurile asociate utilizării tehnologiilor de CE, astfel sporind eficiența acestor sisteme. În acest sens, registrul riscurilor va permite gestiunea centralizată pentru analize a riscurilor existente în RCE. În baza planului de tratare a riscurilor, responsabilii vor lua decizii în ceea ce privește riscurile ce pot fi

ignorate sau tratate. Declarația de aplicabilitate este un document obligatoriu, ce trebuie completat de orice IÎS care are intenția de a se certifica cu standardul ISO 27001. În declarație sunt argumentate cerințelor de securitate implementate și justificări obiective în cazul anumitor cerințe ISO 27001 [17], care nu sunt relevante pentru IÎS. Cerințele de securitate sunt elementele de bază, conform modelului Clements-Hoffman. Identificarea acestora va permite a securiza căile vulnerabile de acces la sistemele de CE și implementarea cerințelor comune pentru IÎS naționale. Pentru a efectua controlul asupra procesului de implementare a cerințelor de securitate, obligatoriu se desemnează persoane responsabile. Indicatorul care se referă la depozitul actualizat cu controale de securitate va putea fi utilizat pentru implementarea cerințelor de securitate comune, conform prevederilor directivei NIS_2. Mai mult ca atât, va permite efectuarea controalelor de securitate obligatorii, așa ca *5.27. Învățarea din incidentele de securitate* și *5.28. Colectarea evidenței* ale standardului ISO 27001 [17].

În compartimentele care urmează este descrisă modalitatea de implementare a CSSCE, conform indicatorilor descriși mai sus.

Elaborarea politicilor de securitate

Politica de securitate reflectă atitudinea pe care o are managementul IÎS față de securitatea sistemelor de CE. Obiectivul principal al implementării politicilor de securitate, conform standardului ISO 27002, este să ofere direcție managementului și sprijin pentru securitatea informațiilor în conformitate cu cerințele de afaceri și cu legile și reglementările relevante [211]. Deși politicile de securitate nu necesită multe resurse financiare pentru realizare, sunt foarte dificil a fi implementate [29], deoarece necesită un efort considerabil pentru echipa de implementare.

În mediile educaționale, scopul unei politici de management al securității rețelei este de a determina controlul administrativ, cerințele procedurale și suportul tehnic pentru a asigura protecția corespunzătoare a informațiilor transmise prin RCE. De asemenea, facilitează protejarea integrității și atenuarea riscurilor și pierderilor asociate amenințărilor de securitate la adresa tehnologiilor comunicaționale universitare, fiind un document dinamic, ce necesită revizuiri periodice [68].

Politicile de securitate pot fi clasificate astfel:

- politici de securitate de nivel înalt (sau organizaționale), în care este stabilită strategia, domeniul de aplicare și eforturile IÎS, numită și politică de securitate generală, politică de securitate TIC, politică InfoSec [91]; acestea necesită modificare doar în cazul modificărilor majore în strategiile IÎS și în care este abordată inclusiv securitatea RCE;

- politici de securitate specifice relevante pentru anumite procese sau tehnologii care utilizează CE; sunt revizuite periodic, când a fost implementată o nouă tehnologie sau în cazul anumitor incidente de securitate; conțin instrucțiuni clare de utilizare a diverselor tehnologii comunicaționale; pot fi documente modulare, independente sau cumulate într-un singur document cuprinzător [29]; sunt elaborate de departamentele IÎS responsabile de gestionarea RCE și SCE;
- politici de securitate aplicate tehnologiilor comunicaționale, parte a procesului de configurare sau mentenanță a dispozitivelor de rețea. Pot fi manageriale, așa ca politica de securitate pentru ruter-e și comutatoare, sau tehnice, așa ca listele de control al accesului, configurările firewall-ului sau ale sistemelor de detecție a intruziunilor, configurarea dispozitivelor de rețea; pot fi implementate înainte de implementarea politicilor specifice și de stabilirea regulilor de utilizare a tehnologiilor comunicaționale; sunt actualizate ori de câte ori sunt identificate noi amenințări la adresa securității CE.

Pentru ca politicile de securitate să fie eficiente, trebuie să îndeplinească următoarele criterii:

- *distribuția* – care poate fi realizată prin mediile electronice sau imprimate pe hârtie, instrucțiunile trebuie să fie clare pentru personal, studenți și părțile interesate;
- *revizuiri periodice* – pentru a se asigura o cât mai precisă afinitate la așteptările IÎS;
- *comprehensiune* – IÎS trebuie să se asigure că personalul, studenții și părțile interesate înțeleg cerințele politicii de securitate;
- *angajamentul* – IÎS trebuie să demonstreze că atât administrația, cât și personalul/studenții sunt de acord să respecte prevederile politicii prin semnarea electronică, de exemplu, introducerea acestei posibilități în sistemul de management universitar sau semnarea în registrele speciale;
- *conformitatea* – prin respectarea cadrului normativ național și internațional.

Politica de securitate trebuie să fie publicată pe pagina web a IÎS, condiție susținută de către cercetători [136], însă, conform prevederilor standardului ISO 27002, aceasta nu trebuie să conțină informații confidențiale. În cazul în care politica de securitate conține date sensibile, aceasta poate fi distribuită prin rețeaua intranet a instituției (în cazul în care există), prin e-mail sau utilizând varianta imprimată [135].

Potrivit mai multor cercetători [136, 212], rămâne a fi încă incertă modalitatea de dezvoltare și implementare a politicilor de securitate, iar lipsa unui ghid care să specifice pas cu pas cum poate fi realizată această activitate reprezintă un neajuns al acestei etape. De asemenea, conținutul politicilor de securitate diferă, ceea ce creează incertitudini cu privire la conținut.

Intrare. **N**ecesitatea de a implementa politici de securitate manageriale și tehnice. În baza analizei standardelor și a celor mai bune practici din domeniu, se propune un cadru ce va putea fi utilizat pentru realizarea politicilor de securitate manageriale în mediul academic. Pentru fiecare din cele 3 etape au fost identificate acțiuni specifice.

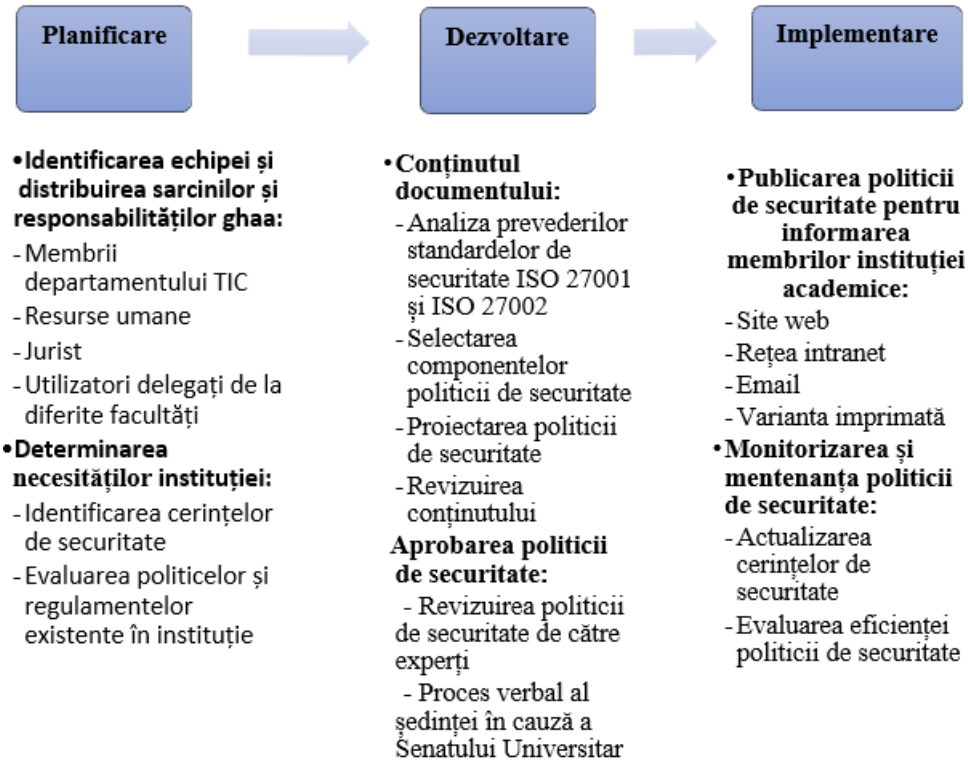

Fig. 3.7. Cadrul generic pentru dezvoltarea politicilor de securitate în IÎS (elaborat de autor)

Etapa de planificare a politicilor de securitate administrative este necesară pentru a identifica responsabilii de realizarea și implementarea politicilor de securitate, pentru ca acestea să fie conforme cu așteptările IÎS față de utilizarea SCE și RCE. Etapa de dezvoltare va contribui la asigurarea conformității conținuturilor cu cerințele standardelor internaționale în domeniu și va finaliza cu aprobarea politicilor de securitate de către Senatul universitar, ca autoritate superioară de conducere. Ultima etapă, de implementare, este cea mai complicată, fiindcă nu este dificil a informa utilizatorii SCE despre prevederile politicilor de securitate, însă este foarte dificil a verifica conformitatea acțiunilor utilizatorilor, mai ales în IÎS, datorită numărului mare și fluctuației utilizatorilor unici ai sistemului. Această etapă este critică pentru un sistem de securitate. Structura propusă în tabelul 3.3, pentru elaborarea politicii de securitate generală și politicilor specifice de securitate, a fost definită ca urmare a analizei structurilor propuse de alți cercetători [29, 212] și organizații specializate [213], conform criteriilor importante pentru IÎS.

Tabelul 3.3. Structura politicii de securitate manageriale (elaborat de autor)

Structura politicii de securitate	Justificări
Titlul	Conform prevederilor din standardul ISO 27002, titlul se referă la tehnologia comunicațională.
Versiune și responsabili de implementare	Deoarece politicile de securitate sunt documente ce necesită permanentă actualizare, este foarte important a stabili la ce versiune se află și pentru când se planifică următoarea actualizare.
Scopul	Descrie așteptările administrației instituției ca rezultat al implementării politicii de securitate, ca de exemplu activele bazate pe CE la care se referă.
Domeniul de aplicare	Descrie domeniul ce va fi acoperit. De exemplu: controlul accesului, securitatea comunicațiilor, utilizarea acceptabilă etc.; cui se adresează respectiva politică de securitate și în ce termene poate fi utilizată tehnologia.
Definiții	Definirea tehnologiilor comunicaționale ce urmează a fi securizate sau ale conceptelor de securitate: confidențialitate, integritate, disponibilitate, pentru a genera claritate.
Cerințele politicii de securitate	Descrie extins, cât mai clar și explicit cerințele instituției față de utilizarea RCE și SCE, care pot fi utilizate de către utilizatori doar pentru a îndeplini procesele universitare, așa ca educația sau instruirea. Poate fi specificat tot în această secțiune și ce nu este permis.
Excepții	Prezintă excepțiile de la prevederile politicii de securitate, cazurile când această politică de securitate nu se aplică.
Penalități	Trebuie să fie clar ce va întreprinde IÎS în cazul când vor fi încălcate prevederile politicii de securitate, în mod echitabil, indiferent de poziția utilizatorului în instituție.
Documente relevante	Descrie alte politici relevante (dacă există) care pot contribui la minimizarea problemelor și incidentelor de securitate, sau link-uri pentru suport adițional.

Acțiuni realizate. Interviurile, sesiunile de brainstorming și analiza domeniilor care ar trebui să fie acoperite prin implementarea politicilor de securitate reprezintă un pas important pentru IÎS.

Ieșire. O politică de securitate ce poate servi ca model este disponibilă în anexa 6. Aspectele acoperite de către IÎS prin implementarea politicilor de securitate pot fi identificate prin discuții și sesiuni, iar cerințele politicilor reieșind din incidentele de securitate cu care s-au confruntat instituțiile sau alte incidente publicate de instituții academice internaționale pentru a preveni potențialele încălcări ale securității CE.

O politică de securitate bazată pe sistem, utilizată pentru a preveni accesul neautorizat pe dispozitivele de rețea, ar putea fi configurarea unui avertisment ca cel din figura 3.8, sau a unei liste de acces pe ruter, pentru a limita accesul la serverul de fișiere, ca cea reprezentată în figura 3.9. Listele de control al accesului pot fi configurate pe dispozitivele de rețea atât pentru traficul de intrare, cât și pentru traficul de ieșire, în dependență de necesitățile instituției.

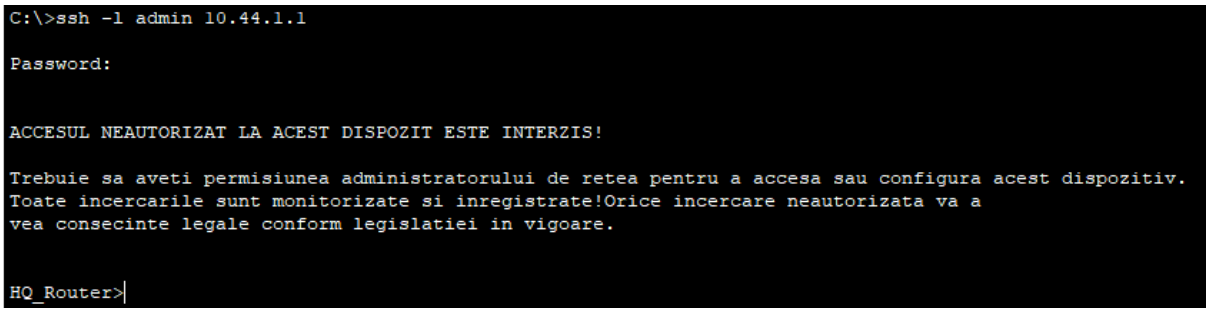

Fig. 3.8. Politică de securitate bazată pe sistem

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard Restrictii_Server_Fisiere
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#permit host 192.168.100.100
R1(config-std-nacl)#deny any
```

Fig. 3.9. Configurare listă de acces al controlului

Este necesar ca politicile de securitate să fie actualizate cu o periodicitate bine stabilită, documentate corespunzător, pentru a se asigura că acestea corespund clar așteptărilor și necesităților IÎS [10]. Modificări în conținutul politicilor de securitate sunt necesare când se modifică domeniul de aplicare, ca în cazul implementării a noi servicii academice electronice sau în cazul depistării atacurilor cibernetice intensificate asupra utilizatorilor finali.

Un exemplu concludent în acest sens este utilizarea poștei electronice corporative, deseori vizată în atacurile cibernetice de tip phishing, phishing-ul reprezentând. Conform rezultatelor cercetării reflectate în capitolul 1, acesta este cel mai des întâlnit atac cibernetic în mediul universitar. Lipsa politicilor de securitate specifice care să acopere utilizarea în siguranță a e-mail-ului, lipsa campaniilor de informare și educare a utilizatorilor și a politicilor de securitate interne prin care să se specifice cum are loc gestionarea poștei corporative a foștilor angajați/studenți facilitează succesul atacurilor phishing.

Criterii de valoare DSR:

- *Aplicabil în grupul-țintă,* prin implementarea politicilor de securitate orientate pe procesele mediului universitar, care vizează activități și incidente ce pot surveni în IÎS;
- *Eficient,* prin stipularea clară a cerințelor față de utilizarea activelor universitare, stabilind de asemenea limite și măsuri corective;
- *Importanță internațională,* prin conformarea la standardele internaționale ISO 27001 și ISO 27002.

Identificarea activelor bazate pe CE importante

Activele primare sunt serviciile care susțin realizarea procesului educațional academic, reflectate în tabelul 3.1. Fiecărui proces secundar academic îi revin mai multe active de suport, fără care procesul educațional nu ar fi realizat. De fapt, anume activele de suport reprezintă ținta atacatorilor cibernetici [168]. Valoarea activelor de suport depinde de impactul lor în funcționarea procesului secundar academic și de costuri. De exemplu, înlocuirea unui dispozitiv de rețea, după cum este ruterul va costa instituția mult mai puțin decât înlocuirea unui server fizic, iar lipsa accesului la Internet pe o anumită dimensiune a rețelei va avea un impact mai mic decât lipsa tuturor serviciilor prestate de un server compromis.

Pentru identificarea activelor valoroase, un suport important este lista de verificare a activelor de suport propusă (anexa 2), în listă pot fi adăugate alte active. Echipa care va utiliza CSSCE ca și cadru de referință, va putea selecta activele din lista de verificare propusă. Mai multe detalii despre valoarea activelor vor fi expuse în etapa de evaluare a riscului.

Intrare. Anexa 2.

Acțiuni realizate. Discuțiile cu părțile interesate, cu responsabilii de procese academice ar putea identifica activele de suport, valoarea și rolul pe care îl au în realizarea procesului secundar. Ședințele comune, la care să participe reprezentanți din mai multe IÎS, ar putea avea ca rezultat o listă completă cu active de suport.

Ieșire. Lista activelor de suport în fiecare proces academic. În tabelul 3.4 sunt prezentate activele de suport identificate prin interviuri cu responsabilii din cadrul IÎS naționale. Lista nu este una definitivă, pot fi adăugate și alte procese academice și active de suport.

Tabelul 3.4. Active de suport (elaborat de autor)

Procese secundare academice	Active de suport				
	Echipamente terminale	**Software**	**Rețea și comunicații**	**Personal**	**Infrastructură**
Sistemul de management informațional studenți/ angajați	Server Desktop PC Laptop	VMWare Virtualizare Linux Server Sistem de stocare centralizat Server Web Server DNS LDAP Server Fișiere Server Email SSL VPN	Switch Ruter Punct de acces Gateway VPN LAN/VLAN Firewall IDS/IPS	Direcția TIC Profesori/ Studenți Personal non-didactic	Camera serverelor Birou UPS Generator Clădire Medii de conexiune Centru de date
Infrastructură TIC	Server Desktop PC Laptop Tabletă Smartphone	Windows Server Active Directory Radius, LDAP Server DHCP	Switch Ruter Punct de acces Gateway VPN LAN/VLAN Firewall IDS/IPS	Direcția TIC Profesori Studenți Personal non-didactic	Camera serverelor Săli de calculatoare Birou de acasă UPS Generator Clădire Medii de conexiune Aer condiționat
Servicii academice comune	Server Desktop PC Laptop Tabletă Smartphone	Server Web Server DNS Server fișiere Server email SSL VPN IPSec VPN Active Directory Windows Server Linux Server	Switch Ruter Punct de acces Gateway VPN LAN/VLAN Firewall IDS/IPS	Direcția TIC Profesori/ Studenți Personal non-didactic	Camera serverelor Săli de calculatoare Birou de acasă UPS Generator Clădire Centru de date Medii de conexiune

Criterii de valoare DSR:

- *Aplicabil în grupul-țintă,* în rezultatul acestei etape SRE sunt identificate activele de suport al fiecărui proces secundar academic;
- *Scalabil,* modulele fiind independente prin construcția lor, vor putea fi adăugate sau eliminate de responsabilii de implementare a CSSCE;
- *Importanță internațională,* toate activele de suport au fost clasificate și identificate conform prevederilor standardului ISO 27005.

Identificarea obiectivelor de securitate și dependența de sistem

Obiectivele de securitate au fost definite ca seturi minime de obiective, care, realizate, asigură securitatea RCE și SCE [33]. Principalele obiective de securitate sunt principiile fundamentale ale securității CE, definite în subcapitolul 3.1, triada CIA [156]: confidențialitatea, integritatea și disponibilitatea. Obiectivele de securitate sunt utilizate pentru a se identifica nivelul de securitate necesar unui anumit proces secundar.

Intrare. Principiile fundamentale ale securității CE.

Acțiuni realizate. Sesiunile de brainstorming și analiza impactului pe care îl pot avea amenințările de securitate asupra unui proces secundar definește importanța realizării obiectivelor de securitate, acestea fiind diferite pentru fiecare proces secundar. De exemplu, pentru sistemele de management universitar confidențialitatea și integritatea este critică, pe când disponibilitatea nu. În schimb, pentru celelalte procese secundare, toate cele 3 obiective de securitate sunt importante, deoarece confidențialitatea utilizatorului este importantă pentru a se asigura că doar persoanele autorizate au acces la teste. Integritatea răspunsurilor înregistrate este de asemenea foarte importantă, deoarece în baza acestora studentul urmează a fi evaluat, iar disponibilitatea este critică pentru ca instituțiile să poată să-și îndeplinească misiunea. Toate aceste aspecte depind de context și mediu, așa că o ședință comună, în care să fie implicate mai multe părți interesate, ar putea evidenția și alte aspecte importante.

Ieșire. După efectuarea acțiunilor descrise mai sus, părțile interesate vor avea o viziune mai bună asupra dependenței sistemului de securitate de obiectivele pe care ar trebui să le îndeplinească. Tabelul 3.5 poate servi drept model.

Tabelul 3.5. Dependența obiectivelor de securitate de sistemul universitar (elaborat de autor)

Procese secundare academice	**Triada CIA**		
	confidențialitate	**integritate**	**disponibilitate**
Servicii academice comune	da	da	da
Infrastructură TIC	da	nu	da
Sistemul de management informațional studenți/angajați	da	da	nu

Reevaluarea importanței realizării obiectivelor de securitate poate fi îndeplinită de părțile interesate din cadrul IÎS. În tabelul 3.5, evaluarea a fost realizată din perspectiva autorului.

Criterii de valoare DSR:

- *Eficient*, deoarece de aceasta depinde deciziile ce vor fi luate și controalele de securitate tehnice ce vor fi implementate prioritar;
- *Importanță internațională*, prin conformarea la standardul ISO 27001.

Identificarea amenințărilor de securitate

Amenințările de securitate aferente proceselor academice au fost identificate, utilizând:

- amenințările comune reflectate în anexa C a standardului ISO 27005, care se referă la activele bazate pe CE [158];
- rezultatele empirice descrise în capitolul 1 al tezei de doctor [100];
- analiza rapoartelor internaționale de securitate și a literaturii științifice pentru anul 2020,
- rezultate ce au fost publicate de către autor în două reviste științifice indexate internațional [46, 55] și la o conferință internațională [47];
- IT Grundschutz Kompendium [164].

Intrare. Au fost elaborate două liste de verificare (anexa 3) ce vor putea fi utilizate pentru identificarea amenințărilor de securitate aferente activelor universitare:

- lista amenințărilor generice de securitate include obiectivele de securitate încălcate (confidențialitatea, integritatea, disponibilitatea) și specificul acestor încălcări: accidentale (totalitatea acțiunilor umane ce provoacă accidental daune activelor), intenționate sau provocate de mediu (nu depind de factorul uman);
- lista amenințărilor specifice de securitate pentru fiecare activ de suport.

Acțiuni realizate. Interviurile și sesiunile de brainstorming vor contribui la identificarea și analiza amenințărilor generice și specifice pentru activele valoroase; testele de penetrare și analiza jurnalelor de sistem vor permite dezvoltarea listelor de verificare, deoarece listele nu sunt exhaustive, noi amenințări de securitate apar cu regularitate.

Ieșire. Lista amenințărilor generice și specifice pentru fiecare activ bazat pe CE important.

Criterii de valoare DSR:

- *Eficient,* prin identificarea amenințărilor generice și specifice de securitate pentru fiecare activ bazat pe CE important;
- *Importanță internațională,* satisfăcută prin utilizarea standardului ISO 27005 și IT Grundschutz Kompendium;
- *Scalabil,* atât amenințările generice, cât și cele specifice vor putea fi preluate de către fiecare instituție.

Evaluarea riscului cibernetic

Scopul acestei etape este de a evalua riscul cibernetic al activelor de suport bazat pe CE identificate. Abordarea holistică a managementului securității CE în IÎS este esențială, deoarece permite a oferi o perspectivă de ansamblu asupra tuturor resurselor care necesită a fi protejate. Metodele de evaluare ale riscului trebuie să ia în considerație dependențele dintre resursele ce

asistă serviciile electronice universitare [214], astfel metodele trebuie să aibă capacitatea de a se adapta și a fi dinamice și potrivite pentru mediul universitar și RCE universitare. Deoarece serviciile electronice sunt în continuă modificare, factorii de risc se modifică [203] și afectează activitatea academică [215], iar managementul riscului este tot mai important [216].

Astfel, se propune o nouă abordare pentru evaluarea riscului prin prisma proceselor secundare academice, deoarece procesele secundare sunt limitate ca număr *versus* activele de suport, care într-o instituție academică sunt foarte variate, iar evaluarea riscurilor de securitate prin prisma proceselor academice susține abordarea holistică a securității CE din mediul academic [10]. Deci, când se proiectează un nou proces academic, se iau în calcul riscurile de securitate, acest nou concept fiind numit ”managementul proceselor de afaceri conștient de risc” [217, 218, 219].

O altă problemă ce poate fi soluționată prin abordarea riscurilor de securitate aferente proceselor de afaceri sunt activele bazat pe CE din Cloud și serviciile prestate de părțile terțe, care fac ca identificarea activelor să fie un proces foarte dificil [214].

Această ipoteză este susținută de mai mulți cercetători, care consideră că este mult mai eficient să abordeze evaluarea riscurilor de securitate din perspectiva proceselor de afaceri [214, 218, 220], adică din perspectiva procesului academic, în limitele acestei lucrări de cercetare.

Activele de suport pot asista unul sau mai multe active primare [196], procese de afaceri, de aceea este foarte important a crea dependențe, analiza va avea un rezultat mult mai precis și corect estimat, deoarece procesele de afaceri sunt sursele primare de securitate [221]. Pentru evaluarea riscului cibernetic se iau în considerație impactul și probabilitatea ca un anumit incident de securitate să aibă loc.

O sursă importantă pentru evaluarea impactului o reprezintă interviurile cu proprietarii proceselor secundare universitare, cu administratorii de rețea și alte persoane interesate. Criteriile după care poate fi evaluat impactul riscului cibernetic sunt reflectate în tabelul 3.6.

Tabelul 3.6. Criteriile de evaluare a impactului (elaborat de autor)

Valoarea calitativă	Valoarea numerică	Descrierea impactului
Neglijabil	1	Nu implică costuri suplimentare, serviciile nu sunt întrerupte, reputația instituției nu este afectată, încălcarea neesențială a obiectivelor de securitate.
Redus	2	Implică costuri reduse, indisponibilitatea RCE și SCE de scurtă durată, mici pierderi ale datelor și impact minor asupra confidențialității.
Mediu	3	Implică costuri medii, indisponibilitatea RCE și SCE pe o anumită perioadă de timp, pierderi ale datelor și impact mediu asupra reputației, impact mediu asupra confidențialității datelor electronice.
Sporit	4	Implică costuri înalte, are ca efect indisponibilitatea de lungă durată a RCE și SCE, pierderea datelor electronice sau încălcarea integrității datelor importante, așa ca datele personale, reușita academică, rezultatele cercetărilor, efect negativ accentuat asupra reputației academice a IÎS.

Drept exemplu poate servi analiza impactului atacurilor DoS/DDoS asupra RCE universitare, luând drept referință figura 3.6, ce reprezintă schema de interconectare a rețelelor de CE a Universității Tehnice a Moldovei, care oferă conexiune de 10 Gbps, utilizând fibra optică ce poate fi exploatată cu un atac DDoS mai mare de 9 Gbps.

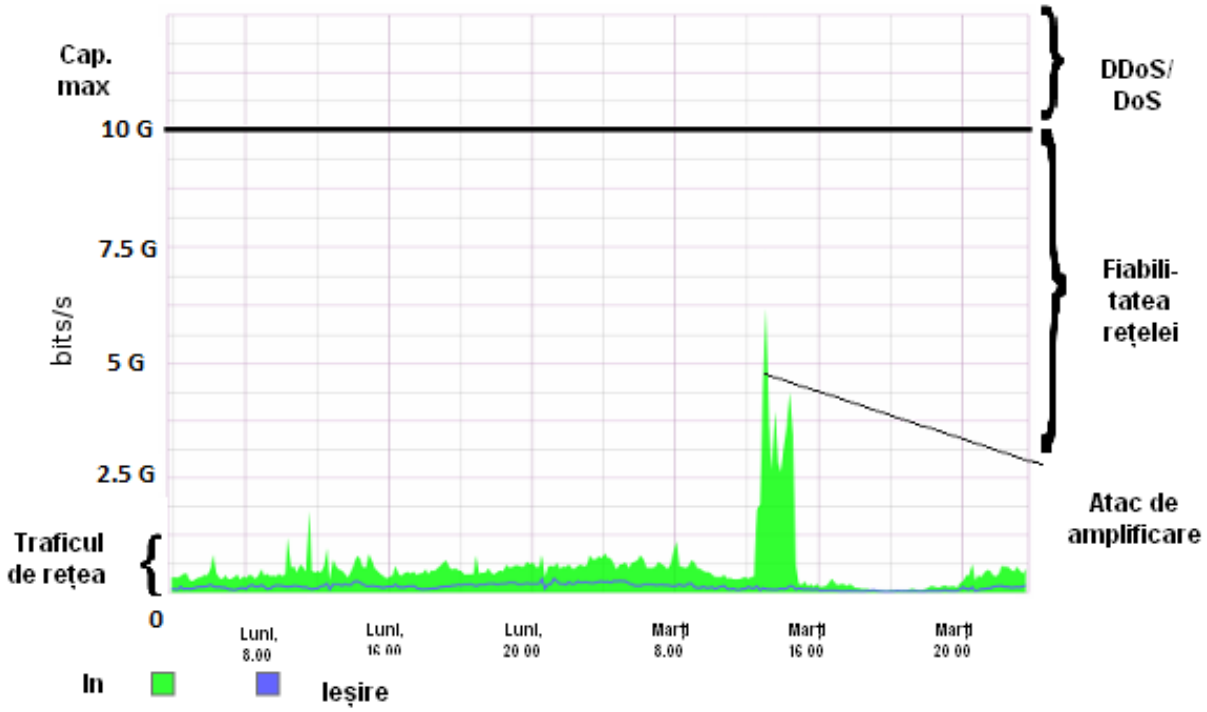

Fig. 3.10. Atacul DDoS/DoS asupra unei rețele cu capacitatea de 10 Gbps (adaptat după [222])

După cum se observă din figura 3.10, fiabilitatea unei asemenea RCE, este reprezentată de decalajul dintre media traficului de rețea consumat în diferite zile, la ore diferite, și sarcina maximă. Utilizatorii finali vor experimenta o degradare a serviciului la traficul de 6-9 Gbps, care va consta în creșterea latenței și vor experimenta un refuz al serviciului în cazul unui trafic mai mare de 9 Gbps. Astfel, luând în calcul tendințele atacurilor de tip DDoS/DoS din ultimii ani, se poate afirma că impactul acestuia ar fi sporit.

Probabilitatea poate fi exprimată prin frecvența cu care amenințările încearcă să exploateze vulnerabilitățile sistemului. În tabelul 3.7 sunt inserate criteriile de evaluare a probabilității.

Tabelul 3.7. Criterii de evaluare a probabilității (elaborat de autor)

Valoarea calitativă	Valoarea numerică	Descrierea probabilității
Neglijabilă	1	Incidentul de securitate are loc o dată pe an
Redusă	2	Incidentul de securitate are loc o dată în trimestru
Medie	3	Incidentul de securitate are loc o dată în lună
Sporită	4	Incidentul de securitate are loc săptămânal

Formula aplicată pentru a calcula valoarea riscului cibernetic este:

$$R=Probabilitatea * Impactul \quad (3.9)$$

Criteriile de evaluare a riscurilor cibernetice sunt următoarele:

- *risc redus*: de la 1-4 (riscul este acceptat);
- *risc mediu*: de la 5-9 (riscul este acceptat condiționat);
- *risc sporit*: de la 10-16 (riscul nu poate fi acceptat).

Criteriile de evaluare a riscurilor cibernetice sunt analizate din perspectiva impactului avut asupra celor 3 obiective de securitate [221]: confidențialitatea, integritatea și disponibilitatea.

Tabelul 3.8. Valoarea riscului cibernetic (elaborat de autor)

Probabilitatea **Impactul asupra RCE și SCE**	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

După rezultatele identificate în tabelul 3.8 se poate observa că pentru un impact foarte înalt, dacă probabilitatea ca acest incident va avea loc este neglijabilă, înseamnă că și riscul rezultat va avea o valoare joasă. În așa mod se verifică valoarea riscului cibernetic și se iau decizii administrative în funcție de criteriile de evaluare a riscurilor specificate mai sus.

Pentru analiza riscului se recomandă identificarea activelor bazate pe CE și valorificarea lor prin prisma relațiilor dependente ce există între activele de suport. De asemenea, este foarte important a calcula costul activului și costul riscului existent, fiindcă nu se implementează cerințe de securitate ce costă mai mult decât valoarea activului protejat. Rentabilitatea economică are un rol important când are loc evaluarea riscului [95].

Conform ISO 27005 [158], fiecărui activ bazat pe CE i se atribuie câte un proprietar, care nu va deține de drept acest bun, însă va fi responsabil și va contabiliza activul. Tot această persoană va fi și proprietarul riscului asociat activului [196]. Se recomandă a fi stabilit proprietarul

proceselor secundare academice [196] și a activelor critice pentru disponibilitatea serviciilor universitare, exemplu reflectat în tabelul 3.9.

Tabelul 3.9. Identificarea proprietarilor activelor informaționale (elaborat de autor)

Nr. d/o	Activul primar	Categoria activului	Adresa	Proprietarul activului
1	Servicii academice comune	Primar	Str.....	Domnul/doamna X/ Departamentul X
2	Sistemul de management informațional studenți/angajați	Primar	Str...	Domnul/doamna Y /Departamentul Y
3	Infrastructură TIC	Primar	Str...	Domnul/doamna Z / Departamentul Z
4	Ruter de bază	Suport	Str...	....

Se recomandă a utiliza baze de date de management a configurației (BDMC), care servesc drept sursă importantă pentru managementul activelor, deoarece oferă detalii importante și permit adăugarea, ștergerea sau modificarea activelor universitare. Deși BDMC nu este responsabil direct de colectarea datelor/activelor, oferă totuși contextul și depozitul necesar pentru a gestiona activele informaționale [221].

După identificarea activelor bazate pe CE universitare trebuie determinată valoarea acestora pentru instituție. Standardul ISO 27005 admite atât evaluarea calitativă, cât și evaluarea cantitativă, fiind o metodă hibrid de management a riscurilor de securitate [196]. Pentru evaluarea calitativă a activului pot fi utilizate următoarele calificative: neglijabil, scăzut, mediu, înalt și foarte înalt. Mai frecvent se implementează trei calificative: scăzut, mediu, înalt, adică, depinde de dimensiunea instituției și de diversitatea serviciilor electronice pe care le prestează [158]. Subprocesele recomandate sunt: identificarea activului, atribuirea activului de suport către procesul secundar academic, calcularea valorii calitative independente a activului după costul și impactul avut în procesul de afaceri aferent, determinarea valorii dependente a activului, iar ultimul pas este identificarea valorii totale a activului informațional. Astfel, valoarea totală a activului dependent reprezintă suma valorii independente și maximum valorii activelor de care acesta depinde, relație încadrată în formula 3.10:

$$V_t = V_{ind} + V_{dep} \tag{3.10}$$

unde:

V_{ind} - poate fi calculată ca suma dintre costul activului bazat pe CE și impactul estimat al activului de suport în procesul de afaceri;

V_{dep} – suma importanței maxime a activelor de care depinde securitatea activului specificat.

Urmează, deci, să fie calculată mai întâi valoarea independentă a activelor, care depinde de costul activului și de impactul pe care îl are în procesele secundare universitate. În tabelele 3.10 și 3.11 se poate observa conversia în valori calitative a costului activului informațional și impactul activului în procesul academic.

Tabelul 3.10. Conversia costului activului într-o valoare calitativă (elaborat de autor)

Valoarea calitativă		**Descrierea**
nivel	**scara**	
Redus	1	Valoarea activului pentru reparație sau înlocuire e mai mică decât 5000 lei
Mediu	2	Valoarea activului pentru reparație sau înlocuire este cuprinsă în intervalul 5000-15000 lei
Sporit	3	Valoarea activului pentru reparație sau înlocuire este mai mare decât 15000 lei

Tabelul 3.11. Conversia impactului activului în procesul academic (elaborat de autor)

Valoarea calitativă		**Descrierea**
nivel	**scara**	
Redus	1	Activul informațional nu are impact asupra proceselor de afaceri universitare
Mediu	2	Reprezintă activ de suport pentru procesul de afaceri
Sporit	3	Activul informațional este important și are impact critic asupra procesului de afaceri

Această abordare a fost recomandată de-a lungul timpului de mai mulți cercetători [214, 219, 223], deoarece are loc o valorificare a activelor informaționale mult mai precisă, luând în calcul dependența activelor [196], însă nu a fost identificată abordarea descrisă în evaluarea riscului cibernetic din instituțiile academice.

Un ultim aspect care susține managementul eficient al riscului cibernetic este instruirea periodică a utilizatorilor sistemelor informaționale universitare [93] atât în momentul angajării (valabil pentru personal) sau admiterii la studii (valabil pentru studenți), cât și la intervale definite de timp, cu o periodicitate cel puțin anuală. Instruirea periodică ar trebui să includă informații despre atacurile cibernetice ce vizează RCE și SCE universitare, cu precădere cele care vizează factorul uman, așa cum sunt atacurile de inginerie socială și phishing-ul. Ar trebui să fie clar descrise semnăturile atacurilor, care îi vor ajuta pe utilizatorii finali să identifice tentativele specifice diferitor tipuri de amenințări de securitate, deoarece orice acțiuni de reducere a riscului cibernetic, din partea specialiștilor, pot eșua în cazul în care utilizatorii finali nu respectă cerințele de securitate în utilizarea RCE și SCE universitare.

Intrare. Drept intrare pentru această etapă SRE servesc rezultatele etapei 2, lista activelor de suport pentru fiecare proces secundar, și a etapei 4, lista amenințărilor generice și specifice de securitate pentru fiecare activ bazat pe CE important.

Acțiuni realizate. Sesiuni de analiză și brainstorming pentru a identifica activele informaționale valoroase și cu risc sporit conform valorii calculate a riscului.

Ieșire. Evaluarea riscului trebuie să fie înregistrată în Registrul riscului cibernetic, luând în considerație bunele practici internaționale [213] sau în Planul de tratare a riscului, recomandat de standardul ISO 27005 [158]. Modelele recomandate de autor pot fi analizate în figurile 3.11 și 3.12.

REGISTRUL RISCURILOR DE SECURITATE											
Departament/Direcție:		**Responsabil ER:**					**Aprobat de:**				**No de referință**
Proces academic:		**Membru ER 1:**									
Locația PA:		**Membru ER 2:**					**Semnătura**				
Data:		**Membru ER 3:**					**Nume:**				
Versiunea:		**Membru ER 4:**					**Funcție:**				
Revizuire planificată:		**Membru ER 5:**					**Data:**				
Identificarea amenințărilor/vulnerabilităților				**Evaluarea riscului**			**Controlul riscului**				
Categorie active	**Active de suport**	**Amenințări/ Vulnerabilități**	**Risc ID**	**Impact**	**Probabilitatea**	**Valoarea riscului**	**Opțiuni tratare riscuri**	**Controale impelementate**	**Proprietarul activului**	**Comentarii**	
Echipamente terminale											
Software											
Rețea și comunicații											
Personal											
Infrastructură											

Fig. 3.11. Model pentru Registrul riscurilor de securitate (elaborat de autor)

PLAN TRATARE RISCURI DE SECURITATE										
Departament/Direcție:		**Responsabil TR:**			**Aprobat de:**					**No de referință**
Proces academic:		**Membru TR 1:**								
Locația PA:		**Membru TR 2:**			**Semnătura**					
Data:		**Membru TR 3:**			**Nume:**					
Versiunea:		**Membru TR 4:**			**Funcție:**					
Revizuire planificată:		**Membru TR 5:**			**Data:**					
Categorie active	**Active de suport**	**Valoarea riscului**	**Amenințări/Vulnerabilități**		**Cerințe de securitate**			**Conformitatea ISO 27001**	**Comentarii**	
					CB	**CSt**	**CS**			
Echipamente terminale	Server									
	Desktop PC/Laptop									
	Smartphone/Tablete									

Fig. 3.12. Model al Planului de tratare a riscului (elaborat de autor)

O etapă importantă pentru IÎS, care are ca scop certificarea în conformitate cu ISO 27001, sau care doresc să verifice nivelul de conformitate a controalelor de securitate implementate cu cele din anexa A a standardului ISO 27001, este ***Declarația de aplicabilitate***, în care se identifică controalele aplicabile în instituțiile academice, se justifică includerea sau excluderea acestora și se verifică statutul controlului. Un model ce poate fi preluat și utilizat este reprezentat în figura 3.13. Declarația de aplicabilitate este documentul obligatoriu în cazul certificării cu ISO 27001 [17].

Clauză Anexa A ISO 27001	Control Anexa A ISO 27001	Descrierea Controlului	Aplicabil	Justificare	Referinţă Control	Statut
A.5 Politicile de securitate a informaţiei						
A.5.1 Directive de management pentru securitatea informaţiei	A.5.1.1 Politicile securităţii informaţiei	Un set de politici pentru securitatea informaţiei trebuie să fie definit, aprobat de către management, publicat şi comunicat angajaţilor şi părţilor terţe relevante.	da	Politica de securitate este necesară pentru a informa angajații/studenții și părțile terțe despre atitudinea IÎS față de securitatea informațiilor	Politica de securitate generală	Implementat
	A.5.1.2 Revizuirea politicii de securitate a informaţiei	Politicile de securitate a informaţiei trebuie să fie revizuite la intervale planificate sau atunci când apar schimbări pentru a asigura conformitatea, compatibilitate şi eficienţa continuă a acestora.	da	Actualizarea obiectivelor și cerințelor din politica de securitate este necesară datorită mediului dinamic specific serviciilor universitare universitare	Informații despre data și persoana responsabilă de revizuirea politicii de securitate	În curs de implementare

Fig. 3.13. Model al Declarației de aplicabilitate (elaborat de autor)

Deși evaluarea riscurilor este foarte importantă pentru identificarea riscului cibernetic aferent unui activ de suport important, această activitate complexă se recomandă a fi realizată doar pentru activele noi sau pentru care nu sunt identificate cerințe de securitate adecvate, sau în cazul producerii unui incident de securitate cu un activ de suport pentru care anterior au fost stabilite cerințele de protecție, însă ele s-au dovedit a fi ineficiente.

Criterii de valoare DSR:

- *Eficient*, datorită identificării activelor bazate pe CE critice;
- *Fazele de implementare,* deoarece specifică clar cum poate fi realizat managementul riscului în mediul universitar;
- *Managementul riscului* este satisfăcut prin evaluarea riscului cibernetic;
- *Importanţă internațională,* deoarece se bazează pe prevederile standardelor ISO 27005 și ISO 27001;
- *Scalabil,* existând posibilitatea de a implementa și utiliza după necesitate oricare din acțiunile și documentele model prezentate.

Identificarea cerințelor de securitate

Este foarte important ca cerințele de securitate să fie cât mai detaliate în datele inițiale, pentru a minimiza erorile în implementarea sistemelor de securitate [224]. Reieșind din aceste considerente, dezvoltarea CSSCE a fost realizată prin sinergia standardelor de securitate ISO 27001, ISO 27002 și a Ghidului tehnic german IT Grundschutz Kompendium. Standardele ISO 27001 și ISO 27002 au fost utilizate ca suport generic, pentru a satisface criteriul de valoare *Importanţă internațională*; iar IT Grundschutz Kompendium – pentru suportul tehnic.

Raționamentele pentru care a fost selectat ghidul german IT Grundschutz Kompendium au fost mai multe. În primul rând, fiindcă recomandă cerințe de securitate tehnice pentru fiecare activ de suport identificat, cerințele de securitate fiind actualizate anual, pe când standardele ISO 27001

și ISO 27002 sunt generice; în al doilea rând, fiindcă este stabilită clar prioritatea cu care trebuie să fie implementate cerințele de securitate: de bază, standard și sporite [164].

Pentru a susține criteriul de valoare, *scalabilitatea*, CSSCE este modular, proprietate recomandată și de cercetători [8], adică pot fi adăugate/modificate noi active de suport ale procesului academic. Prioritizarea implementării cerințelor de securitate poate aduce importante contribuții la minimizarea impactului atacurilor cibernetice și alocarea resurselor financiare necesare [224]. Pentru aceasta, se propune următoarea ordine de implementare:

- *Protecția de bază*, pentru instituțiile academice ce doresc să implementeze propriul concept de securitate a tehnologiilor de CE și să-și asigure o protecție de bază;
- *Protecție standard*, pentru instituțiile ce vor să se conformeze standardelor internaționale de securitate (așa ca ISO 27001);
- *Protecție sporită*, implementată pe activele bazate pe CE universitare care sunt critice și pentru care cerințele de bază și standard nu sunt suficiente.

Fiecare instituție academică poate lua în calcul una sau chiar toate cele trei seturi de cerințe propuse mai sus. Aceasta depinde de strategia instituției și de valoarea activului de suport pentru care se aplică cerințele de protecție, însă ordinea implementării se respectă cu strictețe.

CSSCE ia în calcul următoarele secțiuni din IT Grundschutz Kompendium, versiunea 2021, ce conțin module aplicabile orientate pe activele de suport identificate:

- *SYS* se adresează domeniilor TIC individuale. Conține cerințe de securitate pentru: servere, computere, dispozitive mobile, imprimante și sisteme de telecomunicații;
- *APP* se ocupă de protecția aplicațiilor și serviciilor de comunicații, servicii de director, servicii bazate pe rețea și aplicații afaceri și client. Includ: servere de e-mail, servere web;
- *NET* examinează rețelele de CE sub aspectul conexiunilor de rețea și comunicații. Include module pentru managementul rețelelor, firewall și operațiuni WLAN;
- *ORP* se adresează problemelor de securitate ale personalului;
- *INF* reunește diferite aspecte ale securității infrastructurii, include atât factori arhitecturali, cât și tehnici, de exemplu, modulele Centre de date și Camera serverelor.

Este foarte important a stabili responsabilii pentru implementarea cerințelor de securitate.

Identificarea cerințelor de protecție este un proces iterativ, deoarece cerințele de securitate recomandate necesită validare de către experți. În cadrul IÎS poate fi creată o echipă de specialiști ai direcției TIC. Proprietarii activelor primare și de suport, prin prisma amenințărilor reale cu care se confruntă și a obiectivelor de securitate, vor stabili validitatea cerințelor de securitate, care în caz de necesitate pot fi actualizate. Un document recomandat cu care ar putea finisa această activitate este Raportul de validare a cerințelor de securitate [14].

Intrare. Depozitul cerințelor de securitate (anexa 7); declarația de aplicabilitate; standardul ISO 27001 și standardul ISO 27002 pentru suport generic și verificarea conformității.

Acțiuni realizate. Sesiunile de brainstorming, consultările externe și interviurile cu părțile interesate din cadrul IÎS vor contribui la identificarea cerințelor de securitate conforme cu obiectivele instituționale.

Implementarea cerințelor de securitate prin utilizarea mai multor controale care să asigure protecția activelor de suport, cu precădere a celor din categoria rețea și comunicații, reprezintă pasul cel mai important, deoarece anume dispozitivele de rețea după cum a fost specificat și în capitolul 1, sunt ținta atacurilor cibernetice. Un exemplu de control de securitate pentru nivelul 2 OSI este securitatea porturilor pe un comutator, care va permite a memora anumite adrese MAC ale dispozitivelor terminale, va permite a dezactiva porturile neutilizate și va genera alerte de conectare neautorizată. Utilizarea mediului de simulare Packet Tracer a permis reflectarea modului de implementare a controlului de securitate [225]:

```
switch_decanat(config)#interface range f0/1-2
switch_decanat(config-if-range)#switchport port-security
switch_decanat(config-if-range)#switchport port-security maximum 1
switch_decanat(config-if-range)#switchport port-security mac-address sticky
switch_decanat(config-if-range)#switchport port-security violation restrict
switch_decanat(config-if-range)#interface range f0/3-24, g0/1-2
switch_decanat(config-if-range)#shutdown
```

Un alt exemplu în care este reflectată simularea implementării unui control de securitate la nivel 3 OSI îl reprezintă blocarea cererilor ICMP pe un ruter, care reprezintă una dintre modalitățile de realizare a unui atac de tip DoS și permisiunea de a realiza aceste cereri doar de pe un dispozitiv terminal dedicat. Un alt control de securitate a cărui scop ar avea nu blocarea totală a cererilor ICMP, ci o limitare a numărului admisibil de cereri este limitarea ratei ICMP, care oferă o metodă de limitare a lățimii de bandă ce poate fi utilizată pentru traficul ICMP de intrare pe un port de comutare:

```
router_de_baza(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
router_de_baza(config)#access-list 100 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
router_de_baza(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

Un exemplu de control de securitate implementat pentru nivelul 4 al modelului OSI este utilizarea protocolului TLS/SSL pentru accesul la platformele de învățare, așa ca MOODLE/ELSE și alte resurse web universitare, pentru a evita descoperirea informațiilor de autentificare a utilizatorilor realizate prin atacuri de interceptare a comunicațiilor de date, sau a atacurilor de tip

MiTM. În acest sens, se recomandă a utiliza doar protocolul HTTPS, de nivel 7 OSI și nu protocolul HTTP, care transmite datele în mod necriptat. O problemă similară are și protocolul FTP, care încarcă/descarcă datele necriptate pe server, riscând astfel interceptarea și modificarea acestora.

Ieșire. Lista de verificare a cerințelor de securitate pentru fiecare activ de suport al unui proces secundar academic și identificarea responsabililor pentru implementarea cerințelor de securitate. De asemenea, vor fi identificate controalele de securitate care s-au dovedit a fi ineficiente, eficiente și costurile lor de implementare.

Criterii de valoare DSR:

- *Aplicabil în grupul-țintă,* prin identificarea cerințelor de securitate tehnice, aplicabile activelor bazate pe CE universitare;
- *Eficient,* prin identificarea controalelor de securitate efective cu posibilitatea de actualizare;
- *Scalabil,* echipa de implementare din IÎS va putea selecta din cerințele de securitate propuse care anume să fie implementate;
- *Fazele de implementare* specifică clar ordinea în care trebuie să fie implementate cerințele de securitate: de bază, standard și sporite;
- *Importanța internațională,* având la bază pentru suportul generic standardele ISO 27001 și ISO 27002, iar pentru suportul tehnic – IT Grundschutz Kompendium.

Completarea depozitului cu controale de securitate relevante

Depozitele de securitate sunt create cu scopul reutilizării cerințelor de securitate [14], dar și pentru a crește calitatea acestora: a diminua ambiguitatea, a exclude erorile și alte probleme ce au fost detectate și corectate pe parcurs [226], astfel crescând efectivitatea și utilitatea cerințelor identificate.

Deci, în cazul actualizării cerințelor de securitate, a procesului de audit intern/extern sau a incidentelor de securitate se vor putea identifica soluții ce și-au demonstrat eficiența. Depozitul va conține cartografierea amenințărilor generice și specifice activelor de suport, dar și cerințe de securitate care vor corecta amenințările identificate.

Soluția propusă va asigura continuitatea procesului de asigurare a securității, chiar și când anumiți specialiști valoroși vor pleca din instituție, din diverse motive, deoarece vor fi stocate centralizat cerințele de securitate; mai mult ca atât va permite implementarea cerințelor de securitate comune pentru domeniul educației. Modelul pentru depozitul centralizat de cerințe de securitate poate fi analizat în anexa 8, pentru activul de suport - Server.

Intrare. Depozitul cerințelor de securitate completat în baza modulelor din IT Grundschutz Kompendium și lista amenințărilor generice și specifice de securitate disponibile în anexa 3.

Acțiuni realizate. Prin organizarea sesiunilor de brainstorming, consultărilor externe și interviurilor este posibilă identificarea noilor controale de securitate, potrivite pentru activele informaționale universitare.

Ieșire. Depozit actualizat cu controale de securitate relevante activelor informaționale universitare.

Criterii de valoare DSR:

- *Eficient,* prin posibilitatea de a fi utilizat în comun de toate IÎS naționale, astfel minimizând decalajul dintre cunoștințele părților interesate responsabile pentru implementarea sistemului de securitate.

3.3. Dezvoltarea instrumentului i-CSSCE

În secțiunile anterioare au fost prezentate etapele de implementare și activitățile-cheie ale CSSCE. Pentru a susține IÎS și a se asigura unificarea eforturilor în implementarea cadrului de securitate a fost dezvoltat un prototip de aplicație, care va permite a selecta opțiunile existente pentru fiecare etapă, iar în final se generează un raport, care va putea fi utilizat pentru evaluarea nivelului de implementare a cadrului de securitate și a observa activitățile pentru care încă nu au fost realizate acțiuni. Instrumentul ar putea fi utilizat simultan de mai mulți utilizatori și IÎS, permite crearea mai multor proiecte, se prezintă ca o platformă de gestiune a serviciilor electronice academice, care ar gestiona aspectele organizaționale și operaționale ale CSSCE prin identificarea activelor bazate pe CE importante, identificarea amenințărilor de securitate și a cerințelor și controalelor de securitate, ce au fost sau sunt necesare de implementat, cu scopul luării deciziilor informate. Obiectivul de bază al i-CSSCE constă în determinarea acțiunilor necesare pentru implementarea unui cadru sistemic de securitate complet și a cerințelor de securitate comune pentru domeniul educațional, ceea ce reprezintă una din prioritățile europene, conform prevederilor Directivei NIS_2.

Instrumentul i-CSSCE poate susține procesul de implementare a activităților propuse de CSSCE, pentru a minimiza efortul necesar activităților de management al securității CE. Acesta a fost conceput ca o aplicație web scrisă în PHP, HTML5, JavaScript și utilizează bazele de date MySQL. Vizualizarea pe partea de client are loc în browser și va putea rula pe orice sistem care suportă PHP, JavaScript și MySQL. Instrumentul este format din mai multe module separate, care vor putea fi utilizate în dependență de drepturile de acces ale utilizatorului. Interfața de utilizator a aplicației este formată din mai multe pagini web conexe, ce pot fi accesate din meniu. Fiecare

pagină este asociată cu anumite activități specifice și interacționează între ele printr-o bază de date axată pe MySQL.

Conform modelului formal Clements–Hoffman, care descrie componentele primare ale unui sistem de securitate, au fost create funcții ce vor permite ulterior gestionarea relațiilor dintre acestea:

```
function set_active_suport(){
$Activul_informational = $_POST["ac"];
$Valoarea_riscului = $_POST["val"];
$Proprietarul = $_POST["prop"];
$Categoria = $_POST["categ"];
$Serviciu_electronic_academic = $_POST["sis"];
global $conn;
$sql = "INSERT INTO `active_de_suport`( `Activul_informational`, `Valoarea_riscului`,
`Proprietarul`, `Categoria`, `Serviciu_electronic_academic`)
VALUES  ($Activul_informational,$Valoarea_riscului,$Proprietarul,$Categoria,
$Serviciu_electronic_academic)";
if ($conn->query($sql) === TRUE) {
  get_active_suport(0);
}
    }
function set_cerinte(){
$Cerinta_de_securitate = $_POST["cerin"];
$Control_de_securitate = $_POST["cer_S"];
$Proprietarul = $_POST["prop"];
$Efect = $_POST["efi"];
$Serviciu_electronic_academic = $_POST["sis"];
$Activul_informational = $_POST["act"];
global $conn;
$sql = "INSERT INTO `main_active_table`( `Cerinta_de_securitate`, `Control_de_securitate`,
`Responsabil`, `Serviciu_electronic_academic`, `Activul`, `Efect`)
VALUES ($Cerinta_de_securitate,$Control_de_securitate,$Proprietarul,
$Serviciu_electronic_academic,$Activul_informational,$Efect)";
if ($conn->query($sql) === TRUE) {
```

```
        get_ceritne_active($Activul_informational);

    }
    else{
        echo "error";
    }
}
function get_amenintari_table($act)
{
    global $conn;
    $sql = "SELECT amenintari.ID, amenintari.ctr_secur, ctrl_sec.controale ,
amenintari.amenintare FROM `amenintari`
            INNER JOIN ctrl_sec ON  amenintari.ctr_secur = ctrl_sec.ID
            where amenintari.Activul = $act";
    $result = $conn->query($sql);
    if ($result->num_rows > 0) {
        while ($row = $result->fetch_assoc()) {
            $val = $row["amenintare"];
            $ID = $row["ID"];
            echo "<tr><td> $val </td></tr>";  } } }
```

Pentru evaluarea cantitativă a fost creat un modul separat care permite a calcula, în baza a 30 de întrebări (anexa 9) generate conform indicatorilor de performanță din tabelul 3.2, gradul de implementare a cadrului de securitate. Funcțiile și apelul la funcții care permit evaluarea cantitativă sunt:

```
export function earnPoints_Number(result, answers, point) {
    return result.map((element, i) => answers[i] === element).filter(i => i).map(i =>
point).reduce((prev, curr) => prev + curr, 0)
}
export function earnPoints_Percent(totalPoints, earnPoints) {
    return (earnPoints * 100 / totalPoints).toFixed(3)
}
const { questions: { queue, answers }, result: { result, userId } } = useSelector(state =>
state)
const totalPoints = queue.length /* Possible earn points */
const earnPoints = earnPoints_Number(result, answers, 1) /* Number of earned points */
```

Modul în care poate fi utilizat instrumentul i-CSSCE pentru managementul securității CE va fi reflectat în continuare printr-un studiu de caz.

3.4. Concluzii la capitolul 3

În acest capitol ne-am referit la descrierea conceptului de securitate a CE, descrierea formală a sistemelor de securitate, pentru a argumenta necesitatea implementării unui cadru sistemic de securitate a CE, și la dezvoltarea CSSCE, având la bază standardele internaționale și cele mai bune practici în domeniu. Abordarea sistemică s-a bazat pe modelul PDCA. CSSCE, fiind un sistem sociotehnic, a fost dezvoltat pe două dimensiuni, și anume, pe dezvoltarea aspectelor organizaționale și operaționale.

Astfel, pot fi trase următoarele concluzii referitor la rezultatelor obținute:

1. Abordarea aspectelor organizaționale ale CSSCE a permis crearea platformei și a premiselor necesare pentru implementarea cadrului de securitate holistic care include:

- *Angajamentul administrației*, fără care nu pot fi inițiate procesele de implementare a conceptului de securitate în cadrul organizației și de alocare a resurselor necesare;
- *Stabilirea contextului,* prin care au fost identificate problemele interne/externe ale instituțiilor academice, a fost descris profilul profesional al specialistului responsabil de securitatea CE și relațiile cu părțile terțe;
- *Determinarea domeniului de aplicare* privind prezentarea arhitecturii de referință constituit din procesul primar educațional academic național și susținut de trei procese secundare la care se referă: serviciile academice comune, infrastructura TIC, sistemul de management universitar;

2. Dezvoltarea CSSCE operațional include 7 etape, care pot fi evaluate prin indicatorii de performanță identificați și justificați, după care poate fi verificată conformitatea, în etapa de planificare a propriului concept de securitate universitară cu prevederile CSSCE. Pentru ca CSSCE să poată fi utilizat ca ghid de implementare au fost înaintate următoarele propuneri originale:

- implementarea politicilor de securitate generale, specifice bazate pe sistem pentru care a fost propus un cadru de dezvoltare, o structură a politicilor de securitate și exemple de implementare pe dispozitivele intermediare de rețea a politicilor de securitate tehnice;

- având la bază serviciile academice electronice prestate de către IÎS naționale, au fost elaborate liste de verificare a activelor de suport clasificate în 5 categorii: echipamente terminale, software, rețea și comunicații, personal și infrastructură;
- au fost determinate următoarele obiective de securitate: confidențialitatea, integritatea și disponibilitatea, stabilită dependența obiectivelor de securitate de sistemul informațional academic. Totodată, pentru fiecare proces secundar identificat a fost creată dependența de unul sau mai multe dintre obiectivele enumerate;
- a fost elaborată lista de verificare a amenințărilor generice și specifice mediului universitar pentru fiecare tip de activ de suport universitar, conform următoarelor categorii: echipamente terminale (pc desktop, laptop etc.), software (server Web, server DNS, sisteme de operare bazate pe rețea, sisteme de stocare centralizată etc.), rețea și comunicații (switch, ruter etc.), personal (angajați, studenți ș.a.) și infrastructură (centru de date, UPS, clădire etc.). Drept contribuție originală a fost determinat, pentru fiecare amenințare generică de securitate, principiul de securitate pe care îl încalcă: confidențialitatea, integritatea sau disponibilitatea;
- a fost propusă o metodă de evaluare a riscului de securitate, determinate criteriile de evaluare a impactului (drept exemplu au servit atacurile DoS/DDoS asupra rețelelor de CE) și propusă o metodă de evaluare a riscului cibernetic prin prisma relațiilor dependente dintre activele de suport; au fost propuse modele pentru Registrul riscurilor de securitate, Planul de tratare a riscurilor și Declarația de aplicabilitate pentru a facilita procesul de conformitate cu ISO 27001;
- CSSCE este modular; a fost propus un mod de prioritizare a cerințelor de securitate și prezentate câteva exemple reale de implementare a controalelor de securitate pentru nivelurile 2, 3 și 4 ale modelului OSI;
- a fost creat și completat depozitul controalelor de securitate care va putea fi utilizat în comun de IÎS.

3. A fost dezvoltat instrumentul i-CSSCE, care permite a gestiona și a evalua nivelul de implementare a cadrului de securitate atât în aspectele organizaționale, cât și operaționale.

4. EVALUAREA CADRULUI SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE

Deși metoda DSR are șase etape, pentru care au fost identificate activități relevante în capitolul 2, două activități totuși pot fi apreciate ca având o importanță majoră: dezvoltarea și evaluarea cadrelor [116, 122]. Rezultatul aplicării metodei DSR sunt cunoștințele prescriptive sub formă de artefacte IT și recomandări [122]. Cunoștințele prescriptive sunt definite de cercetători ca descrierea și recomandarea anumitor sarcini concrete, care derivă din studiul științific și empiric [227]. Cunoștințele prescriptive acumulate în urma procesului de dezvoltare a cadrului sistemic de securitate nu au nicio valoare [228], ceea ce duce la imposibilitatea de a demonstra că sistemul obținut va soluționa problema practică identificată, dacă cadrul nu a fost evaluat. Scopul oricărui proces DSR este să rezolve probleme practice [107, 122]. Afirmațiile care descriu cunoștințele prescriptive obținute prin metoda DSR rezumă la demonstrarea utilității cadrului în mediul pentru care a fost proiectat [122]. Evaluarea cadrului ar trebui să demonstreze că acesta este aplicabil în practică. Confirmarea și validarea cadrului obținut, în urma aplicării proceselor DSR, se realizează prin evaluare înainte ca acesta să fie implementat în practică [122].

Astfel, s-a decis ca evaluarea CSSCE să se realizeze în mediul natural [229] prin consultarea experților în domeniu, selectați din diferite medii: academic, industrial, guvernamental, din organizațiile naționale și internaționale și a părților interesate din IÎS, Republica Moldova, contribuind astfel la acuratețea cunoștințelor prescriptive [229] ale CSSCE, și printr-un studiu de caz care va demonstra aplicabilitatea acestuia.

4.1. Studiu de caz

După analiza domeniului de aplicare a fost selectată RCE, care interconectează laboratoarele Facultății Electronică și Telecomunicații, UTM, pentru a reflecta posibilitatea de implementare a sistemului de securitate prin cele 7 etape de operaționalizare a CSSCE. Laboratoarele de studii fac parte din procesul educațional academic Infrastructură TIC. Meta-modelul care include structura ierarhică redundantă a RCE, ce asigură accesul la Internet pentru laboratoarele de studii, este reflectat în figura 4.1, care are dispozitive intermediare de rețea per fiecare strat: acces, agregare și de bază.

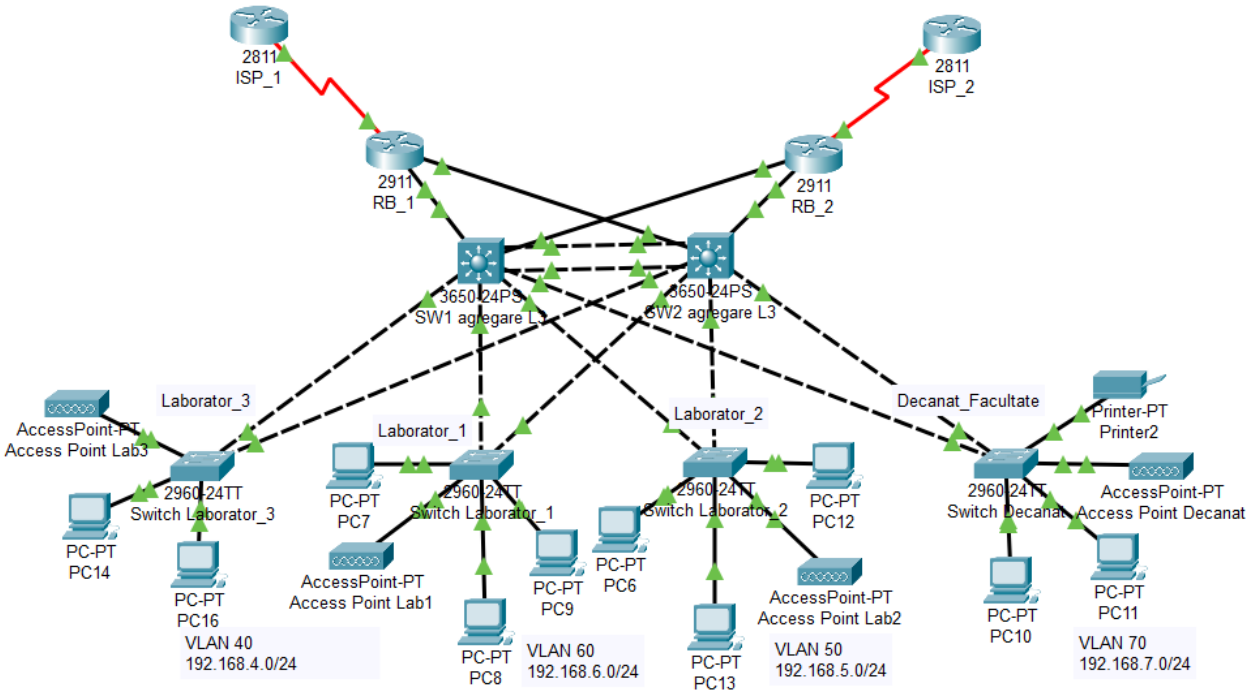

Fig. 4.1. Meta-model infrastructură RCE redundantă,
Facultatea Electronică și Telecomunicații, UTM (elaborat de autor)

Prototipul instrumentului i-CSSCE care a fost dezvoltat permite a crea proiecte noi, în dependență de necesitățile utilizatorului (figura 4.2); în cazul dat se va face referință la laboratoarele cu echipament specializat.

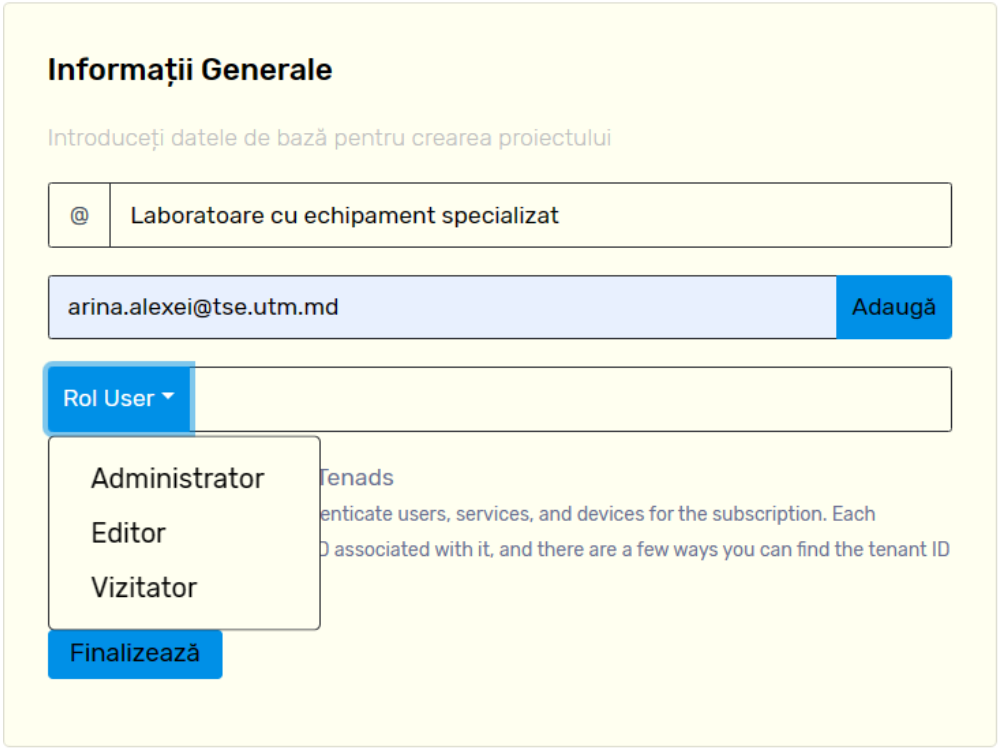

Fig. 4.2. Crearea proiectului

La fiecare proiect pot avea acces mai mulți utilizatori, care vor deține autorizații diferite în dependență de rolul pe care îl au (figura 4.3).

Fig. 4.3. Roluri predefinite pentru utilizatori

Ulterior pot fi adăugate informațiile necesare care se referă la serviciul electronic academic, la categoria active de suport, la active de suport, la cerințele și controalele de securitate relevante (figura 4.4).

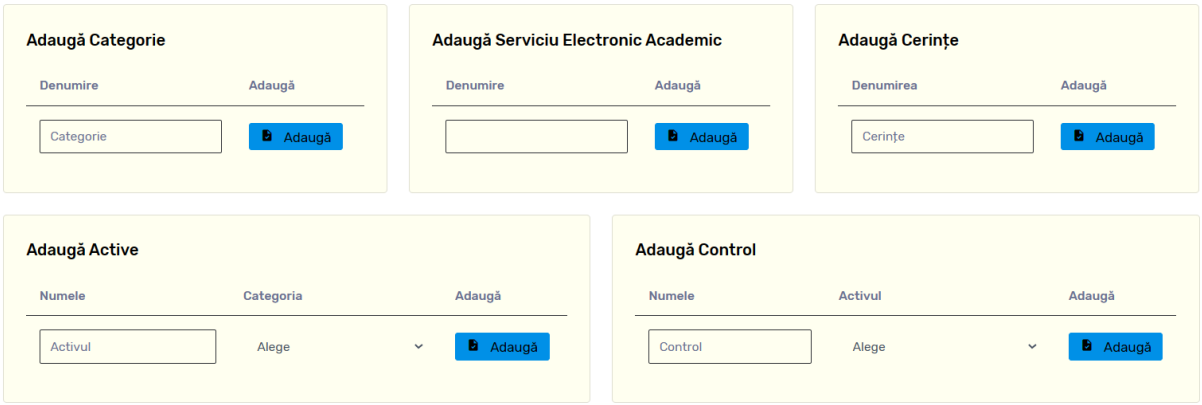

Fig. 4.4. Completarea proiectului

Etapa 1. Elaborarea politicilor de securitate specifice

Fluxul de lucru pentru această activitate a fost descris în subcapitolul 3.2, utilizat ca ghid de implementare în mediul studiat. Astfel, a fost elaborată politica specifică de securitate pentru laboratoarele facultății, ce poate fi utilizată pentru orice medii de laborator, deoarece se referă la utilizarea acceptabilă a dispozitivelor terminale universitare, care reprezintă un risc sporit pentru

RCE și sunt utilizate în comun de diverși utilizatori, cu nivel de educare aferent securității greu de estimat.

Intrare:

- cadrul generic pentru dezvoltarea politicilor de securitate în IÎS;
- structura politicii de securitate.

Acțiuni realizate: interviuri cu inginerii responsabili de laboratoarele facultății, sesiunile de brainstorming cu administrația facultății și analiza domeniului de aplicare reflectat în figura 4.1.

Fig. 4.5. Adăugare politici de securitate

Ieșire: politica de utilizare acceptabilă a dispozitivelor universitare (anexa 6).

Etapa 2. Identificarea activelor bazate pe CE importante

Scopul acestei etape este de a identifica activele importante pentru procesul educațional academic analizat, necesare pentru funcționarea securizată a laboratoarelor de studii.

Intrare:

- lista de verificare a activelor de suport (anexa 2);
- infrastructura RCE a laboratoarelor de studii.

Acțiuni realizate: interviuri, chestionare, discuții cu inginerii responsabili de RCE universitare, ședințe cu administrația facultății.

Ieșire: după analiza infrastructurii RCE a Facultății Electronică și Telecomunicații, activele de suport corespunzătoare au fost atribuite procesului secundar academic.

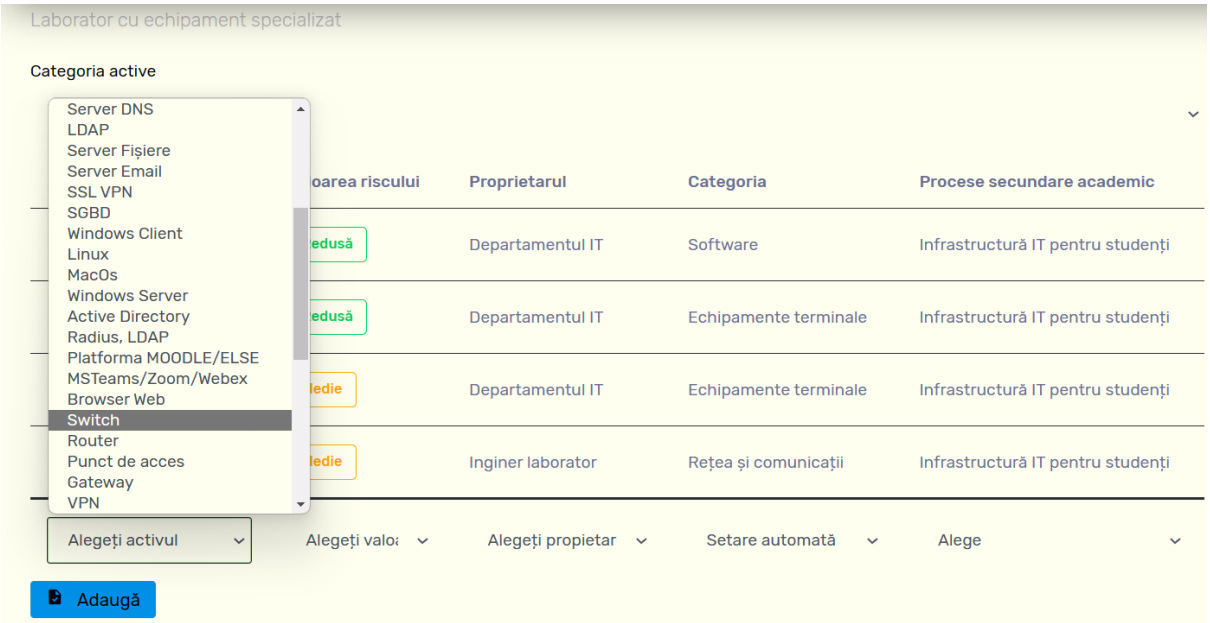

Fig. 4.6. Adăugare active de suport

Etapa 3. Identificarea obiectivelor de securitate și dependența de sistem

În această etapă este necesar a identifica obiectivele de securitate pentru laboratoarele de studii. Obiectivele de securitate pentru întreg procesul educațional academic au fost identificate în subcapitolul 3.2.

Intrare:

- dependența obiectivelor de securitate de sistemul universitar;
- lista activelor de suport în etapa 2.

Acțiuni realizate: sesiuni de brainstorming și analiza cerințelor.

Ieșire: lista obiectivelor de securitate.

	Active primare	Confidențialitatea	Integritatea	Disponibilitatea
☐	Laboratoare cu Echipament Specializat	DA	NU	DA
☐	Aplicații pentru Video Conferință	NU	NU	DA
☐	Platforme de învățare online	DA	DA	DA

Fig. 4.7. Dependența față de obiectivele de securitate

Etapa 4. Identificarea amenințărilor de securitate

Pentru ca ulterior să poată fi selectate cerințe de securitate relevante și eficiente, este necesar a identifica amenințările specifice și generice pentru activele de suport identificate în etapa 2.

Intrare:

- lista de verificare a amenințărilor generice și specifice de securitate (anexa 3);
- lista activelor de suport în etapa 2.

Acțiuni realizate: interviuri, sesiuni de brainstorming, teste de penetrare, analiza jurnalelor de sistem.

Ieșire: lista amenințărilor generice și specifice pentru fiecare activ de suport al laboratoarelor de studii, cum pot fi acestea vizualizate și după caz adăugate în depozit este reprezentat în figura 4.8.

Fig. 4.8. Amenințări de securitate

Etapa 5. Evaluarea riscului cibernetic

Modelul propus pentru evaluarea riscului cibernetic aferent activelor universitare a fost utilizat pentru a calcula valoarea dependentă a activelor de suport din laboratoarele Facultății Electronică și Telecomunicații. Această activitate va permite a identifica care dintre activele de suport analizate reprezintă risc cibernetic cu o valoare mai înaltă, a cărui impact este semnificativ și necesită revizuirea periodică a cerințelor de securitate.

Intrare:

- lista amenințărilor generice și specifice pentru fiecare activ de suport al laboratoarelor de studii;
- lista activelor de suport în etapa 2.

Acțiuni realizate: sesiuni de analiză și brainstorming cu inginerul din cadrul laboratorului și Direcției TIC.

Ieșire: valoarea activelor de suport, reflectată în figura 4.9.

Laboratoare Cu Echipament Specializat

#	Activului	Valoarea	Cerințe implementate	Termen realizare
1	Desktop PC	Redusă	8	Sep 15, 2023
2	Switch Acces	Medie	6	Sep 15, 2023
3	Switch Agregare	Sporită	2	Oct 12, 2023
4	Router De Bază	Sporită	2	Oct 12, 2023
5	WLAN Utilizare	Sporită	2	Oct 12, 2023

Adaugă active de suport

Fig. 4.9. Valoarea calitativă a activelor de suport (elaborat de autor)

Astfel, prin studiul de caz prezentat care poate servi drept exemplu, se pot identifica activele bazate pe CE cu valoare sporită, pentru care ulterior se vor identifica cerințele de securitate implementate, dar și cerințele de securitate ce trebuie luate în calcul. Important este să se facă o analiză cost–beneficiu [91], înainte de implementarea cerințelor de securitate costisitoare [168].

Etapa 6. Identificarea cerințelor de securitate

La baza identificării cerințelor de securitate stau rezultatele (ieșirile) din fiecare dintre cele 5 etape descrise mai sus astfel, încât cerințele de securitate propuse să ia în calcul politicile de securitate, activele de suport, obiectivele de securitate, amenințările generice și specifice și valoarea riscului cibernetic calculat.

Intrare:

- politica de utilizare acceptabilă a dispozitivelor universitare (anexa 6);
- lista activelor de suport ale laboratoarelor de studii;
- lista obiectivelor de securitate;
- Lista amenințărilor generice și specifice pentru fiecare activ de suport al laboratoarelor de studii (anexa 3);
- valoarea activelor de suport.

Acțiuni realizate: sesiuni de brainstorming între inginerii din cadrul laboratoarelor de studii și Direcției TIC, Departamentului Resurse Umane și Serviciului Deservire blocuri; consultări externe, interviuri cu specialiștii din alte instituții universitare.

Ieșire: lista cerințelor de securitate pentru activele de suport ale laboratoarelor de studii.

Se propune ca pentru activele cu o valoare a riscului redusă și medie să fie implementate cerințele de securitate de bază, exemplu fiind dat în figurile 4.10 și 4.11.

Desktop PC

Statut	Cerința de securitate	Control de securitate	Eficacitate	Responsabil
	Protejarea procesului de boot	Documentarea configurărilor dispozitivelor de rețea	Efec	Departamentul IT
	Activarea mecanismelor de actualizare automată	Documentarea configurărilor dispozitivelor de rețea	Efec	Ingineri laborator
	Activarea mecanismelor de actualizare automată	Documentarea configurărilor dispozitivelor de rețea	Non	Departamentul IT
	Activarea mecanismelor de actualizare automată	Documentarea configurărilor dispozitivelor de rețea	Efec	Ingineri laborator
	Regulamentul de instalare și configurare software	Documentarea configurărilor dispozitivelor de rețea	Efec	Ingineri laborator
	Autorizare sigură a utilizatorului	Stocarea securizată a parolelor de acces	Efec	Ingineri laborator

Fig. 4.10. Cerințe de securitate privind activele de suport cu risc redus

Switch Acces

Statut	Cerința de securitate	Control de securitate	Eficacitate	Responsabil
	Crearea listei de verificare a configurației pentru routere și comutatoare	Documentarea configurărilor dispozitivelor de rețea	Efec	Direcția TIC
	Protecție împotriva utilizării greșite a mesajelor ICMP	Stocarea securizată a parolelor de acces	Efec	Direcția TIC
	Crearea listei de verificare a configurației pentru routere și comutatoare	Stocarea securizată a parolelor de acces	Efec	Direcția TIC
	Administrare folosind o rețea de management separată	Stocarea securizată a parolelor de acces	Efec	Direcția TIC
	Administrare folosind o rețea de management separată	Stocarea securizată a parolelor de acces	Efec	Direcția TIC
	Administrare folosind o rețea de management separată	Stocarea securizată a parolelor de acces	Efec	Direcția TIC

Fig. 4.11. Cerințe de securitate privind activele de suport cu risc mediu

Se propune ca pentru activele cu risc sporit de securitate să fie implementate prioritar cerințe de securitate ce asigură protecția de bază și ulterior, dacă este necesar cerințele de securitate ce asigură protecția standard (figura 4.12).

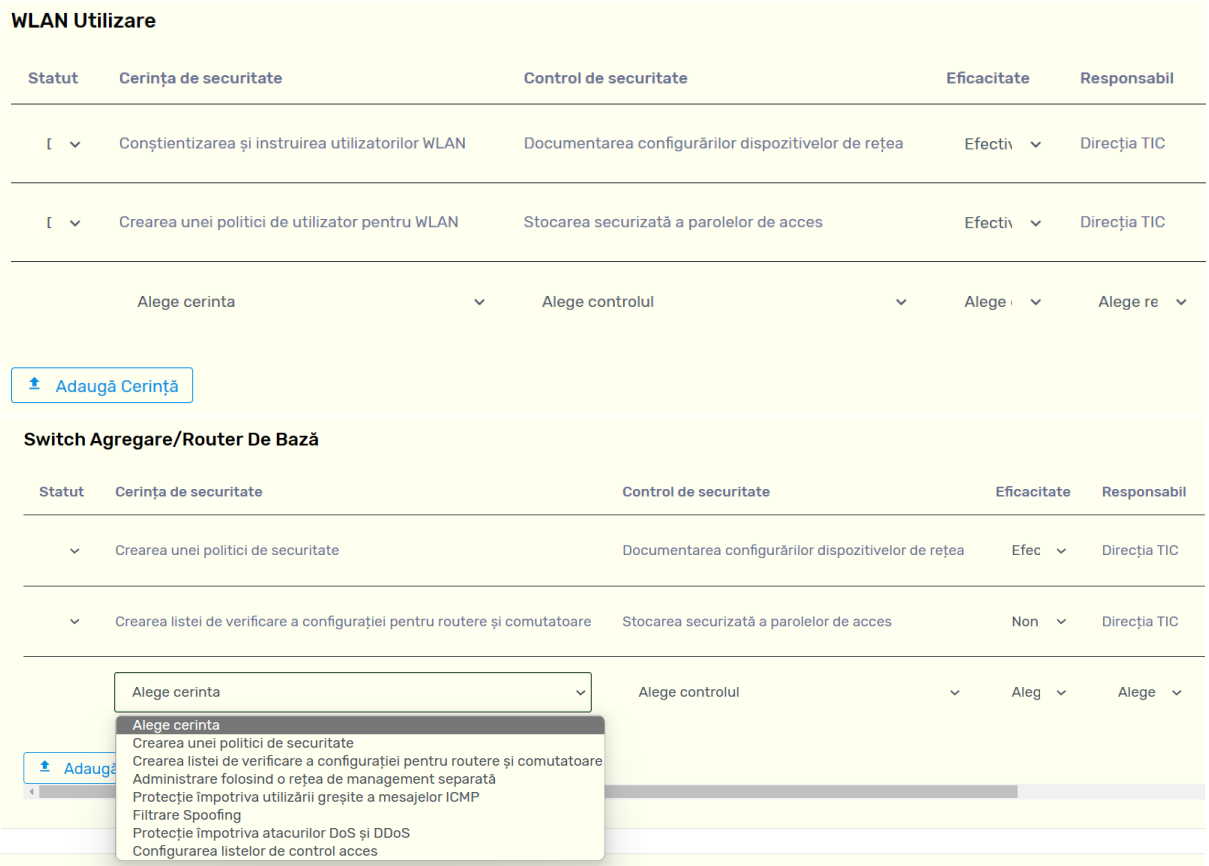

Fig. 4.12. Cerințe de securitate privind activele de suport cu risc sporit

Etapa 7. Completarea depozitului cu controale de securitate relevante

În ultima etapă se completează depozitul central de cerințe de securitate care lipsesc. Se face o analiză și se actualizează cerințele existente prin eliminarea cerințelor de securitate ineficiente sau dificil de implementat și se calculează costurile de implementare pentru fiecare cerință de securitate.

Intrare: depozitul cerințelor de securitate (anexa 8).

Acțiuni realizate: sesiuni de brainstorming, consultări externe, interviuri cu părțile interesate din universitățile naționale.

Ieșire: cepozit actualizat cu cerințe și controale de securitate.

Fig. 4.13. Depozit cerințe de securitate

În modulul adăugat pentru a evalua cantitativ nivelul de implementare a CSSCE se poate observa procentajul înregistrat de instituție în baza a 30 de întrebări (anexa 9).

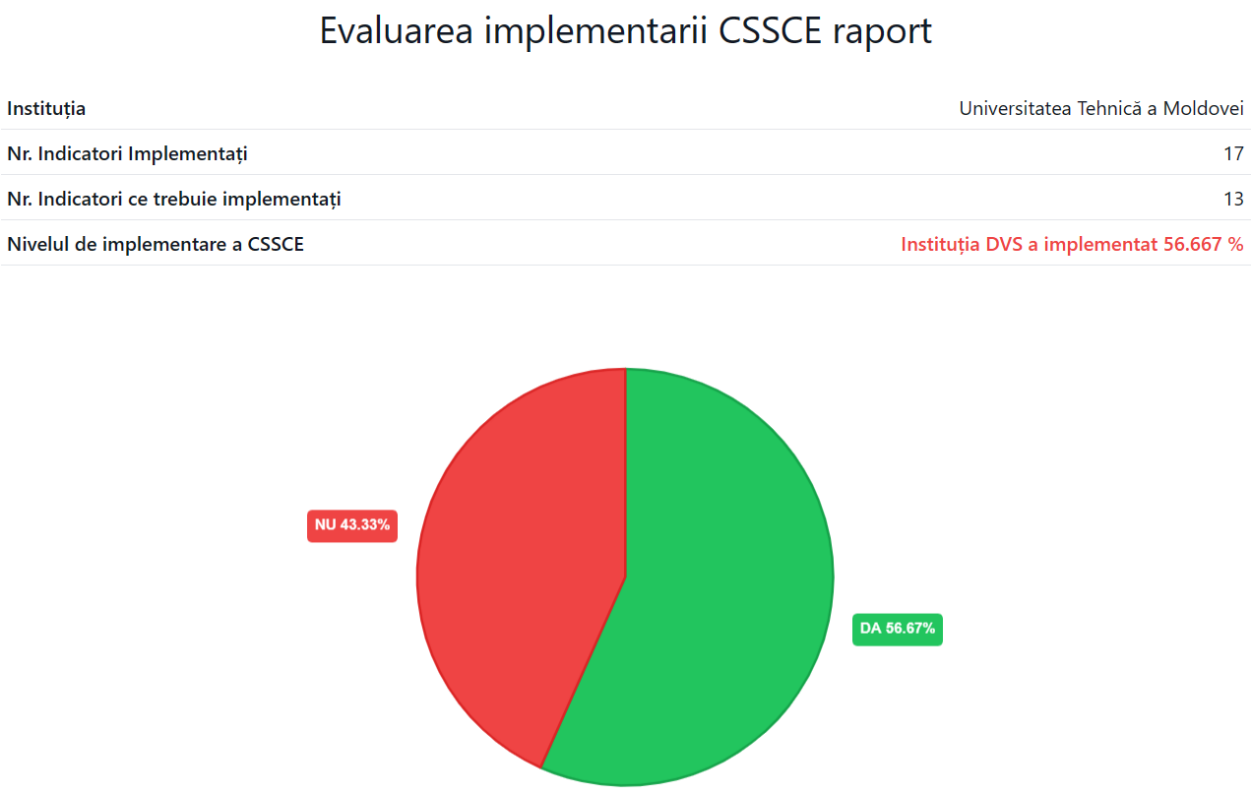

Fig. 4.14. Raport evaluare implementare CSSCE

4.2. Utilizarea metodei Delphi pentru evaluarea prototipului CSSCE

Metoda Delphi este o procedură de cercetare metodică și interactivă prin care se încearcă obținerea avizelor de la experții independenți cu privire la un anumit subiect de studiu [15]. Avizele experților sunt utilizate ca suport pentru adoptarea deciziilor [230] și pentru evaluarea rezultatelor cercetării. În limitele acestei lucrări de cercetare, avizele experților au contribuit la evaluarea prototipului CSSCE, ținând cont de criteriilor de valoare, pentru a înțelege cât de bine prototipul CSSCE satisface criteriile în baza cărora a fost dezvoltat.

Caracteristicile generice ale metodei Delphi sunt: selectarea experților, crearea unui panel (metodă de investigație repetitivă pentru urmărirea evoluției unui fenomen prin solicitări de informații, de la aceleași grupuri de persoane), anonimitatea participanților, iterații și feedback (conexiune inversă) [15].

Experții selectați, potriviți pentru studiul Delphi, trebuiau să fie specialiști în domeniul TIC, securității cibernetice/informației sau domenii conexe, capabili să vadă conexiuni între dezvoltarea națională și internațională, să aibă cunoștințe tehnice și manageriale, să fie capabili a lua în considerație diferite opinii, deseori chiar neconvenționale, pentru a reuși să creeze ceva inovativ [231] și eterogen, precum recomandă anumite lucrări științifice [232]. Cei 15 experți selectați pentru acest studiu fac parte din mediul academic, al industriei și guvernamental, activând în organizații naționale și internaționale. Pentru a participa la acest studiu, experții au fost contactați prin email.

Domeniile de expertiză ale experților selectați pentru Panelul 1 sunt: Implementarea standardelor de securitate informațională (26,7%), Administrarea RCE (33,3%), Elaborarea politicilor și a strategiilor de securitate informațională (26,7%), Ofițer de Securitate Informațională (6,7%), Expert în cadrul Organizațiilor guvernamentale (6,7%), Manager proiecte (46,7%), Cercetător din mediul academic (40%), Inginer date și administrarea datelor și sistemelor (6,7%), Asigurarea calității serviciilor și managementul serviciilor Telco și IT (6,7%), Manager tehnic în domeniul infrastructurii TI (6,7%), Inginer fiabilitate site-uri (6,7%). Întrebarea care s-a referit la domeniul de expertiză a fost non-exclusivă, de aceea rezultatele nu se raportează sută la sută; respondenții au putut selecta unul sau mai multe domenii de expertiză. Organizațiile din care fac parte experții sunt: Endava, I.M. "Orange Moldova" SA, SOFTCOM, RM, Huawei Technologies Co., Ltd., ITGroup & Services SRL, Agenția Servicii Publice, Institutul de Dezvoltare a Societății Informaționale, Capitol Canary Inc, Huawei Technologies Deutschland, San Jose State University, Universitatea de Stat Moldova, ULIM, STI al MAI. Experții au o vastă experiență: de peste 10 ani (66,7%), între 5-10 ani (26,7%) și 1-5 ani (6,7%).

Pentru Panelul 2, format din specialiști responsabili din cadrul IÎS pentru securitatea CE sau specialiști din direcțiile TIC inițiați în domeniu, au fost recrutate 9 persoane. Metoda Delphi recomandă grupuri de 10-30 participanți [233, 234]. Însă în anumite cazuri, panelul poate fi creat dintr-un număr mai mic [15], atunci când există anumite limitări, cum ar fi, de exemplu, numărul mic de IÎS din RM. La sondaj au participat specialiști din următoarele IÎS: UTM, UPSC, USMF, ASEM, UASM, ULIM, USARB.

Imediat ce au fost recrutați, participanții la studiul Delphi au primit prin e-mail documentul *Consimțământ informat, Capitolul 3* din teza de doctor și *articolul științific* care reflectă întregul parcurs al cercetării [196]. În baza materialelor de suport, au fost rugați să completeze chestionarul, dând aviz fiecărui criteriu de valoare, din cele 7 identificate în capitolul 2, pentru a evalua cum satisfce CSSCE fiecare criteriu. Chestionarul a fost creat cu instrumentul Google Formulare, des utilizat în cercetările științifice [235], deoarece este ușor de aplicat și gratuit.

Participanților le-a fost garantat anonimatul, aceasta fiind o condiție obligatorie a metodei Delphi. Experții au primit câte un ID de identificare de la ID1–ID15 pentru Panelul 1 și de la IDS1–IDS9 pentru Panelul 2. Această caracteristică susține ideile expertului, indiferent de statutul lui, fără a influența alți experți și fără a avea frică de a face declarații publice nepotrivite [231]. Acest aspect garantează răspunsuri și rezultate mai obiective [15].

Întrebările din chestionar, după care a fost evaluat prototipul CSSCE, sunt următoarele: ”Este prototipul CSSCE aplicabil în instituțiile de învățământ superior?”, ”Sunt identificate fazele de implementare a prototipului CSSCE în mediul universitar?”, ”Este descris profilul specialistului responsabil de securitate?”, ”Prototipul CSSCE recomandă modalitatea prin care managementul riscului poate fi realizată într-o instituție academică?”, ”Puteți aprecia prototipul CSSCE ca fiind eficient și că poate contribui la îmbunătățirea securității CE a universităților din RM?”, ”Este prototipul CSSCE scalabil, poate fi aplicat în orice instituție academică, indiferent de dimensiunea sau complexitatea serviciilor electronice?”, ”În ce măsură prototipul CSSCE se conformează standardelor din domeniul securității informaționale pe dimensiunile acoperite?”.

Pentru înregistrarea calificativelor date de participanți a fost utilizată scara Likert, care permite a înregistra nivelul de acord/dezacord al participanților la sondaj, cu o anumită afirmație [236]. Varianta clasică a scării Likert utilizează 5 sau 7 calificative [236]. În acest studiu, a fost utilizată varianta cu 5 calificative: „total de acord”, „de acord”, „neutru”, „dezacord” și „dezacord total”. Astfel, pentru confirmarea CSSCE, a fost nevoie ca valoarea criteriilor să se încadreze între „total de acord” și „de acord”, pe scara Likert. Participanții la sondaj, care au înregistrat rezultate egale sau mai mici de calificativul 3, au fost contactați suplimentar prin e-mail, li s-au transmis materiale de suport suplimentare sau argumente, după care și-au reevaluat aprecierea dată. Aceasta

reprezintă una dintre proprietățile tehnicii Delphi, prin care se sugerează mai multe iterații, până ce nu se ajunge la consens cu experții. Pentru procesarea rezultatelor sondajului, fiecărui calificativ i se atribuie o valoare numerică, un exemplu în acest sens fiind inclus în tabelul 4.1.

Tabelul 4.1. Calificative scară Likert

Calificativul	Valoarea numerică
Dezacord total	**1**
Dezacord	**2**
Neutru	**3**
De acord	**4**
Total de acord	**5**

Criteriile de evaluare și calificativele disponibile pot fi consultate în anexa 4.

Procesarea statistică a fost utilizată pentru a prezenta rezultatele chestionarului, aceasta fiind metoda ce se potrivește cel mai bine pentru a prezenta rezultate științifice [230]. Statistica descriptivă a fost utilizată pentru a identifica nivelul de consens între respondenții la sondaj [230] în baza unei analize subiective; au fost utilizați următorii indicatori statistici: media și deviația standard. Statistica inferențială a fost utilizată pentru a identifica consensul în evaluarea CSSCE dintre experții în domeniu și părțile interesate din IÎS, a fost utilizată metoda Kendall's W [16]. Pentru procesarea statistică a rezultatelor sondajului a fost utilizat instrumentul SPSS, produs de IBM, versiunea trial, datorită faptului că este unul dintre cele mai complete instrumente software pentru interpretarea datelor statistice și este actualizat periodic [175].

4.2.1. Aplicarea statisticii descriptive

Statistica descriptivă a fost utilizată cu scopul prelucrării de bază a rezultatelor rundelor Delphi, deoarece reprezintă baza analizei cantitative și pentru a generaliza rezultatele sondajului [230]. Statisticile descriptive calculează în ce măsură datele observate se grupează în jurul unei valori [230]. După cum s-s menționat, la prezentarea rezultatelor rundelor Delphi, realizate pentru evaluarea CSSCE, au fost aplicați indicatorii statistici media și deviația standard, pentru a determina distribuția datelor în sondaj.

Media reprezintă măsurarea tendinței centrale și se referă la valoarea medie a unui grup [174]. În acest caz, media va reflecta tendința centrală [237] din ambele panele ale studiului Delphi, pentru a satisface criteriile de valoare. A fost calculată după formula:

$$\bar{x} = \frac{\sum x}{n}, \tag{4.1}$$

unde: x – este fiecare răspuns înregistrat;

n – este numărul de respondenți la sondaj.

Deviația standard oferă o perspectivă asupra nivelului de variație existente într-un grup de valori [174]. Se măsoară abaterea (diferența) de la media grupului analizat. Formula după care va fi calculată deviația standard [237] este următoarea:

$$\sigma=\sqrt{\frac{\Sigma(X_i-X)^2}{N}}, \tag{4.2}$$

unde: σ - deviația standard;

X - media;

X_i - respondentul i din panelul Delphi;

N - numărul total de respondenți.

Datele inițiale ale sondajului au fost introduse în Editorul de date statistice ale instrumentului IBM SPSS și au fost obținute rezultatele ce pot fi analizate din tabelul 4.2.

Tabelul 4.2. Rezultatele statisticii descriptive (elaborat de autor)

Nr. d/o	Criterii de evaluare a prototipului CSSCE	N	Minimum	Maximum	Media	Deviația standard
1	Este prototipul CSSCE aplicabil în instituțiile de învățământ superior?	24	4,00	5,00	4,6667	,48154
2	Sunt identificate fazele de implementare a prototipului CSSCE în mediul universitar?	24	4,00	5,00	4,5417	,50898
3	Este descris profilul specialistului responsabil de securitate CE?	24	4,00	5,00	4,5000	,51075
4	Prototipul CSSCE recomandă modalitatea prin care managementul riscului poate fi realizat într-o instituție academică?	24	4,00	5,00	4,6250	,49454
5	Puteți aprecia prototipul CSSCE ca fiind eficient și că poate contribui la îmbunătățirea securității CE a universităților din RM?	24	4,00	5,00	4,7500	,44233
6	Este prototipul CSSCE scalabil, poate fi aplicat în orice instituție academică, indiferent de dimensiunea sau complexitatea serviciilor electronice?	24	4,00	5,00	4,5000	,51075
7	Se conformează prototipul CSSCE standardelor din domeniul securității informaționale pe dimensiunile acoperite?	24	4,00	5,00	4,5833	,50361
	Valid N	24				

Pornind de la datele incluse în tabelul 4.2, putem afirma că participanții la studiul Delphi au apreciat prin *Acord* și *Acord total* satisfacerea criteriilor de valoare ale prototipului CSSCE după media înregistrată, iar răspunsurile date au fost destul de dispersate. rezultate în baza cărora prototipul CSSCE poate fi confirmat în etapa post-dezvoltare și poate fi recomandat pentru implementare în IÎS din RM.

4.2.2. Aplicarea statisticii inferențiale

Statistica inferențială prezintă calcule complexe, metode matematice care utilizează teoria probabilității [238], cu scopul de a face inferențe între rezultatele sondajului, adică între datele observate și deducții ce nu pot fi identificate prin analiza simplă a datelor [239]. Statistica inferențială utilizează teste parametrice și non-parametrice pentru a face generalizări. Testele parametrice sunt utilizate în cazurile în care informațiile despre eșantion sunt cunoscute [238], iar testele neparametrice sunt similare cu cele parametrice, însă media eșantionului nu mai constituie un element foarte important [240].

Coeficientul de concordanță, numit W al lui Kendall [241], reprezintă un test neparametric al statisticii inferențiale, utilizat pentru a măsura acordul dintre evaluatorii sondajului, care oferă calificative [230] rezultatelor științifice obținute. Pentru a îndeplini scopul etapei de evaluare a prototipului CSSCE a fost utilizat W al lui Kendall, pentru a compara rezultatele Panelului 1, format din experți în domeniu, cu rezultatele Panelului 2, format din părțile interesate din cadrul IÎS, pentru a calcula în ce măsură de conformitate respondenții la sondaj au apreciat CSSCE [241]. Cu cât va fi mai mare coeficientul W al lui Kendall, cu atât consensul va fi mai apropiat de valoarea 1 [230], ceea ce înseamnă că respondenții ambelor panele au evaluat sondajul în mod similar. Astfel, evaluarea CSSCE nu a înregistrat aprecieri contrare, acordul de rang al răspunsurilor fiind asemănător [230], iar rezultatele pot fi considerate valide. Formulele după care este calculat W al lui Kendall [242, 243] sunt:

$$R_i - \sum_{j=1}^{m} r_{ij}, \tag{4.3}$$

unde: i – criteriul de evaluare;

m – numărul de panele Delphi care evaluează *n* criterii.

$$R - m(n+1)/2, \tag{4.4}$$

$$S - \sum_{i=1}^{n} (R_i - R)^2, \tag{4.5}$$

unde: S – abaterea statistică a sumei pătratelor rândurilor cumulate ale rangurilor R_i;

R – media valorilor lui R_i.

Valoarea coeficientului de concordanță al lui Kendall ia valori cuprinse între 0 și 1, putând fi calculată după următoarea formulă:

$$W = \frac{12S}{m^2(n^3-n)}, \quad (4.6)$$

unde: W – coeficientul de concordanță;

n – numărul obiectelor evaluate, în cazul dat, criteriile de valoare ale CSSCE;

m – numărul de evaluatori participanți la studiul Delphi;

$m^2(n^2-n)/12$ – maximum posibil al valorii lui S, în cazul în care există unanimitate totală între respondenții la sondaj.

Rezultatele aplicării acestei metode statistice va determina gradul de concordanță dintre valoarea medie a calificativelor obținute pentru fiecare criteriu de valoare înregistrat de Panelul 1 și Panelul 2. Gradul de concordanță al W al lui Kendall poate fi analizat din tabelul 4.3.

Tabelul 4.3. Interpretarea rezultatelor (adaptat după [193])

W al lui Kendall	Interpretarea rezultatelor
0	Dezacord
0.10	Acord slab
0.30	Acord moderat
0.60	Acord puternic
1	Acord perfect

Datele obținute incluse în tabelul 4.2 cu referire la valorile înregistrate pentru media aritmetică au fost introduse în Editorul de date statistice ale instrumentului IBM SPSS. Au fost supuse analizei statistice două seturi de date pentru Panelul 1 (experți) și pentru Panelul 2 (specialiști IÎS). Rezultatele obținute pot fi analizate din tabelul 4.4.

Tabelul 4.4. Ranguri obținute (elaborat de autor)

Nr. d/o	Criterii de evaluare a prototipului CSSCE	Rangul mediu
1	Este prototipul CSSCE aplicabil în instituțiile de învățământ superior?	5,50
2	Sunt identificate fazele de implementare a prototipului CSSCE în mediul universitar?	2,50
3	Este descris profilul specialistului responsabil de securitate CE?	2,25
4	Prototipul CSSCE recomandă modalitatea prin care managementul riscului poate fi realizată într-o instituție academică?	4,25
5	Puteți aprecia prototipul CSSCE ca fiind eficient și că poate contribui la îmbunătățirea securității CE a universităților din RM?	7,00
6	Este prototipul CSSCE scalabil, poate fi aplicat în orice instituție academică, indiferent de dimensiunea sau complexitatea serviciilor?	2,25
7	Se conformează prototipul CSSCE standardelor din domeniul securității informaționale pe dimensiunile acoperite?	4,25

În baza rezultatelor din tabelul 4.4, valoarea coeficientului **W al lui Kendall = 0,752,** ceea ce indică, conform interpretării datelor prezentate în tabelul 4.3, un acord puternic între cele 2

panele ale studiului Delphi. Aprecierile experților din Panelul 1 sunt în acord puternic cu aprecierile specialiștilor din cadrul IÎS, care au participat la Panelul 2, ceea ce confirmă o dată în plus că prototipul CSSCE satisface toate criteriile de valoare după care a fost proiectat și ulterior dezvoltat.

4.3. Evaluarea calitativă a prototipului CSSCE

Sondajul a inclus, pe lângă întrebările aferente domeniului de expertiză, stagiul de muncă și cele 7 întrebări pentru evaluarea prototipului CSSCE, o secțiune în care participanții erau rugați să prezinte recomandări și sugestii pentru îmbunătățirea prototipului CSSCE.

Sugestiile experților au permis a perfecta prototipul CSSCE, iar modificări relevante au fost efectuate în secțiunile capitolului 3: *Domeniul de aplicare, Politici de securitate* și *Evaluarea riscului cibernetic*.

Recomandările înregistrate de experți au fost următoarele:

- ID4: ”*M-aș bucura mult ca sistemul de învățământ de stat, împreună cu alte sisteme, să aibă un astfel de framework implementat cap–coadă și menținut în timp!*”;
- ID6: ”*Abordarea securității cibernetice din universități ca sistem interdependent și stabilirea clară a etapelor de implementare a framework-ului, descrierea cerințelor de securitate va avea un impact important asupra tuturor universitățile din țară”*;
- ID9: ”*Crearea conceptului de securitate informațională în cadrul instituțiilor de învățământ din RM va ridica nivelul de securitate al serviciilor acordate, va crea un cadru comun și prognozabil în domeniul securității informaționale a procesului de învățământ și activităților aferente* ”;
- ID12: ”*Se recomandă a implementa în toate instituțiile de învățământ superior*”;
- ID13: ”*CSSCE oferă o resursă importantă pentru organizarea securității informaționale în instituțiile de învățământ superior. În același timp, prin sinergia standardelor din domeniu, se pot economisi resurse*”.

În plus, rezultatele cercetării au fost expediate la doi profesori din Germania de la care s-a solicitat feedback.

Profesorul Wolfgang Hommel de la Universität der Bundeswehr München, fost Ofițer-șef de securitate informațională la Centrul de supercomputere din Leibniz, a oferit următorul feedback: *”Îmi place abordarea generală pe care o luați în cercetarea dvs. și sper că aceasta va duce și la progrese practice”.*

Dr. Robert Müller-Török, profesor de e-Guvernare și reprezentant al Strategiei UE pentru regiunea Dunării, membru al Consiliului de Administrație al Societății Austriece de Calculatoare,

conferențiar la Universitatea de Administrație Publică și Finanțe Ludwigsburg, a apreciat astfel prototipul CSSCE: ”*Este un ghid complet, care poate fi folosit ca un cadru de referință de către orice universitate din Republica Moldova*”.

4.4. Analiza comparativă a cadrelor de securitate

În acest subcapitol va fi expusă analiza comparativă a prototipului CSSCE, ca rezultat științific al prezentei teze de doctor, cu strategiile de securitate propuse de către alți cercetători analizate în capitolul 2. Etapele metodei științifice utilizate pentru dezvoltarea prototipului CSSCE și recomandările din standardul ISO 27001 au fost utilizate ca și criterii de referință, pentru a identifica similitudinea dintre cadrele de securitate propuse anterior de către cercetători și CSSCE, dar și de a sublinia originalitatea și inovația CSSCE, rezultatele analizei fiind incluse în tabelul 4.5.

Rezultatele au evidențiat caracterul secvențial al cadrelor de securitate orientate spre procesul educațional academic atât pentru aspectele de management, cât și pentru procesul de operaționalizare.

Tabelul 4.5. Analiza comparativă a cadrelor de securitate (elaborat de autor)

	Activități	**[8]**	**[126]**	**[127]**	**[128]**	**[129]**	**[130]**	**[99]**	**[133]**
Management (ISO 27001)	Aprobarea administrației				+				
	Stabilirea contextului	+	+		+		+		
	Domeniul de aplicare			+			+	+	
Operaționalizare (SRE)	Elaborarea politicilor de securitate	+			+		+		+
	Identificarea activelor	+		+	+	+	+	+	
	Identificarea obiectivelor de securitate							+	
	Identificarea amenințărilor			+	+	+	+	+	
	Evaluarea riscului	+		+	+	+	+	+	+
	Identificarea cerințelor de securitate			+	+	+	+	+	
	Completarea depozitului			+					
Șabloane, documente obligatorii	Declarația de aplicabilitate				+				
	Registrul riscului								
	Lista verificare active								
	Politica de securitate				+				
	Plan de tratare riscuri			+	+	+			

Cu referire la procesul de operaționalizare a sistemului de securitate, se poate menționa că, chiar dacă unele lucrări științifice includeau una din cele 7 etape de operaționalizare, acestea erau destul de generice. Politicile de securitate erau abordate superficial, fără a specifica care sunt necesitățile și fără a oferi un model tip care să poată fi implementat. Etapa în care se identifică activele informaționale importante, de asemenea, se prezenta ca un proces secvențial, care nu conținea o listă completă cu active clasificate pe diferite categorii, care asigură un anumit serviciu electronic academic. Obiectivele de securitate importante ale fiecărui serviciu electronic academic nu au fost anterior specificate. De asemenea, cu referire la amenințările generice și specifice de securitate, prototipul CSSCE a completat lista amenințărilor generice cu obiectivele de securitate care sunt încălcate de o anumită amenințare și au fost identificate amenințările de securitate specifice pentru fiecare activ bazat pe CE important, lucru care nu a mai fost realizat anterior.

Pentru evaluarea riscului cibernetic a fost propusă o nouă abordare, care vine să faciliteze acest proces imperativ prin identificarea activelor valoroase pentru diverse procese secundare, abordare care simplifică mult procesul de evaluare a riscului cibernetic, într-un mediu complex, după cum este cel universitar, care deține mii de active bazate pe CE, iar evidența și valoarea acestora este greu de determinat, fără o referire clară la impactul avut de activ în realizarea proceselor academice. Astfel, valoarea activelor bazate pe CE este determinată de nivelul de rețea la care aderă: acces, agregare sau de bază.

Specificarea cerințelor de securitate, în alte lucrări științifice, era un proces fragmentat și nu unul cuprinzător ca cel propus în lucrarea de față, în care au fost specificate clar cerințele de securitate de bază, standard și sporite pentru fiecare activ bazat pe CE universitar, pentru fiecare categorie: echipamente terminale, software, rețea și comunicații, personal și infrastructură. Iar ca finalitate a fost creat un depozit care conține cerințe de securitate relevante activelor, care să poată fi utilizat în comun de către practicieni, actualizat și validat periodic.

Cu referire la lucrările științifice studiate nu au fost identificate prototipuri ale unor instrumente software dezvoltate de către cercetătorii vizați, care să poată fi implementate în mediile universitare.

4.5. Concluzii la capitolul 4

Evaluarea este una dintre principalele etape ale metodei DSR. Prototipul CSSCE a fost evaluat, utilizând studiul de caz, care a permis simularea procesului de implementare a CSSCE în cadrul unei facultăți, și a metodei Delphi, conform criteriilor de valoare ale CSSCE, fiind efectuată prelucrarea statistică a datelor înregistrate care au contribuit la confirmarea și validarea CSSCE.

În baza rezultatelor obținute pot fi trase următoarele concluzii:

1. Pentru perfecționarea rezultatelor științifice aplicative și confirmarea utilității prototipului CSSCE au fost identificați 24 de experți în domeniu, care au evaluat prototipul CSSCE în baza unui chestionar și au propus sugestii de îmbunătățire, adăugând valoare aplicativă.

2. Implicarea în sondaj a specialiștilor din cadrul IÎS a contribuit la diseminarea rezultatelor științifice obținute în lucrarea de față privind prototipul CSSCE pentru părțile interesate.

3. Indicatorii statisticii descriptive utilizați pentru prelucrarea rezultatelor sondajului au permis a identifica o valoare medie a calificativelor înregistrate, prin care s-a confirmat satisfacerea criteriilor sondajului cu valoarea medie de 4,5 (din valoarea maximă posibilă 5,0) a celor 15 experți și 9 specialiști din IÎS, care au participat la sondaj. Totodată, poate fi menționată dispersia datelor ce se datorează anonimatului participanților implicați, care nu au fost influențați de alte opinii decât de cea proprie, când au evaluat prototipul CSSCE, conform criteriilor de valoare.

4. Testul non-parametric al statisticii inferențiale în baza coeficientului de concordanță W al lui Kendall a permis determinarea acordului dintre Panelul 1 și Panelul 2 format din experții care au evaluat prototipul CSSCE. Coeficientul de concordanță a constituit W=**0,752**, astfel conform valorilor din tabelul 4.3, confirmă acordul puternic între evaluatorii CSSCE. Deci, prototipul CSSCE poate fi validat.

5. Recomandările experților care au participat la sondajul de evaluare a prototipului CSSCE reprezintă o resursă valoroasă pentru confirmarea rezultatelor științifice obținute privind prototipul CSSCE.

6. Analiza comparativă dintre 8 cadre de securitate, propuse anterior de către alți cercetători și CSSCE, în baza prevederilor obligatorii ale standardului ISO 27001 și a etapelor de operaționalizare a cadrelor de securitate, a permis de a demonstra originalitatea și inovația rezultatelor științifice din această teză de doctor.

CONCLUZII FINALE ȘI RECOMANDĂRI

Cadrele sistemice prin care se abordează holistic securitatea CE reprezintă o parte semnificativă a procesului de asigurare a protecției mediilor electronice. Însă o astfel de abordare cuprinzătoare a securității CE în mediul academic este insuficient cercetată, ipoteză susținută de mai mulți cercetători [8, 9, 196] și demonstrată în prezenta teză de doctor.

Așadar, conform problemei de cercetare identificate și a sarcinilor stabilite în capitolul 1, pot fi trase următoarele concluzii finale:

1. Principala contribuție a tezei constă în elaborarea unui cadru inovativ CSSCE necesar pentru asigurarea securității CE universitare de sus în jos, ce corespunde strategiei de dezvoltare formală a sistemelor de securitate și stabilește un proces clar de implementare constituit din 7 etape importante de operaționalizare a CSSCE și care poate fi evaluat cantitativ prin 12 indicatori-cheie de performanță.
2. Este propusă o nouă definiție a conceptului de securitate a comunicațiilor electronice în baza elementelor-cheie identificate, iar concluzia generală constă în faptul că securitatea nu poate fi măsurată datorită complexității elementelor fuzzy, care formează sistemul de securitate, respectiv și securitatea CE fiind fuzzy, iar scopul implementării cadrului sistemic de securitate este de a crea un scenariu cât mai securizat pentru rețelele și serviciile de CE, reieșind din șirul amenințărilor de securitate existente într-un anumit moment de timp.
3. A fost dezvoltat un model de evaluare a CSSCE prin care a fost evaluat și confirmat cadrul sistemic de către experții și persoanele responsabile din IÎS, prin utilizarea metodei Delphi, iar media obținută a constituit aproximativ 4,6 din 5 puncte posibile conform scării Likert. Rezultatele științifice obținute au fost implementate în 3 IÎS naționale, care în prezent gestionează RCE complexe, după cum sunt Universitatea Tehnică a Moldovei, Universitatea de Stat de Medicină şi Farmacie „Nicolae Testemiţanu” din Republica Moldova și Universitatea Liberă Internațională din Moldova (după cum a fost menționat în primele 3 concluzii se referă și la celelalte IÎS din RM).
4. Analiza comparativă dintre CSSCE și alte cadre de securitate elaborate de cercetători la nivel internațional a demonstrat originalitatea soluției propuse în teză prin elaborarea unei noi metode de evaluare a riscului activelor bazate pe CE; determinarea principiilor de securitate supuse amenințărilor generice de securitate; specificarea cerințelor de securitate și a priorității de implementare; crearea unui depozit care conține cerințele de securitate, amenințările și activele importante ce pot fi utilizat de către practicieni pentru a se asigura implementarea cerințelor de securitate comune IÎS; dezvoltarea prototipului i-CSSCE care va putea fi utilizat

ca ghid în procesul de implementare a CSSCE și pentru a avea o privire de ansamblu asupra statutului securității CE în IÎS naționale.

5. CSSCE și prototipul i-CSSCE au fost validate prin utilizarea studiului de caz. Drept referință a servit Facultatea Electronică și Telecomunicații, UTM, acțiune ce a permis reflectarea întregului parcurs al implementării CSSCE. Cunoștințele și simulările au fost intercalate ulterior în cadrul orelor de curs și lucrărilor de laborator la disciplinele *Securitatea informației în sistemele de telecomunicații* și *Securitatea informației* din cadrul Facultății Electronică și Telecomunicații și la disciplina *Tehnologii ale securității informaționale* din cadrul Facultății Calculatoare, Informatică și Microelectronică, UTM.

Implicații

Eforturile autorului pe întreaga perioadă a studiului au fost orientate spre obținerea contribuțiilor valoroase în domeniul securității CE, care pot fi preluate de către cercetători, practicienii în domeniu și responsabilii de elaborarea politicilor și strategiilor de securitate la nivel guvernamental.

Cercetătorii pot utiliza prototipul CSSCE elaborat în prezenta teză în abordarea sistemică a securității CE și ca un cadru de referință pentru a fi comparat cu rezultatele științifice proprii sau pentru a contribui la îmbunătățirea prototipului CSSCE. De asemenea, amenințările de securitate identificate pot fi analizate și utilizate în cercetările ulterioare.

Practicienii în domeniu pot utiliza în activitățile de asigurare a securității CE, în perioada post-implementare a serviciului educațional academic, abordarea sistemică propusă de autor, cu referință la operaționalizarea prototipului CSSCE, sau în perioada de implementare, pentru a se asigura cu un sistem de securitate conform standardelor internaționale.

Responsabilii de elaborarea politicilor și strategiilor de securitate la nivel guvernamental pot utiliza contribuțiile practice din prezenta teză la perfectarea politicii de securitate, a strategiilor și indicatorilor de performanță, pentru a verifica maturitatea și completitudinea sistemelor de securitate.

Limite ale cercetării

Datorită caracterului permanent dinamic și iterativ al securității, prototipul CSSCE nu pretinde a fi varianta completă. Cu toate acestea, studiul din prezenta teză reprezintă o primă încercare, la nivel național, de a realiza un cadru sistemic de securitate a CE, conform standardelor în domeniu și a celor mai bune practici, pentru respectarea principiilor fundamentale de securitate.

Deoarece mulțimea amenințărilor de securitate este fuzzy, apărând cu regularitate noi amenințări, CSSCE va necesita modificări și ajustări periodice.

Deși componenta subiectivă a studiului a fost redusă maximal posibil, nu poate fi exclusă totuși în totalitate, deoarece prototipul CSSCE este rezultatul unei analize a factorului uman care poate fi parțial subiectivă, iar abordările pot fi diferite de la individ la individ.

Direcții viitoare de cercetare

Problema de cercetare analizată în această lucrare se referă la un domeniu foarte vast și important, cu un nivel de incertitudine dificil de evaluat. Mai mult ca atât, securitatea nu poate fi considerată obiectivă, deoarece derivă din percepția individului, iar cercetările riguroase în acest domeniu reprezintă doar o pistă inițială. Cercetările viitoare vor contribui la modificarea anumitor aspecte sau la adăugarea de noi elemente semnificative pentru cadrul sistemic de securitate. Deși au fost obținute rezultate științifice importante, sunt absolut necesare și obligatorii în perspectivă studii empirice suplimentare pentru a determina eficacitatea prototipului CSSCE. Prototipul aplicației i-CSSCE poate servi la evaluarea inițială a securității, însă în timp va necesita perfectarea politicilor, cerințelor și controalelor de securitate pentru o analiză cât mai cuprinzătoare a mediului.

Prototipul CSSCE a fost elaborat pentru procesul educațional academic și nu acoperă procesul de cercetare în IÎS, astfel în lucrările viitoare ale autorului sau ale altor cercetători, eforturile s-ar putea concentra pe extinderea domeniului de aplicare a CSSCE, pentru a se asigura integritatea și confidențialitatea rezultatelor științifice și a proprietății intelectuale în IÎS.

De asemenea, Industria 4.0 și utilizarea tot mai frecventă a dispozitivelor IoT în campusurile universitare impune necesitatea abordării amenințărilor și vulnerabilităților de securitate specifice acestor dispozitive. Cercetările viitoare s-ar putea concentra pe analiza și elaborarea cadrelor de securitate care să abordeze securitatea pe această dimensiune.

Obiectivele pe termen lung sunt crearea strategiilor standardizate la nivel de stat, pentru organizațiile cu profiluri similare, care să conțină recomandări clare și explicite, astfel încât să faciliteze, în secolul tehnologiilor moderne, abordarea sistemică a CE.

Precizări finale

Digitalizarea și automatizarea procesului educațional academic al instituțiilor de învățământ superior din Republica Moldova este un proces foarte important și fundamental în crearea unui mediu educațional modern, aliniat la revoluția industrială 4.0. Astfel, asigurarea

securității CE, în RCE universitare extinse și parțial deschise, are un rol tot mai important, care va crește în următoarea perioadă de timp cu aceeași intensitate cu care are loc digitalizarea.

Cadrul sistemic de securitate a CE, rezultat din cercetările efectuate în prezenta teză de doctor, reprezintă un suport metodologic și aplicativ important.

Instituțiile de învățământ superior care vor implementa prototipul CSSCE derivat din rezultatele cercetărilor vor beneficia de un cadru sistemic de securitate eficient, conform standardelor internaționale în domeniu și celor mai bune practici; clar definit, va diminua entropia existentă în orice sistem complex și va oferi siguranță în prestarea serviciilor educaționale moderne și intens tehnologizate.

BIBLIOGRAFIE

1. AL-GHAMDI, M. I. Effects of knowledge of cyber security on prevention of attacks. In: *Materials Today: Proceedings,* Apr. 2021. DOI: 10.1016/J.MATPR.2021.04.098. ISSN 2214-7853.
2. **ALEXEI, Ar**, ALEXEI, An. The difference between cyber security vs information security. In: *Journal of Engineering Science*, vol. XXIX, no. 4, 2022, pp. 72 - 83. ISSN 2587-3474. DOI: https://doi.org/10.52326/jes.utm.2022.29(4).08.
3. *Enisa Threat Landscape 2021*. ENISA, 2021 [citat 5.09.2022]. Disponibil: https: //www. enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/full Report.
4. *Cost of a Data Breach Report 2022*. IBM Security, 2022 [citat 6.09.2022]. Disponibil: https://www.ibm.com/downloads/cas/3R8N1DZJ.
5. *Enisa Threat Landscape for Ransomware Attacks.* ENISA, 2022 [citat 5.09.2022]. Disponibil: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks/@@download/fullReport.
6. *Significant Cyber Incidents.* Center for Strategic and International Studies (CSIS), 2022 [citat 19.03.2022]. Disponibil: https://www.csis.org/programs/strategic-technologies-program/ significant-cyber-incidents.
7. *Cyber Security Report*. Check Point Research, 2021 [citat 20.03.2022]. Disponibil: https://www.checkpoint.com
8. REHMAN, H., MASOOD, A., CHEEMA, A. R. Information Security Management in academic institutes of Pakistan. In: *2013 2nd National Conference on Information Assurance (NCIA),* 2013, pp. 47-51. DOI: 10.1109/NCIA.2013.6725323. e-ISBN: 978-1-4799-1288-9.
9. FOUAD, S. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. In: Journal of Cyber Policy. 2021, vol. 6(2), pp. 137–154. DOI: 10.1080/23738871.2021.1973526. ISSN: 2373-8871.
10. **ALEXEI, Ar.**, NISTIRIUC, P., ALEXEI, An. The holistic approach to cybersecurity in academia. In: *Central and Eastern European eDem and eGov Days (CEEeGov), September 22-23, 2022*. Budapest, Hungary, pp.106-111. ACM, New York, NY, USA, 6 pages. DOI: https://doi.org/10.1145/3551504.3551516. ISBN: 978-1-4503-9766-7.
11. LUO, X. Security protection to industrial control system based on Defense-in- Depth strategy. In*: WIT Transactions on Engineering Sciences*. 2016, nr. 113, pp. 19–27. E-ISSN: 1743-3533.

12. KITCHENHAM, B. Procedures for Performing Systematic Reviews. In: *Eversleigh NSW 1430*. 2004. ISSN:1353-7776.
13. VOM BROCKE, J., HEVNER, A., MAEDCHE, A. Introduction to Design Science Research. In: *Design Science Research. Cases*. 2020. Springer. DOI: 10.1007/978-3-030-46781-4_1.D. ISBN: 978-3-030-46780-7.
14. MELLADO, D., FERNÁNDEZ-MEDINA, E., PIATTINI, M. Applying a Security Requirements Engineering Process. In: *European Symposium on Research in Computer Security*. 2006, pp. 192–206. DOI: 10.1007/11863908_13. ISBN: 978-3-540-44601-9
15. SKINNER, R., et al. The Delphi Method Research Strategy in Studies of Information Systems. In: *Communications of the Association for Information Systems*. 2015, vol. 37. DOI: 10.17705 /1CAIS.03702. ISSN: 1529-3181.
16. GEARHART, A., et al. Use of Kendall's coefficient of concordance to assess agreement among observers of very high-resolution imagery. In: *Geocarto International*. 2013, vol. 28, no. 6, pp. 517–526. DOI: 10.1080/10106049.2012.725775.
17. ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT. International Organization for Standardization. Geneva, Switzerland, 2022. [citat 02.03.2023].
18. GÜRKAYNAK, G., YILMAZ, I., TASKIRAN, N. P. Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age. In: *Computer Law & Security Review*. Apr. 2014, vol. 30, no. 2, pp. 179–189. DOI: 10.1016/j.clsr.2014.01.010. ISSN: 0267-3649.
19. SHARON, K. B. *Telecommunications Law in the Internet Age*. Elsevier, 2002, p. 516. DOI: 10.1016/B978-1-55860-546-6.X5022-4. ISBN 978-1-55860-546-6.
20. *Guide to the Privacy and Electronic Communications Regulations.* Information Commissioners Office, 2018 [citat 30.09.2022]. Disponibil: chrome-extension://oemmndcbldboie bfnladd acbdf madadm/https://ico.org.uk/media/for-organisations/guide-to-pecr-2-4.pdf
21. ADEKA, M. I., SHEPHERD, S. J., ABD-ALHAMEED, R. Telecommunication network security. In: *Clary TS (Ed.) Horizons in Computer Science Research*, vol. 10, 2015, pp. 1–33. ISBN: 978-1-63463-740-4.
22. FRENZEL, L. E. *Principles of Electronic Communication Systems*. McGrawHill Education, 4th ed., 2016. ISBN: 978-0-07-337385-0.
23. KUMAR, K., KUMAR, V., SEEMA. Security and Privacy Preservation for Data Communication Network. In: *Procedia Computer Science*. 2022, vol. 215 (C), pp 1–7. DOI: 10.1016/j.procs.2022.12.001. ISSN: 1877-0509.

24. *Legea Comunicațiilor Electronice RM*. Parlamentul RM, 2007 [citat 30.09.2022]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=84365&lang=ro.
25. SCRIPCARIU, L., BOGDAN, I., NICOLAESCU, Ș.V., GHEORGHE, C.G., NICOLAESCU, L. *Securitatea rețelelor de comunicații*. Iași: Casa De Edidură "VENUS", 2008. ISBN 978-973-756-074-2.
26. *Recommendation ITU-R V.662-2. Terms and definitions.* International Telecommunication Union, 1993.
27. *Security in telecommunications and information technology*. ITU-T Technical Report, 2020.
28. DZUNG, D., NAEDELE, M., VON HOFF, T. P., CREVATIN, M. Security for Industrial Communication Systems. In: *Proceedings of the IEEE*. 2005, vol. 93, no. 6, pp. 1152–1177. DOI: 10.1109/JPROC.2005.849714. ISSN 1558-2256.
29. WHITMAN, M. E., MATTORD, H.J. *Principles of Information Security*. 7th ed. Cengage Learning, 2021. ISBN 9781337102063.
30. CĂPĂŢÂNĂ, Gheorghe, CERBU, Olga. Some Educational Problems in Informational Security. In: *Information Technologies and Security*, 2012, pp. 344–352. ISBN 978-9975-4172-3-5.
31. COSTAŞ, Ilie. Factorii de influenţă asupra dezvoltării infrastructurii informaţionale a societăţii. În: *Conferința Științifică Internațională "Rolul investițiilor în dezvoltarea economiei digitale în contextul globalizării financiare"*, 2016. ISBN 978-9975-75-866-6.
32. WILLS, Mike. *The Official (ISC)2 SSCP CBK Reference.* 5th ed. John Wiley & Sons, Inc. Indianapolis, Indiana, 2020. ISBN 1119874866.
33. *DIRECTIVA (UE) 2018/1972. Codul european al comunicațiilor electronice*. PARLAMENTUL EUROPEAN and CONSILIUL UNIUNII EUROPENE, Jurnalul Oficial al Uniunii Europene, 2018 [citat 30.09.2022]. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32018L1972&from=EN#d1e2668-36-1.
34. BRAGARU, T., BRICEAG, V., MALCOCI, V., GALAICU, V. Securitatea informației vis-à-vis de securitatea informațională. În: *STUDIA UNIVERSITATIS MOLDAVIAE*, vol. 2, no. 122, pp. 38–47, 2019. ISSN 1857-2073.
35. *Glossary*. National Institute of Standards and Technology, [citat 16.09.2022]. Disponibil: https://csrc.nist.gov/glossary/term/.
36. *TELECOMMUNICATIONS OPERATIONS. Security Management Directive System MD Number: 4800*. Department of Homeland Security, [citat 03.03.2022]. Disponibil:

https://docplayer.net/9316461-Department-of-homeland-security-management-directive-system-md-number-4800-telecommunications-operations.html.

37. JAY, Rosemary. *Data Protection Law and Practice*. 5th ed. Sweet & Maxwell, 2020. ISBN 0414070968.
38. YAN, D. A Systems Thinking for Cybersecurity Modelling. In: *Computer Science*, Jan. 2020. DOI: https://doi.org/10.48550/arXiv.2001.05734.
39. *Overview of cybersecurity*. International Telecommunication Union, [citat 10.09.2022]. Disponibil:https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets.
40. *Glosar de termeni*. ANRCETI, [citat 05.12.2021]. Disponibil: https://www.anrceti.md/glossary/T.
41. *Asset management guidelines in telecommunication organizations. Information and network security – Security management*. International Telecommunication Union, 2011, [citat 03.03.2022]. Disponibil: https://www.itu.int/rec/T-REC-X.1057-201105-I/en.
42. *Data communication networks: open systems interconnection (OSI); security, structure and application*. International Telecommunication Union, 1991, [citat 04.03.2022]. Disponibil: https://www.itu.int/rec/T-REC-X.
43. *Security architecture for systems providing end-to-end communications.* International Telecommunication Union, 2003, [citat 04.03.2022]. Disponibil: https://www.itu.int/rec/T-REC-X.805.
44. SALTZER, J. H., REED, D. P., CLARK, D.D. End-to-end arguments in system design. In: *ACM Transactions on Computer Systems*, vol. 2, no. 4, pp. 277–288, Nov. 1984. DOI: 10.1145/357401.357402. ISBN 0-89006-337-0.
45. ISENBERG, P., et al. Collaborative visualization: Definition, challenges, and research agenda. In: *Information Visualization*, vol. 10 (4), October 2011 pp 310–326. DOI: https://doi.org/10.1177/1473871611412817. ISSN 1473-8716.
46. **ALEXEI, Ar.**, Alexei, An. Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. In: *International Journal of Scientific & Technology Research*. 2021, vol. 10(3), pp 128-133. ISSN: 2277-8616.
47. **ALEXEI**, **Ar.** NETWORK SECURITY THREATS TO HIGHER EDUCATION INSTITUTIONS. In: *CEE e|Dem and e|Gov Days*. May 2021, pp. 323–333. DOI: 10.24989/ocg.v341.24. ISBN 978-3-7089-2121-1.

48. BALAREZO, J. F., WANG, S., CHAVEZ, K. G., AL-HOURANI, A., KANDEEPAN, S. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. In: *Engineering Science and Technology*, vol. 31, p. 101065, Jul. 2022. DOI: 10.1016/J.JESTCH.2021.09.011. ISSN 2215-0986.
49. ELIYAN, L. F., PIETRO, R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. In: *Future Generation Computer Systems*, vol. 122, pp. 149–171, Sep. 2021. DOI: 10.1016/j.future.2021.03.011. ISSN 0167-739X.
50. *DDoS THREAT INTELLIGENCE REPORT*. Netscout, 2022, [citat 04.09.2022]. Disponibil: https://www.netscout.com/threatreport/.
51. PRABADEVI, B., JEYANTHI, N. A Review on Various Sniffing Attacks and its Mitigation Techniques. In: *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 3, p. 1117, Dec. 2018. DOI: 10.11591/ijeecs.v12.i3.pp1117-1125. ISSN 2502-4752.
52. JAVEED, D., BADAMASI, U.M. Man in the Middle Attacks: Analysis, Motivation and Prevention. In: *International Journal of Computer Networks and Communications Security*, vol. 8, no. 7, pp. 52–58, Jul. 2020. DOI: 10.47277/IJCNCS/8(7)1. ISSN 2410-0595.
53. RAMESH, P., BHASKARI, D. L. A Comprehensive Analysis of Spoofing. In: *International Journal of Advanced Computer Science and Applications*, vol. 1, no. 6, 2010. DOI: 10.14569/IJACSA.2010.010623.
54. JACOVIC, M. et al. Mitigating RF jamming attacks at the physical layer with machine learning. In: *IET Communications*, vol. 17, no. 1, pp. 12–28, Jan. 2023. DOI: 10.1049/cmu2.12461. ISSN:1751-8636.
55. **ALEXEI, Ar,** ALEXEI, An. Analysis of IoT security issues used in Higher Education Institutions. In: *INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH*. 2021, vol. 09, no. 05. DOI: 10.47191/ijmcr/v9i5.01. ISSN 2277-2286.
56. BEAMAN, C., et al. Ransomware: Recent advances, analysis, challenges and future research directions. In: *Computer Security*, vol. 111, p. 102490, Dec. 2021. DOI: 10.1016/j.cose.2021.102490. ISSN 0167-4048.
57. SAPALO SICATO, J. C., et al. VPN Filter Malware Analysis on Cyber Threat in Smart Home Network. In: *Applied Sciences*, vol. 9, no. 13, p. 2763, Jul. 2019. DOI: 10.3390/app9132763. ISSN: 2076-3417.

58. TRAN LE, D., et al. Malware Spreading Model for Ruters in Wi-Fi Networks. In: *IEEE Access,* vol. 10, pp. 61873–61891, 2022. DOI: 10.1109/ACCESS.2022.3182243. ISSN 2169-3536.
59. *TELECOM SECURITY INCIDENTS 2021*. ENISA, 2022 [citat 04.10.2022]. Disponibil: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://www.enisa.europa.eu/publications/telecom-security-incidents-2021/@@download/fullReport.
60. GRECU, M., COSTAȘ, I., REABOI, A. E-Government services in Moldova: value and opportunities. In: *CEE e|Dem and e|Gov Days*, 2017, pp. 347–357. ISBN 978-3-903035-14-0.
61. *Raport despre executarea în semestrul I 2020 a Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020*. Ministerul Economiei și Infrastructurii al RM, 2020 [citat 07.10.2021]. Disponibil: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://me.gov.md/sites/default/files/raport_evaluare_hg_811_2015_-_07.06.2021.pdf
62. *HOTĂRÎRE nr. 201 din 28-03-2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică*. Guvernul RM, Monitorul Oficial nr. 109-118 art. 277, Apr. 07, 2017 [citat 20.11.2020]. Disponibil: https://mei.gov.md /sites/default/files/ hg_201 _2017 _cerinte_ minime_obligatorii_de_securitate_cibernetica.pdf
63. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Council of the European Union and European Parliament, Jul. 19, 2016 [citat 28.02.2022]. Disponibil: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148).
64. *Sectoral/ thematic threat analysis*. ENISA Threat Landscape, 2020 [citat 28.02.2022]. Disponibil: https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis.
65. *Priorities for EU research Analysis*. ENISA, 2017 [citat 28.09.2022]. Disponibil: https://www.enisa.europa.eu/publications/priorities-for-eu-research
66. JANG-JACCARD, J., NEPAL, S. A survey of emerging threats in cybersecurity. In: *Journal of Computer and System Sciences*. 2014, vol. 80(5), pp. 973–993. DOI: 10.1016/j.jcss. 2014. 02.005. ISSN 0022-0000.
67. ALI, M.N.B., HOSSAIN, M.E., PARVEZ, M.M. Design and Implementation of a Secure Campus Network. In: *International Journal of Emerging Technology and Advanced Engineering*, vol. 5, no. 7, 2015. ISSN 2250–2459.

68. BOLANIO, J. B., et al. Network Security Policy for Higher Education Institutions based on ISO Standards. In: *Mediterranean Journal of Basic and Applied Sciences*, vol. 05, no. 01, pp. 01–17, 2021. DOI: 10.46382/MJBAS.2021.5101. ISSN 2581-5059.
69. WASWAS, D., JWAIFELL, M. The Role of Universities' Electronic Management in Achieving Organizational Excellence: Example of Al Hussein Bin Talal University. In: *World Journal of Education*, vol. 9, no. 3, p. 53, Jun. 2019. DOI: 10.5430/wje.v9n3p53. ISSN 1925-0746.
70. PAGUIGAN, J. S., ALBINO, M. G, COSTALES, J.A. An Assessment and Design of Campus Network Using Collapsed-Core Architecture. In: *2022 IEEE 10th International Conference on Information, Communication and Networks (ICICN)*, Aug. 2022, pp. 10–14. DOI: 10.1109/ICICN56848.2022.10006457.
71. HABIB, M. N., et al. Transforming universities in interactive digital platform: case of city university of science and information technology. In: *Education and Information Technology*, vol. 26, no. 1, pp. 517–541, Jan. 2021. DOI: 10.1007/s10639-020-10237-w. ISSN 1573-7608.
72. ENOCH, J.D., SUNNY, O., CHRISTOPHER, A. Design and Simulation of a Secured Enterprise Network for Faculty of Engineering, Rivers State University. In: *Computer Engineering and Intelligent Systems*, vol. 10, no. 5, 2019. ISSN 2222-1727.
73. SUNG, Y.-W. E., et al. Towards Systematic Design of Enterprise Networks. In: *IEEE/ACM Transactions on Networking*, vol. 19, no. 3, pp. 695–708, Jun. 2011. DOI: 10.1109/TNET.2010.2089640. ISSN 1558-2566.
74. *Cost of a Data Breach Report*. Ponemon Institute and IBM, 2020 [citat 09.01.2021]. Disponibil: https://www.ibm.com/security/digital-assets/cost-data-breach-report.
75. *Education Report*. Kaspersky. [citat 09.12.2020]. Disponibil: https://media.kaspersky content hub .com /wp-content/uploads/sites/43/2020/09/04113558/education _report_04092020 _2 .pdf
76. PANJA, B., et al. Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. In: *2013 International Conference on Collaboration Technologies and Systems (CTS)*. 2013, pp. 397–403. DOI: 10.1109/CTS.2013.6567261. ISBN:978-1-4673-6403-4.
77. COVENTRY, L., BRANLEY, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. In: *Maturitas.* 2018, vol. 113, pp. 48–52. DOI: 10.1016/ j.maturitas. 2018.04.008. ISSN 0378-5122.

78. ANI, U. D., HE, H., TIWARI, A. Human factor security: evaluating the cybersecurity capacity of the industrial workforce. In: *Journal of Systems and Information Technology*. 2019, vol. 21, no. 1, pp. 2–35. DOI: 10.1108/JSIT-02-2018-0028. ISSN: 1328-7265.
79. BREWER, R. Ransomware attacks: detection, prevention and cure. In: *Network Security*. 2016, no. 9. DOI: 10.1016/S1353-4858(16)30086-1. ISSN 1353-4858.
80. DESHMUKH, R., DEVADKAR, K. K. Understanding DDoS Attack & its Effect in Cloud Environment. In: *Procedia Computer Science*. 2015, vol.49. DOI: 10.1016/j.procs.2015.04.245. ISSN 1877-0509.
81. HUTCHINS, M. J., et al. Framework for Identifying Cybersecurity Risks in Manufacturing. In: *Procedia Manufacturing*, Jan. 2015, vol. 1, pp. 47–63. DOI: 10.1016/j.promfg.2015.09.060. ISSN 2351-9789.
82. *IT-Grundschutz Informationssicherheit mit System*. BSI, 2020. [citat 12.07.2021]. Disponibil:https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/ Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.
83. KHTHER, R. A., OTHMAN, M. Cobit Framework as a Guideline of Effective it Governance in Higher Education: A Review. In: *International Journal of Information Technology Convergence and Services*. 2013, vol. 3, no. 1. DOI: 10.5121/ijitcs.2013.3102. ISSN: 2231-1939.
84. GËRVALLA, M., PRENIQI, N., KOPACEK, P. IT infrastructure library (ITIL) framework approach to IT governance. In: *IFAC-PapersOnLine*. Oct. 2018, vol. 51, no. 30, pp. 181–185. DOI: 10.1016/j.ifacol.2018.11.283. ISSN: 1474-6670.
85. *ISO Survey of certifications to management system standards.* International Organization for Standardization, 2020, [*citat* 20.03.2021]. Disponibil: https://www.iso.org/committee/54998.
htmlt=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top.
86. **ALEXEI**, **A.** Cyber Security Strategies for Higher Education Institutions. In: *Journal of Engineering Science*. 2021, vol. XXVIII, no. 4, pp. 74–92. DOI: 10.52326/ jes.utm. 2021. 28 (4).07. ISSN 2587-3474.
87. *Politica de securitate privind Sistemul Resurselor Informatice şi de Comunicaţii.* Iași: Universitatea „Alexandru Ioan Cuza, 2004, [*citat* 04.03.2021]. Disponibil: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://dcd.uaic.ro/doc/Politica_si_Planul_de_Securitate_RIC.pdf.

88. *POLITICA IT&C*. Universitatea din București, 2019, [citat 04.03.2021]. Disponibil: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://unibuc.ro/wp-content/uploads/2020/02/Politica-ITC-UniBuc_V.1.pdf
89. *Instrumentul Bibliometric Național.* Institutul de Dezvoltare a Societății Informaționale. [citat 10.03.2022]. Disponibil: https://ibn.idsi.md/.
90. COJOCARU, I., COJOCARU, I. A bibliomeric analysis of cybersecurity research papers in Eastern Europe: Case study from the Republic of Moldova. In: *Central and Eastern European eDem and eGov Days*. Mar. 2019, vol. 335, pp. 151–162, DOI: 10.24989/ocg.v335.12. ISBN: 978-3-7089-1898-3.
91. BOLUN, I., CIORBĂ, D., ZGUREANU, A., BULAI, R. Informatics security assessment in the Republic of Moldova. In: *Journal of Engineering Science*, vol. XXVII, no. 4, pp. 103–119, 2020. DOI:10.5281/zenodo.4288297. ISSN 2587-347.
92. BOLUN, I., CIORBA, D., BULAI, R., CALIN, R., BODOGA, C. State of infosecurity in the Republic of Moldova. In: *International Symposium "Actual Problems of Mathematics and Informatics,"* 2020, pp. 94–95. ISBN 978-9975-45-677-7.
93. BOLUN, I., BULAI, R., CIORBA, D. Support of education in cybersecurity. In: *Pro Publico Bono - Magyar Közigazgatás*, vol. 9, no. 1, pp. 128–147, Aug. 2021. DOI: 10.32575/ ppb. 2021.1.8. ISSN 2063-9058.
94. BUZDUGAN, A., CAPATANA, G. Cyber Security Maturity Model for Critical Infrastructures. In: *Smart Innovation, Systems and Technologies,* Vol.276, 2022, pp. 225–236, București, România. DOI: 10.1007/978-981-16-8866-9_19. ISBN 978-981-16-8865-2.
95. Черней Г., Охрименко С., Леаху Ф. *Безопасность автоматизированных информационных систем*. Кишинев: Ruxanda, 1996, 186 стр. ISBN 9975-60-767-5М-187-96.
96. COJOCARIU, A.-C., VERZEA, I., CHAIB, R. Aspects of Cyber-Security in Higher Education Institutions. In: *Innovation in Sustainable Management and Entrepreneurship*. 2020, pp. 3–11. DOI: 10.1007/978-3-030-44711-3_1. ISBN: 978-3-030-44711-3.
97. MUMTAZ, N. Analysis of information security through asset management in academic institutes of Pakistan. In: *2015 International Conference on Information and Communication Technologies (ICICT), IEEE*. Dec. 2015. DOI: 10.1109/ICICT.2015. 7469581. ISBN 9781467389082.

98. **ALEXEI**, **A.** Ensuring Information Security in Public Organizations in the Republic of Moldova through the ISO 27001 Standard. In: *Journal of Social Sciences*. 2021, vol. IV(1). DOI: 10.52326/jss.utm.2021.4(1).11. ISSN 2587-3490.

99. SUROSO, J. S., FAKHROZI, M. A. Assessment of Information System Risk Management with Octave Allegro at Education Institution. In: *Procedia Computer Science*. 2018, vol. 135. DOI: 10.1016/j.procs.2018.08.167. ISSN 1877-0509.

100. **ALEXEI, Ar**, NISTIRIUC, P., ALEXEI, An. Empirical Study of Cyber Security Threats in Moldovan Higher Education Institutions. In: *The 12th International Conference on Electronics, Communications and Computing*. Chișinău: UTM, 20-21 octombrie 2021. ISBN 978-9975-45-776-7.

101. GONZÁLEZ-GRANADILLO, G., GONZÁLEZ-ZARZOSA, S., DIAZ, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. In: *Sensors.* Jul. 2021, vol. 21, no. 14, p. 4759. DOI: 10.3390/s21144759. ISSN: 1424-8220.

102. **LACHI, Arina**, SOROCHIN, S. Analiza modelelor de detecție a intruziunilor moderne. In: *6th International Conference "Telecommunications, Electronics and Informatics" ICTEI 2018.* 24-27 mai 2018, pp. 470-472, Chișinău, Moldova. ISBN 978-9975-45-540-4.

103. ANTUNES, M., et al. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. In: *Journal of Cybersecurity and Privacy*. 2021, vol. 1, no. 2, pp. 219–238. DOI: 10.3390/jcp1020012. E-ISSN 2624-800X.

104. CERBU, Olga, LAZARENCO, Oxana. Politica de securitate a tehnologiilor informaţionale în administraţia publică centrală. În: *Teoria şi practica administrării publice*, 2014, pp. 414–416. ISBN: 978-9975-4241-9-6.

105. BUZDUGAN, Aurelian. Information system for cyber security maturity assessment. In: METODOLOGII CONTEMPORANE DE CERCETARE ŞI EVALUARE, 2021, pp. 98–102. ISBN: 978-9975-159-16-6.

106. DRESCH, A., LACERDA, D. P., ANTUNES, J/ Design Science Research. In *Cham: Springer International Publishing*. 2015. DOI: 10.1007/978-3-319-07374-3. ISBN: 978-3-319-07373-6.

107. HEVNER, MARCH, PAR, RAM. Design Science in Information Systems Research. In: *MIS Quarterly*. 2004, vol. 28, no. 1. DOI: 10.2307/25148625. ISSN: 0276-7783.

108. BASKERVILLE, R. Design Science Research Contributions: Finding a Balance between Artifact and Theory. In: *Journal of the Association for Information Systems*. 2018, vol. 19, no. 5. DOI: 10.17705/1jais.00495. ISSN: 1536-9323.

109. CHANDRA KRUSE, L., SEIDEL, S., VOM BROCKE, J. Design Archaeology: Generating Design Knowledge from Real-World Artifact Design. In: *Tulu, B., Djamasbi, S., Leroy, G. (eds) Extending the Boundaries of Design Science Theory and Practice*. DESRIST 2019. Lecture Notes in Computer Science, vol 11491. Springer, Cham. DOI: 10.1007/978-3-030-19504-5_3. ISSN 0302-9743.

110. LEE, A. S., THOMAS, M., BASKERVILLE, R. L. Going back to basics in design science: from the information technology artifact to the information systems artifact. In: *Information Systems Journal*. 2015, vol. 25, no. 1. DOI: 10.1111/isj.12054. ISSN: 1350-1917.

111. WATSON, BOUDREAU, CHEN. Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community. In: *MIS Quarterly*. 2010, vol. 34, no. 1. DOI: 10.2307/20721413. ISSN: 0276-7783.

112. BECKER, J. et al. In Search of Information Systems (Grand) Challenges. In: *Business & Information Systems Engineering*. 2015, vol. 57, no. 6. DOI: 10.1007/s12599-015-0394-0. ISSN: 2363-7005.

113. SIMON, H.A. The Sciences of the Artificial. In: *3rd ed. London: MIT Press, Cambridge Massachusetts*, 1996. ISBN 9780262193740.

114. PEFFERS, K., et al. A Design Science Research Methodology for Information Systems Research. In: *Journal of Management Information Systems*. 2007, vol. 24, no. 3. DOI: 10.2753/MIS0742-1222240302. ISSN: 0742-1222.

115. VAISHNAVI, V. K., KUECHLER, W. L. Design Science Research in Information Systems. In: *Ais*. 2004, pp. 1–45. DOI: 10.1007/978-1-4419-5653-8. ISBN: 978-1-4419-5652-1.

116. MARCH, S. T., SMITH, G. F. Design and natural science research on information technology. In: *Decision Support Systems*. 1995, vol. 15, no. 4, pp. 251–266. DOI: 10.1016/0167-9236(94)00041-2. ISSN: 0167-9236.

117. JOHANNESSON, P., PERJONS, E. An Introduction to Design Science. In: *Cham: Springer International Publishing*. 2014. DOI: 10.1007/978-3-319-10632-8. ISBN: 978-3-319-10631-1.

118. VENABLE, J., PRIES-HEJE, J. A Comprehensive Framework for Evaluation in Design Science Research. In: *Design Science Research in Information Systems. Advances in Theory and Practice*. 2012, pp. 423–438. DOI: 10.1007/978-3-642-29863-9_31. ISBN 978-3-642-29862-2.

119. **ALEXEI, A.** Using Design Science Research Method to Develop a Cyber Security Framework for HEIs in Moldova. In: *The 12th International Conference on Electronics,*

Communications and Computing. Chișinău: UTM, 20-21 octombrie 2021. ISBN 978-9975-45-776-7.

120. PRAT, N., COMYN-WATTIAU, I., AKOKA, J. A Taxonomy of Evaluation Methods for Information Systems Artifacts. In: *Journal of Management Information Systems.* 2015, vol. 32, no. 3, pp. 229–267. DOI: 10.1080/07421222.2015.1099390. ISSN: 0742-1222.
121. MIJAC, M. Evaluation of Design Science instantiation artifacts in Software engineering research. In: *Proceedings of the Central European Conference on Information and Intelligent Systems*. 2019, pp.313-321. ISSN: 1847-2001.
122. SONNENBERG, C., VOM BROCKE, J. Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research. In: *Peffers, K., Rothenberger, M., Kuechler, B. (eds) Design Science Research in Information Systems. Advances in Theory and Practice. DESRIST 2012. Lecture Notes in Computer Science, vol 7286*. Springer, Berlin, Heidelberg. 2012, pp. 381–397. DOI: 10.1007/978-3-642-29863-9_28. ISBN 978-3-642-29862-2
123. CHRISTIE, E., et al. Prototyping Strategies: Literature Review and Identification of Critical Variables. In: *ASEE Annual Conference.* 2012. DOI: 10.18260/1-2--21848. ISSN 2153-5965.
124. NUNAMAKER, J. F., CHEN, M., PURDIN, T. Systems Development in Information Systems Research. In: *Journal of Management Information Systems*. 1990, vol. 7, no. 3, pp. 89–106. ISSN: 07421222.
125. CHENG, S. Reference Manager Mendeley. 2014. [citat 01.04.2021]. Disponibil: https://www.elsevier.com/connect/exporting-to-mendeley-from-scopus-and-sciencedirect.
126. YUSTANTI, W. An analysis of Indonesia's information security index: a case study in a public university. In: *IOP Conference Series: Materials Science and Engineering*. 2018, vol. 296. DOI: 10.1088/1757-899X/296/1/012038. ISSN: 1757-8981.
127. JOSHI, C., SINGH, U. K. Information security risks management framework – A step towards mitigating security risks in university network. In: *Journal of Information Security and Applications.* 2017, vol. 35. DOI: 10.1016/j.jisa.2017.06.006. ISSN: 2214-2126.
128. ITRADAT, A. et al. Developing an ISO 27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. In: *Jordan Journal of Mechanical & Industrial Engineering.* 2014, vol. 8, no. 2, pp. 102–118. ISSN 1995-6665.
129. HOMMEL, W., METZGER, S., STEINKE, M. Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization. In: *EUNIS Journal of Higher Education IT.* 2015. ISSN 2519-1764.

130. DAS, S., MUKHOPADHYAY, A., BHASKER, B. Today's Action is Better than Tomorrow's Cure - Evaluating Information Security at a Premier Indian Business School. In: *Journal of Cases on Information Technology*. 2013, vol. 15, no. 3. DOI: 10.4018/jcit.2013070101. ISSN: 1548-7717.

131. ARAFAT, J., et al. Emergence of Robust Information Security Management Emergence of Robust Information Security Management ergence of Robust Information Security Management Structure around the world wide Higher Education Structure around the world wide Higher Education Institutions: Institutions:aMultifaceted Security Solution. In: *International Journal of Computer Science Issues*. 2012. ISSN 1694-0814.

132. LIU, C.-W. HUANG, P., LUCAS, H. C. IT Governance, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education. In: *SSRN Electronic Journal*. 2016. DOI: 10.2139/ssrn.2850178. ISSN: 1556-5068.

133. KANG, C. M., JOSEPHNG, P. S., ISSA, K. A study on integrating penetration testing into the information security framework for Malaysian higher education institutions. In: *2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC*). 2015, pp. 156-161. DOI: 10.1109/ISMSC.2015.7594045. E- ISBN:978-1-4799-7896-0.

134. NAAGAS, M. A., et al. Defense-through-Deception Network Security Model: Securing University Campus Network from DOS/DDOS Attack. In: *Bulletin of Electrical Engineering and Informatics*. 2018, vol. 7, no. 4. DOI: 10.11591/eei.v7i4.1349. ISSN: 2089-3191.

135. ISMAIL, W. B., et al. A generic framework for information security policy development. In: *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*. 2017, pp. 1-6. DOI: 10.1109/EECSI.2017.8239132. ISBN:978-1-5386-0550-9.

136. GHAZVINI, A., SHUKUR, Z., HOOD, Z. Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education. In: *International Journal of Advanced Computer Science and Applications*. 2018, vol. 9, no. 8. DOI: 10.14569/ IJACSA. 2018.090853. ISSN: 2158-107X.

137. SUWITO, M. H., et al. An Analysis of IT Assessment Security Maturity in Higher Education Institution. In: *International Conference on Information Science and Applications, ICISA 2016 – Minh*. 2016, vol. 376, pp. 701-713. DOI: 10.1007/978-981-10-,0557-2_69. ISBN 978-981-10-0556-5.

138. CHEUNG, S. K. S. Information Security Management for Higher Education Institutions. In: *Advances in Intelligent Systems and Computing*. 2014, vol 297. DOI: 10.1007/978-3-319-07776-5_2. ISSN 2194-5357.

139. ZENG, Y., et al. Information system and management for campus safety. In: *EM-GIS '19: Proceedings of the 5th ACM SIGSPATIAL International Workshop on the Use of GIS in Emergency Management*. Nov. 2019, pp.1-6. DOI: 10.1145/3356998.3365760. ISBN 9781450369657.

140. SANCHEZ-PUCHOL, F., PASTOR-COLLADO, J. A., BORRELL, B. Towards an Unified Information Systems Reference Model for Higher Education Institutions. In: *Procedia Computer Science.* Jan. 2017, vol. 121, pp. 542–553. DOI: 10.1016/j.procs.2017.11.072. ISSN: 1877-0509.

141. MANTRA, I. G. N., et al. Web vulnerability assessment and maturity model analysis on Indonesia higher education. In: *Procedia Computer Science*. Jan. 2019, vol. 161, pp. 1165–1172. DOI: 10.1016/j.procs.2019.11.229. ISSN: 1877-0509.

142. ZULAZEZE, S., et al. Implementing IT Security Penetration Testing in Higher Education Institute. In: *Australian Journal of Basic and Applied Sciences*. 2014, vol. 8(21), pp. 67–72. ISSN: 1991-8178.

143. BIANCHI, I. S., SOUSA, R. D. IT Governance Mechanisms in Higher Education. In: *Procedia Computer Science.* 2016, vol. 100. DOI: 10.1016/j.procs.2016.09.253. ISSN: 1877-0509.

144. HINA, S., PANNEER, D., SELVAM, D., LOWRY, P. B. Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. In: *Computer Secur*ity. Nov. 2019, vol. 87, p. 101594. DOI: 10.1016/j.cose.2019.101594. ISSN: 0167-4048.

145. AGRAWAL, B., JAIN, A. Missing Values Prediction for Cyber Vulnerability Analysis in Academic Institutions. In: *International Journal of Computer Applications*. 2018, vol. 180, no. 43. DOI: 10.5120/ijca2018917129. ISBN: 973-93-80898-69-1.

146. ANANTHI CLARAL MARY, T., ARUL LEENA ROSE, P.J. Implications, Risks And Challenges Of Cloud Computing In Academic Field – A State-Of-Art. In: *International Journal of Scientific & Technology Research.* 2019, vol. 8, no. 12, pp. 3268–3278. ISSN 2277-861.

147. LIU, C.-W., HUANG, P., LUCAS, H. C. Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. In: *Journal of Management*

Information Systems. 2020, vol. 37, no. 3. DOI: 10.1080/07421222.2020.1790190. ISSN: 0742-1222.

148. GULTOM, H. C., et al. Sixware Cybersecurity Framework Development To Protect Defense Critical Infrastructure And Military Information Systems. In: *International Journal of Scientific & Technology Research*. 2021. ISSN 2277-8616.
149. XINLI, Li. The Design of Information Security Management System in College. In: *Proceedings of the American Society for Composites–Thirty-Sixth Technical Conference on Composite Materials*. 2016. ISBN: 978-1-60595-393-9.
150. GUNAWAN, I. Analysis And Implementation Of Operational Security Management On Computer Center At The University X. In: *CCE 2014*.
151. PEREIRA, C., FERREIRA, C., AMARAL, L. An IT value management capability model for Portuguese universities: A Delphi study. In: *Procedia Computer Science*. Jan. 2018, vol. 138, pp. 612–620. DOI: 10.1016/j.procs.2018.10.082. ISSN 1877-0509.
152. ELGELANY, A., GAOUD, W. Cloud Computing: Empirical Studies in Higher Education A Literature Review. In: *International Journal of Advanced Computer Science and Applications.* 2017, vol. 8, no. 10, pp. 121–127. DOI: 10.14569/ IJACSA. 2017. 081 017. ISSN: 2158-107X.
153. NOWAK, G. J. Information Security Management with accordance to ISO27000 Standards: Characteristics, implementations, benefits in global Supply Chains. In: *Logistyka*. 2015, pp. 639–654. ISSN 1231-5478.
154. HAUFE, K., et al. ISMS Core Processes: A Study. In: *Procedia Computer Science*. 2016, vol. 100, pp. 339–346. DOI: 10.1016/J.PROCS.2016.09.167. ISSN: 1877-0509.
155. ASOSHEH, A., HAJINAZARI, P., KHODKARI, H. A practical implementation of ISMS. In: *7th International Conference on e-Commerce in Developing Countries:with focus on e-Security*. 2013, pp 1-17. DOI: 10.1109/ECDC.2013.6556730. ISBN:978-1-4799-0394-8.
156. DISTERER, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. In: *Journal of Information Security*. 2013, vol. 04, no. 02. DOI: 10.4236/jis.2013.42011. ISSN: 2153-1234.
157. WOLDEN, M., VALVERDE, R., TALLA, M. The effectiveness of COBIT 5 information security framework for reducing cyber-attacks on supply chain management system. In*: IFAC-PapersOnLine*. 2015, vol. 28, no. 3, pp. 1846–1852. DOI: 10.1016/j.ifacol.2015.06.355. ISSN: 2405-8963.
158. ISO/IEC 27005: Information technology – Security techniques – Information security risk management. International Organization for Standardization. Geneva, Switzerland, 2018.

159. JOHNSON, L. *Security Controls Evaluation, Testing, and Assessment Handbook*. Elsevier, 2020. DOI: 10.1016/C2018-0-03706-8. ISBN 978-0-12-818427-1.

160. NADIG, D., RAMAMURTHY, B. Securing Large-scale Data Transfers in Campus Networks. In: *SDN-NFVSec '19: Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization.* 2019, pp. 29–32, 2019. DOI: 10.1145/3309194.3309444. ISBN 9781450361798.

161. MISHIMA, K. Secure Campus Network System with Automatic Isolation of High Security Risk Device. In: *SIGUCCS '18: Proceedings of the 2018 ACM SIGUCCS Annual Conference*. 2018, pp. 107–110. DOI: 10.1145/3235715.3235738. ISBN 9781450355827.

162. TSUNODA, H., KEENI, G. M. Security by simple network traffic monitoring. In: *SIN '12: Proceedings of the Fifth International Conference on Security of Information and Networks*. 2012, pp. 201–204. DOI: 10.1145/2388576.2388608. ISBN 9781450316682.

163. ISNIAH, S., HARDI PURBA, H., DEBORA, F. Plan do check action (PDCA) method: literature review and research issues. In: *Jurnal Sistem dan Manajemen Industri*. 2020, vol. 4, no. 1, pp. 72–81. DOI: 10.30656/jsmi.v4i1.2186. ISSN: 2580-2887.

164. *IT-Grundschutz Compendium Edition 2021*. Federal Office for Information Security. [citat 13.11.2021]. Disponibil: https://www.bsi.bund.de/EN/Topics/ITGrundschutz /itgrundschutz _node.html

165. *National Cyber Security Center*. [citat 02.12.2021] Disponibil: https://www.ncsc.gov. uk/ (accessed Aug. 29, 2021).

166. BECKERS, K., et al. Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation. In: *2012 Seventh International Conference on Availability, Reliability and Security*. 2012, pp. 242–248. DOI: 10.1109/ARES.2012.35. ISBN:978-1-4673-2244-7.

167. REHMAN, S., GRUHN, V. An Effective Security Requirements Engineering Framework for Cyber-Physical Systems. In: *Technologies (Basel*). 2018, vol. 6, no. 3, p. 65. DOI: 10.3390 /technologies6030065. ISSN 2227-7080.

168. REHMAN, S. *Security requirements engineering: a framework for cyber-physical systems*. Essen, 2020. DOI: https://doi.org/10.17185/duepublico/71232.

169. SKINNER, R., et al. The Delphi .Method Research Strategy in Studies of Information Systems. In: *Communications of the Association for Information Systems*. 2015, vol. 37. DOI: 10.17705 /1CAIS.03702. ISSN: 1529-3181.

170. POWELL, C. The Delphi technique: myths and realities. In: *Journal of Advanced Nursing.* 2003, vol. 41, no. 4. DOI: 10.1046/j.1365-2648.2003.02537.x. ISSN: 0309-2402.

171. VENABLE, J., PRIES-HEJE, J. BASKERVILLE, R. FEDS: a Framework for Evaluation in Design Science Research. In: *European Journal of Information Systems*. 2016, vol. 25, no. 1, pp. 77–89. DOI: 10.1057/ejis.2014.36. ISSN: 0960-085X.

172. WIERINGA, R. J. *Design Science Methodology for Information Systems and Software Engineering*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. DOI: 10.1007/978-3-662-43839-8. ISBN: 978-3-662-43838-1.

173. MYERS, M. D. NEWMAN, M. The qualitative interview in IS research: Examining the craft. In: *Information and Organization*. 2007, vol. 17, no. 1. DOI: 10.1016/j.infoandorg. 2006.11.001. ISSN: 1471-7727

174. SYKES, F., GANI. Statistical terms Part 1: The meaning of the MEAN, and other statistical terms commonly used in medical research. In: *South African Dental Journal*. 2016, vol. 71, pp. 274–278. ISSN 2519-0105.

175. ARKKELIN, D. L. Using SPSS to Understand Research and Data Analysis. In: *Psychology Curricular Materials 1*. 2014.

176. HOFFMAN, L.J., CLEMENTS, D. *Fuzzy computer security metrics: a preliminary report*. Berkeley, 1977.

177. YESIN, V., et al. Technique for Evaluating the Security of Relational Databases Based on the Enhanced Clements–Hoffman Model. In: *Applied Sciences*, vol. 11, no. 23, p. 11175, Nov. 2021. DOI: 10.3390/app112311175. ISSN: 20763417.

178. JOHNSON, L. Cybersecurity framework. In: *Security Controls Evaluation, Testing, and Assessment Handbook*. 2020, pp. 537–548. DOI: 10.1016/B978-0-12-818427-1.00012-4. ISSN 23198613.

179. HOROWITZ, B. M. Policy Issues Regarding Implementations of Cyber Attack: Resilience Solutions for Cyber Physical Systems. In: *AAAI Spring Symposium - Technical Report*. 2019, pp. 87–100. DOI: 10.1016/B978-0-12-817636-8.00005-3. ISBN 978-0-12-817636-8.

180. DONALDSON, S. E., et al. Cybersecurity Frameworks. In: *Enterprise Cybersecurity, Berkeley,* CA: Apress. 2015. DOI: 10.1007/978-1-4302-6083-7_17. ISBN: 978-1-4302-6082-0.

181. KOONG, K., YUNIS, M. Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework. In: *AMCIS*. 2015. ISSN: 2010-3654.

182. MERCHAN-LIMA, J. et al. Information security management frameworks and strategies in higher education institutions: a systematic review. In: *Annals of Telecommunications*. Jul. 2020. DOI: 10.1007/s12243-020-00783-2. ISSN: 0003-4347.

183. OLTRAMARI, A. et al. General Requirements of a Hybrid-Modeling Framework for Cyber Security. In: *2014 IEEE Military Communications Conference*. 2014, pp. 129-135. DOI: 10.1109/MILCOM.2014.28. ISSN: 2155-7578.
184. Cardoso, L. S. Quality and security usability. In: *ITU-T Wksp. End-to-End QoE/QoS*, 2006.
185. IRVINE, C., LEVIN, T. Quality of security service. In: *Proceedings of the 2000 workshop on New security paradigms - NSPW '00, 2000*, pp. 91–99. DOI: 10.1145/366173.366195. ISBN 1581132603.
186. PANIGRAHI, A., PATRA, M. R. Network Intrusion Detection Model Based on Fuzzy-Rough Classifiers. In: *Handbook of Neural Computation*, Elsevier, 2017, pp. 109–125. DOI: 10.1016/B978-0-12-811318-9.00006-5. ISBN 978-0-12-811318-9.
187. ZADEH, L. A. Fuzzy sets. In: *Information and Control*, vol. 8, no. 3, pp. 338–353, Jun. 1965. DOI: 10.1016/S0019-9958(65)90241-X. ISSN 0019-9958.
188. BOJADZIEV, G., BOJADZIEV, M. *Fuzzy Sets, Fuzzy Logic, Applications*. World Scientific, vol. 5, 1996. DOI: 10.1142/2867. ISBN: 978-981-02-2606-0.
189. GUŢULEAC, E., ZAPOROJAN, S., MORARU, V., SCLIFOS, A. Performance modeling of network defense in breadth systems by matrix rewriting srn with fuzzy parameters. In: *Journal of Engineering Science*, vol. XXVI, no. 3, pp. 38–53, 2019. ISSN 2587-3474.
190. ANDERSON, C., BASKERVILLE, R. L., KAUL, M. Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. In: *Journal of Management Information Systems*, vol. 34, no. 4, pp. 1082–1112, Oct. 2017. DOI: 10.1080/07421222.2017.1394063. ISSN: 0742-1222.
191. SZCZEPANIUK, E. K., et al. Information security assessment in public administration. In: *Computers and Security*. 2020, vol. 90, p. 101709. DOI: 10.1016/ j.cose.2019. 1017 09. ISSN 0167-4048.
192. RYTOV, M., et al. Security policy development for small business using an automated system. In: *Automation and modeling in design and management*, vol. 2019, no. 3, pp. 9–18, Nov. 2019. DOI: 10.30987/article_5d8d113d6e9f18.01574772. eISSN: 2658-6436.
193. JABAREEN, Y. Building a Conceptual Framework: Philosophy, Definitions, and Procedure. In: *International Journal of Qualitative Methods*. 2009, vol. 8, no. 4. DOI: 10.1177/160940690900800406. ISSN 1609-4069.
194. ADOM, D. HUSSEIN, E. AGYEM, J. A. Theoretical and Conceptual Framework: Mandatory Ingredients of a Quality Research. In: *International Journal of Scientific Research*. 2018, vol. 7. ISSN 2277 – 8179.

195. FISHER, C. “Researching and Writing a Dissertation: a guidebook for business students”, 2007. ISBN 0273710079.
196. **ALEXEI, Arina.** Design & Development of a Cyber Security Conceptual Framework for Higher Education Institutions in the Republic of Moldova. In: *Scientific and Practical Cyber Security Journal (SPCSJ)*. 2022, vol. 6(1), pp. 35–52. ISSN 2587-4667.
197. “Senatul Universitar.” [citat 10.06.2021]. Disponibil: https://utm.md/administratia / senatul/ (accesat Oct. 07, 2021).
198. *Strategia Securității Informaționale a RM pentru perioada 2019-2024*. Parlamentul RM. [citat 07.10.2021]. Disponibil: chrome-extension://efaidnbmnnnibpcajpcglclefind mkaj/ viewer.html?pdfurl=https%3A%2F%2Fgov.md%2Fsites%2Fdefault%2Ffiles%2F document%2Fattachments%2Fintr23_86.pdf.
199. SHOJAIE, B. *Implementation of information security management systems based on the ISOIEC 27001 standard in different cultures*. 2018.
200. MAYNARD, S. B. ONIBERE, M., AHMAD, A. Defining the Strategic Role of the Chief Information Security Officer. In: *Pacific Asia Journal of the Association for Information Systems*. 2018. DOI: 10.17705/1pais.10303. ISSN 1943-7536.
201. DILLEN, Y., et al. From ‘manager’ to ‘strategist. In: *International Journal of Entrepreneurial Behavior & Research*. 2019, vol. 25, no. 1. DOI: 10.1108/IJEBR-01-2017-0010. ISSN: 1355-2554.
202. REEGÅRD, K., BLACKETT, C., KATTA, V. The Concept of Cybersecurity Culture. In: *29th European Safety and Reliability Cnference (ESREL)*. 2019. DOI: 10.3850/978-981-11-2724-3_0761-cd. ISBN: 978-981-11-2724-3.
203. HARKINS, M. W. The 21st Century CISO. In: *Managing Risk and Information Security* Berkeley, CA: Apress, 2016. DOI: 10.1007/978-1-4842-1455-8_10. ISBN 978-1-4842-1456-5.
204. PÄÄKKÖNEN, P., PAKKALA, D. Reference Architecture and Classification of Technologies, Products and Services for Big Data Systems. In: *Big Data Research*. 2015, vol. 2, no. 4, pp. 166–186. DOI: 10.1016/J.BDR.2015.01.001. ISSN: 2214-5796.
205. ANGELOV, S., GREFEN, P., GREEFHORST, D. A framework for analysis and design of software reference architectures. In: *Information and Software Technology*. 2012, vol. 54, no. 4, pp. 417–431. DOI: 10.1016/j.infsof.2011.11.009. ISSN: 0950-5849.
206. SVENSSON, C., HVOLBY, H.-H. Establishing a Business Process Reference Model for Universities. In: *Procedia Technology*. 2012, vol. 5, pp. 635–642. DOI: 10.1016/j.protcy.2012.09.070. ISSN: 2212-0173.

207. IVANOV, V., et al. Securing the Core University Business Processes. In: *Camenisch, J., Kisimov, V., Dubovitskaya, M. (eds) Open Research Problems in Network Security. iNetSec 2010. Lecture Notes in Computer Science.* Springer, Berlin, Heidelberg. 2011, vol 6555, pp. 104–116. DOI: 10.1007/978-3-642-19228-9_9. ISBN 978-3-642-19227-2

208. STAUNTON, C., SLOKENBERGA, S., MASCALZONI, D. The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. In: *European Journal of Human Genetics*. 2019, vol. 27, no. 8, pp. 1159–1167. DOI: 10.1038/s41431-019-0386-5. ISSN: 1018-4813.

209. SAVOLA, R. M. Quality of security metrics and measurements. In: *Computer Security*, vol. 37, pp. 78–90, Sep. 2013. DOI: 10.1016/j.cose.2013.05.002. ISSN 0167-4048.

210. WANG, A. J. A. Information security models and metrics. In: *Proceedings of the 43rd annual southeast regional conference on - ACM-SE 43*, 2005, p. 178. DOI: 10.1145/1167253. 1167295. ISBN 1595930590.

211. ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls. International Organization for Standardization. Switzerland. 2013.

212. FLOWERDAY, S., TUYIKEZE, T. Information security policy development and implementation: The what, how and who. In: *Computers & Security*. 2016, vol. 61. DOI: 10.1016/j.cose.2016.06.002. ISSN 0167-4048.

213. *Implementation Guideline ISO/IEC 27001:2013*. ISACA, Germany Chapter. Oberwallstr. Berlin, 2017.

214. HARIYANTI, E., DJUNAIDY, A., SIAHAAN, D. O. A Conceptual Model for Information Security Risk Considering Business Process Perspective. In: *2018 4th International Conference on Science and Technology (ICST)*. Aug. 2018. DOI: 10.1109/ICSTC. 2018. ISBN:978-1-5386-5814-7.

215. ROJAS, O. G., LESMES, S. Value at Risk Within Business Processes: An Automated IT Risk Governance Approach. In: *International Conference on Business Process Management*. 2016. DOI: 10.1007/978-3-319-45348-4_21. ISBN 978-3-319-45347-7.

216. BULAI, R., BESLIU, V. Methodologies and Tools of Information Security Risk Management. In: *Information Technologies and Security*, 2012, pp. 62–70. ISSN 1313-8251.

217. AHMED, N., MATULEVIČIUS, R. Securing business processes using security risk-oriented patterns. In: Computer Standards & Interfaces. 2014, vol. 36, no. 4, pp. 723–733. DOI: 10.1016/j.csi.2013.12.007. ISSN: 0920-5489.

218. KHANMOHAMMADI, K., HOUMB, S.H. Business Process-Based Information Security Risk Assessment. In: *2010 Fourth International Conference on Network and System Security*, Sep. 2010, pp. 199–206. DOI: 10.1109/NSS.2010.37. ISBN:978-1-4244-8484-3.

219. JAKOUBI, S., TJOA, S., GOLUCH, S., KITZLER, G. Risk-Aware Business Process Management—Establishing the Link Between Business and Security. In: *Xhafa, F., Barolli, L., Papajorgji, P. (eds) Complex Intelligent Systems and Their Applications*. Springer Optimization and Its Applications, vol 41. Springer, New York, NY.2010, pp. 109–135. DOI: 10.1007/978-1-4419-1636-5_6. ISBN 978-1-4419-1635-8.

220. GOETTELMANN, E., et al. A Security Risk Assessment Model for Business Process Deployment in the Cloud. In: *2014 IEEE International Conference on Services Computing*. Jun. 2014, pp. 307–314. DOI: 10.1109/SCC.2014.48. ISBN:978-1-4799-5066-9.

221. FIKRI, M., et al. Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. In: *Procedia Computer Science*. 2019, vol. 161, pp. 1206–1215. DOI: 10.1016/J.PROCS.2019.11.234. ISSN: 1877-0509.

222. ULVEN, J. B., WANGEN, G. A Systematic Review of Cybersecurity Risks in Higher Education. In: *Future Internet*, vol. 13, no. 2, p. 39, Feb. 2021. DOI: 10.3390/fi13020039. ISSN 19995903.

223. SUH, B., HAN, I. The IS risk analysis based on a business model. In: *Information & Management*. 2003, vol. 41, no. 2, pp. 149–158. DOI: 10.1016/S0378-7206(03)00044-2. ISSN 0378-7206.

224. BOLUN, I. Prioritization of Cybersecurity Measures. In: *The 11th International Conference on Electronics, Communications and Computing.* 2021, pp. 194–199. ISBN 978-9975-45-776-7.

225. MORARU, V., GUŢULEAC, E., CĂRBUNE, V. Active learning of networking in the GNS3 virtualized environment. In*: International Conference on Electronics, Communications and Computing*, 2019, p. 75. ISBN 978-9975-108-84-3.

226. TOVAL, A., et al. Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach. In: *Requirements Engineering*. 2002, vol. 6, no. 4, pp. 205–219. DOI: 10.1007/PL00010360. ISSN: 0947-3602.

227. JACKSON, P. From space to function. In: *Web 2.0 Knowledge Technologies and the Enterprise*. 2010, pp. 137–154. DOI: 10.1016/B978-1-84334-537-4.50005-3. ISBN 978-1-84334-537-4.

228. IIVARI, J. A Paradigmatic Analysis of Information Systems As a Design Science. In: *Scandinavian Journal of Information Systems*. 2007, vol. 19, p. 5. ISSN 1901-0990.

229. SHRESTHA, A., CATER-STEEL, A., TOLEMAN, M. A. How to communicate evaluation work in design science research? An exemplar case study. In: *25th Australasian Conference on Information Systems*. 2014. ISBN: 978-1-927184-26-4.

230. OLIVERO, M. A., et al. A Delphi study to recognize and assess systems of systems vulnerabilities. In: *Information and Software Technology*. 2022, vol. 146. DOI: 10.1016/J. INFSOF.2022.106874. ISSN 0950-5849.

231. LILJA, K, LAAKSO, K., PALOMÄKI, J. Using the Delphi method. In: *Proceedings of PICMET '11: Technology Management in the Energy Smart World (PICMET).* 2011, pp. 1–10. ISBN 978-1-890843-24-5.

232. ROWE, G., WRIGHT, G. Expert Opinions in Forecasting: The Role of the Delphi Technique. In: *Armstrong, J.S. (eds) Principles of Forecasting. International Series in Operations Research & Management Science*, vol 30. Springer, Boston, MA.2001. DOI: 10.1007/978-0-306-47630-3_7. ISBN 978-0-7923-7401-5.

233. BALDWIN, A. A., TRINKLE, B. S. The Impact of XBRL: A Delphi Investigation. In: *The International Journal of Digital Accounting Research*. 2011, vol. 11. DOI: 10.4192/1577-8517-v11_1. ISSN: 1577-8517.

234. WORRELL, J. L., GANGI, P. M., BUSH, A. A. Exploring the use of the Delphi method in accounting information systems research. In: *International Journal of Accounting Information Systems.* 2013, vol. 14, no. 3. DOI: 10.1016/j.accinf.2012.03.003. ISSN: 1467-0895.

235. NURMAHMUDAH, E., NURYUNIARTI, R. Google forms utilization for student satisfaction survey towards quality of service at Universitas Muhammadiyah Tasikmalaya. In: *Journal of Physics: Conference Series.* 2020, vol. 1477, no. 2, p. 022003. DOI: 10.1088/1742-6596/1477/2/022003. ISSN 1742-6596.

236. JOSHI, A. S., et al. Likert Scale: Explored and Explained. In: *British Journal of Applied Science & Technology*. 2015, vol. 7, no. 4, pp. 396–403. DOI: 10.9734/ BJAST /2015 / 14975. ISSN: 2231-0843.

237. ALI, Z., BHASKAR, SB. Basic statistical tools in research and data analysis. In: *Indian Journal of Anaesthesia*. 2016, vol. 60, no. 9, p. 662. DOI: 10.4103/0019-5049.190623. ISSN: 0019-5049.

238. MUKASA, E. S., et al. The Effects of Parametric, Non-Parametric Tests and Processes in Inferential Statistics for Business Decision Making
—A Case of 7

Selected Small Business Enterprises in Uganda. In: *Open Journal of Business and Management*. 2021, vol. 09, no. 03, pp. 1510–1526. DOI: 10.4236/ojbm.2021.93081. ISSN: 2329-3284.

239. *Inferential Statistics*. In: The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation, 2455 Teller Road, Thousand Oaks, California 91320: SAGE Publications, Inc., 2018. DOI: 10.4135/9781506326139.n325.
240. COVACI, M. Applied_statistics_in_psychology. 2020. DOI: 10.5281/zenodo.4106953.
241. LEGENDRE, P. Species associations: the Kendall coefficient of concordance revisited. In: *Journal of Agricultural, Biological, and Environmental Statistics*. 2005, vol. 10, no. 2, pp. 226–245. DOI: 10.1198/108571105X46642. ISBN 978-3-902938-52-7.
242. KENDALL, M. G., SMITH, B. B. The Problem of m Rankings. In: *The Annals of Mathematical Statistics*. 1939, vol. 10, no. 3, pp. 275–287. DOI: 10.1214/aoms/1177732186.
243. MOSLEM, S., et al. Analysing Stakeholder Consensus for a Sustainable Transport Development Decision by the Fuzzy AHP and Interval AHP. In: *Sustainability*. 2019, vol. 11, no. 12, p. 3271. DOI: 10.3390/su11123271. ISSN: 2071-1050.

ANEXE

Anexa 1. Publicații științifice ale autorului

Nr. d/o	Articole științifice publicate	Referința în teză
1	**ALEXEI, Ar.**, ALEXEI, An. The difference between cyber security vs information security. În: *Journal of Engineering Science*, Volumul XXIX, no. 4 (2022), pp. 72 – 83. DOI: https://doi.org/10.52326/jes.utm.2022.29(4).08.	[2]
2	**ALEXEI, Ar.**, NISTIRIUC, P., ALEXEI, An. THE HOLISTIC APPROACH TO CYBERSECURITY IN ACADEMIA. În lucrările conferinței: *Central and Eastern European e|Dem and e|Gov Days 2022*. ACM. Budapesta, Ungaria.	[10]
3	**ALEXEI, Ar.**, ALEXEI, An. Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning. În: *International Journal of Scientific & Technology Research*, Volumul 10, Numărul 3, martie 2021, pag. 128-133. ISSN: 2277-8616.	[46]
4	**ALEXEI, A.** Network Security Threats to Higher Education Institutions. In: *Central and Eastern European e|Dem and e|Gov Days 2021*. Budapesta: National University of Public Service, 16-17 september 2021, pp. 323–333. ISBN: 978-3-903035-30-0. ISSN: 2520-3401. DOI: https://doi.org/10.24989/ocg.v341.24.	[47]
5	**ALEXEI, Ar.**, ALEXEI, An. Analysis of IoT security issues used in Higher Education Institutions. In: *International Journal of Mathematics and Computer Research*, Vol. 09, No. 5, 2021, pp. 2277-2286. DOI: https://doi.org/10.47191 /ijmcr/v9i5.01.	[55]
6	**ALEXEI, A.** Cyber Security Strategies For Higher Education Institutions. In: *Journal of Engineering Science*, Vol. XXVIII, No 4, pp.74–92. ISSN 2587-3474. DOI: https://doi.org/10.52326/jes.utm.2021.28(4). 07.	[86]
7	**ALEXEI, Ar.**, NISTIRIUC, P., ALEXEI, An. Empirical Study of Cyber Security Threats in Moldovan Higher Education Institutions. In: *The 12th International Conference on Electronics, Communications and Computing.* Chișinău: UTM, 20-21 october 2021. ISBN 978-9975-45-776-7.	[100]
8	**LACHI, Arina**, SOROCHIN, S. Analiza modelelor de detecție a intruziunilor moderne. În lucrările conferinței: 6th International Conference "Telecommunications, Electronics and Informatics" ICTEI 2018. 24-27 mai 2018, pp. 470-472, Chișinău, Moldova.	[102]
9	**ALEXEI, A.** Using Design Science Research Method to Develop a Cyber Security Framework for HEIs in Moldova. In: *The 12th International Conference on Electronics, Communications and Computing*. Chișinău: UTM, 20-21 october 2021. ISBN 978-9975-45-776-7.	[119]
10	**ALEXEI, A.** Ensuring Information Security in Public Organizations in the Republic of Moldova through the ISO 27001 Standard. In: *Journal of Social Sciences*, Vol. IV, No. 1, march 2021, pp. 84-94. ISSN 2587-3490. DOI: https://doi.org/10.52326/jss.utm.2021.4(1).11.	[98]
11	**ALEXEI, A.** Design & Development of a Cyber Security Conceptual Framework for Higher Education Institutions in the Republic of Moldova. In: *Scientific and Practical Cyber Security Journal (SPCSJ)*, Vol. 6, No. 1, march 2022, pp. 35–52. ISSN 2587-4667.	[196]

Anexa 2. Active de suport universitare bazate pe CE

Active de suport				
Echipamente terminale	**Software**	**Rețea și comunicații**	**Personal**	**Infrastructură**
Server	VMWare Virtualizare	Switch	Personal didactic	Camera serverelor
Desktop PC	Windows Server	Ruter	Personal non-didactic	Birou
Laptop	Linux Server	Punct de acces	Studenți	Birou de acasă
Smartphone	Container date	Gateway VPN	Direcția TIC	Birou mobil
Tablete	Sistem de stocare centralizat	VOIP		Clădire
Medii amovibile	Server Web	LAN/VLAN		Săli de curs, laboratoare
	Server DNS	Firewall		UPS
	LDAP			Generator
	Radius			Medii de conexiune
	Server Fișiere			Centru de date
	Server Email			Surse de alimentare
	Server DHCP			Aer condiționat
	SSL VPN			
	L2TP VPN			
	Server NTP			

Sursa: elaborat de autor ca rezultat al interviurilor cu specialiștii din IÎS naționale.

Anexa 3. Amenințări generice și specifice de securitate

Tabelul A3.1. Lista de verificare a amenințărilor generice de securitate

Amenințări generice de securitate					
Nr.	**Tip**	**Nr.**	**Amenințarea**	**Valoare de bază Confidențialitate (C), Integritate (I), Disponibilitate (D)**	**Origine Accidental (A), Intenționat (I), Mediu (M)**
1	Daune fizice	1	Focul	D	A,I,M
		2	Apa	I,D	A,I,M
		3	Pământ, praf, coroziune	I,D	A,I,M
		4	Distrugerea dispozitivelor sau a mediilor de date	D	A,I,M
		5	Evenimente majore în mediu	C,I,D	A,I,M
2	Evenimente naturale	6	Condiții meteo nefavorabile	I,D	M
		7	Inundații	D	M
		8	Catastrofe de mediu	D	A,I,M
		9	Război	C,I,D	I
3	Pierderea serviciilor esențiale	10	Întreruperea sau funcționarea defectuoasă a sursei de alimentare	I,D	A,I,M
		11	Defecțiunea sau disfuncționalitatea rețelelor de alimentare	D	A,I
		12	Defecțiunea sau disfuncționalitatea furnizorilor de servicii	C,I,D	A,I,M
		13	Defecțiunea sau disfuncționalitatea rețelelor de comunicații	I,D	A,I
		14	Lipsa resurselor	D	A, I
4	Perturbări din cauza radiației	15	Interferența electromagnetică	I,D	A,I,M
		16	Interceptarea radiației compromițătoare	C	A,I,M
5	Compromiterea informației	17	Planificarea slabă sau lipsa de ajustare	C,I,D	A,I
		18	Interceptarea informației/Spionaj	C	I
		19	Dezvăluirea informațiilor care ar trebui protejate	C	I
		20	Informații din surse nesigure	C,I,D	A,I
		21	Manipularea informațiilor	I	I
		22	Utilizarea sau administrarea incorectă	C,I,D	A

			a dispozitivelor și sistemelor		
		23	Pierderea datelor	D	I,A
		24	Pierderea integrității informațiilor care ar trebui protejate	I	A,I
6	Defecțiuni tehnice	25	Dispozitive sau sisteme nefuncționale	D	A
		26	Defecțiunea dispozitivelor sau a sistemelor	C,I,D	A
		27	Vulnerabilități sau erori software	C,I,D	A
		28	Pierderea dispozitivelor, suporturilor de date și a documentelor	C,D	A,I
7	Acțiuni neautorizate	29	Furt de identitate	C,I,D	I
		30	Coerciție, extorcare sau corupție	C,I,D	I
		31	Utilizarea incorectă a datelor cu caracter personal	C	I,A
		32	Repudierea acțiunilor	C,I	I
		33	Intrare neautorizată în încăperi	C,I,D	I
		34	Utilizarea incorectă a autorizațiilor	C,I,D	I
		35	Utilizarea sau administrarea neautorizată a dispozitivelor și sistemelor	C,I,D	I
		36	Utilizarea sau administrarea incorectă a dispozitivelor și sistemelor	C,I,D	I
		37	Încălcarea legilor sau a contractelor	C,I,D	I
		38	Acces neautorizat în sistemele IT	C,I	I
		39	Importul mesajelor	C,I	I
		40	Manipularea hardware-ului sau software-ului	C,I,D	I
		41	Furt de dispozitive, suporturi de date și documente	C,D	I
		42	Atacul cibernetic	C,I,D	I
		43	Sabotajul	D	I
8	Compromiterea serviciilor	44	Programe malițioase	C,I,D	I
		45	Refuzul serviciilor (Denial of Service)	D	I
		46	Inginerie socială	C,I	I

Tabelul A3.2. Lista de verificare a amenințărilor specifice de securitate

Amenințări specifice de securitate		
Categorie active	**Active de suport**	**Amenințări/vulnerabilități specifice importante**
Echipamente terminale	Server	• Utilizarea sau administrarea incorectă a dispozitivelor și sistemelor • Pierderea datelor • Dispozitive sau sisteme nefuncționale • Defecțiunea dispozitivelor sau a sistemelor • Atacul cibernetic • Programe malițioase • Refuzul serviciilor (Denial of Service)
	Desktop PC	• Programe malware • Pierderea datelor din cauza stocării locale a datelor • Defecte hardware în sistemele client • Utilizarea neautorizată a tehnologiilor TIC • Instalarea componentelor și aplicațiilor inutile ale sistemului de operare • Ascultarea camerelor folosind microfoane și camere • Administrarea sau utilizarea incorectă a dispozitivelor și sistemelor
	Laptop	• Degradarea datorită schimbării mediilor operaționale • Furtul și pierderea laptopurilor • Modificări nereglementate ale utilizatorilor de laptopuri
	Smartphone/Tablete	• Lipsa actualizărilor sistemului de operare • Vulnerabilități software în aplicațiile preinstalate • Manipularea smartphone-lor și tabletelor • Malware pentru smartphone-uri și tablete • Atacurile web asupra browserelor mobile • Folosirea frauduloasă a datelor despre sănătate, fitness sau locație • Folosirea frauduloasă a datelor sensibile de pe ecranul de blocare • Pericole legate de utilizarea privată a smartphone-urilor și tabletelor legate de muncă • Amenințări legate de dispozitivele proprii • Drepturi extinse prin vulnerabilități
Software	VMWare Virtualizare	• Planificare proastă a virtualizării • Configurație proastă a virtualizării • Resurse insuficiente pentru sistemele TIC virtuale • Scurgeri de informații sau blocaje de resurse din cauza instantaneelor • Eșecul serverului de administrare pentru sistemele de virtualizare • Folosirea greșită a instrumentelor pentru oaspeți • Software de virtualizare compromis
	Linux Server	• Colectarea neautorizată a informațiilor despre sistem și utilizator • Exploatarea mediului de script • Încărcarea dinamică a bibliotecilor utilizate în comun • Software din surse terțe

	Windows Server 2012	• Planificare proastă a Windows Server 2012 • Utilizarea neglijentă a cloud-ului • Administrarea necorespunzătoare a serverelor Windows • Utilizarea necorespunzătoare a politicilor de grup (GPO) • Pierderea integrității informațiilor sau proceselor sensibile • Achiziția neautorizată sau utilizarea abuzivă a drepturilor de administrator • Acces la distanță compromis
	Active Directory	• Planificarea inadecvată a limitelor de securitate • Relații de încredere excesive sau neglijente • Lipsa caracteristicilor de securitate din cauza sistemelor de operare mai vechi și a nivelului funcțional al domeniului • Operarea de roluri și servicii suplimentare pe controlere de domeniu • Monitorizarea și documentarea insuficientă a drepturilor delegate • Autentificare nesigură • Conturi de serviciu cu prea multe drepturi sau insuficient de sigure • Utilizarea aceleiași parole de administrator local pe mai multe sisteme TIC
	Sistem de stocare centralizat	• Setări implicite nesigure ale componentelor de stocare • Manipularea datelor prin intermediul sistemului de stocare • Pierderea confidențialității din cauza metodelor de replicare bazate pe stocare • Accesul la informațiile altor clienți folosind falsificarea • Ocolirea separării logice a rețelei • Defecțiunea componentelor soluției de stocare • Obținerea accesului fizic la switch-uri
	Server Web	• Pierderea reputației • Manipularea serverului web • Refuzarea serviciului (DoS) • Pierderea datelor confidențiale • Încălcarea legilor sau reglementărilor • Depanare insuficientă
	Server DNS	• Eroare de server DNS • Lățimea de bandă a liniei inadecvată • Planificarea inadecvată a utilizării DNS • Informații de domeniu incorecte • Configurarea incorectă a unui server DNS • Manipularea DNS • Deturnarea DNS • DNS DoS
	LDAP	• Planificarea inadecvată a OpenLDAP • Separarea inadecvată a accesului offline și online la OpenLDAP
	Server Fișiere	• Eroare server de fișiere • Caracteristici insuficiente ale serverului de fișiere • Verificarea insuficientă a fișierelor stocate • Conceptul de autorizare de acces insuficient • Stocarea de date nestructurată

		• Pierderea datelor stocate pe serverele de fișiere • Ransomware
	SSL VPN	• Planificarea inadecvată a utilizării VPN • Furnizori de servicii VPN nesiguri • Configurarea nesigură a clienților VPN pentru acces la distanță • Setări implicite nesigure pentru componentele VPN
	Server Email general	• Planificarea insuficientă a utilizării e-mailului • Configurarea incorectă a clienților și serverelor de e-mail • Nesiguranța e-mailului • Programe malware în e-mailuri • Inginerie socială • Citirea și manipularea e-mail-urilor
	Microsoft Exchange Server și Outlook	• Reguli insuficiente pentru Exchange și Outlook • Migrarea incorectă a Exchange • Acces inadmisibil de browser la Exchange • Conectarea neautorizată a altor sisteme la Exchange • Administrarea necorespunzătoare a site-ului și a drepturilor de acces la date în Exchange și Outlook • Configurarea incorectă a Exchange • Configurarea necorespunzătoare a Outlook • Funcționarea defectuoasă și utilizarea greșită a macro-comenzilor interne și a interfețelor de programare în Outlook
Rețea și comunicații	Switch și Ruter	• Refuzul de serviciu distribuit (DDoS) • Manipulare • Configurarea incorectă a unui ruter sau comutator • Planificarea și proiectarea necorespunzătoare • Componente de rețea active incompatibile • Atacuri de impersonare: IP, MAC, ARP • Ascultare în rețea • MitM • Atacuri cu programe malițioase
	LAN, VLAN Arhitectură și Design	• Eșecul sau funcționarea insuficientă a mediilor de comunicație • Acces nesecurizat la rețea • Structurarea inadecvată a rețelei
	LAN, VLAN Management	• Acces neautorizat la componentele centrale de gestionare a rețelei • Acces neautorizat la componentele individuale ale rețelei • Interferențe neautorizate în comunicarea de gestionare a rețelei • Sincronizarea temporală insuficientă a componentelor de gestionare a rețelei
	WLAN Operare	• Eșecul sau întreruperea unei rețele radio • Planificarea inadecvată a utilizării WLAN-ului • Reguli insuficiente privind utilizarea WLAN-ului • Selectarea necorespunzătoare a metodelor de autentificare • Configurarea incorectă a infrastructurii WLAN • Mecanisme de securitate WLAN insuficiente • Interceptarea comunicațiilor WLAN

		• Simularea unui punct de acces fals • Acces LAN neprotejat la punctele de acces
	WLAN Utilizare	• Cunoașterea insuficientă a regulilor și procedurilor • Nerespectarea măsurilor de securitate • Interceptarea comunicațiilor WLAN • Analiza datelor de conectare legate de comunicațiile fără fir • Simularea unui punct de acces fals
	Firewall	• Refuzul de serviciu distribuit (DDoS) • Manipulare • Ocolirea regulilor firewall • Configurarea incorectă și erori în operarea unui firewall
Personal	Personal didactic Personal non-didactic Studenți	• Lipsa de personal • Cunoașterea insuficientă a regulilor și procedurilor • Neatenție în manipularea informațiilor • Calificări insuficiente ale angajaților
Infrastructură	Camera serverelor	• Planificarea incorectă • Controale insuficiente de acces la site • Monitorizarea insuficientă • Aer condiționat insuficient într-un centru de date • Foc • Apă • Protecția insuficientă împotriva efracției • Defecțiunea sursei de alimentare • Contaminare
	Birou	• Acces neautorizat la site • Deteriorări din cauza condițiilor nefavorabile de muncă • Manipulări de către personalul de curățenie, personalul terță parte sau vizitatori • Manipularea sau distrugerea echipamentelor, accesoriilor, informațiilor sau software-ului într-o cameră de birou • Furt • Cabluri expuse
	Birou de acasă	• Reguli insuficiente pentru locurile de muncă de acasă • Acces neautorizat în încăperile sensibile ale unui loc de muncă acasă • Utilizarea defectuoasă a TIC din cauza condițiilor nefavorabile de lucru la locul de muncă la domiciliu • Transport nesigur de fișiere și medii de stocare • Eliminarea necorespunzătoare a suporturilor de stocare și a documentelor • Manipularea sau distrugerea tehnologiilor TIC, accesoriilor, informațiilor sau software-ului la locul de muncă de acasă • Risc mai mare de furt la locul de muncă la domiciliu
	Birou mobil	• Reguli insuficiente pentru locurile de muncă mobile • Degradarea datorită schimbării mediilor operaționale • Manipularea sau distrugerea sistemelor TIC, accesoriilor, informațiilor sau software-ului la un loc de muncă mobil • Întârzieri cauzate de disponibilitate limitată temporar • Transport nesigur de fișiere și medii de stocare

		• Eliminarea necorespunzătoare a suporturilor de stocare și a documentelor • Pierderea confidențialității informațiilor sensibile • Furtul sau pierderea suporturilor de stocare sau a documentelor
	Săli de curs, laboratoare	• Reguli insuficiente • Incompatibilitate între sistemele TIC externe și interne • Amenințări cauzate de vizitatori • Cabluri expuse • Furt • Pierderea confidențialității informațiilor sensibile
	Clădire	• Foc • Fulger • Apă • Riscuri naturale și dezastre • Amenințări în vecinătate • Acces neautorizat • Încălcarea legilor sau reglementărilor • Protecție insuficientă împotriva incendiilor • Defecțiunea sursei de alimentare
	Medii de conexiune	• Arderea cablurilor • Dimensionarea necorespunzătoare a cablurilor • Documentație insuficientă privind cablarea • Distribuitori protejați necorespunzător • Deteriorarea cablului • Fluctuații de tensiune, supratensiune și subtensiune • Utilizarea de benzi de alimentare de calitate scăzută • Conexiuni prin cablu neautorizate • Deteriorarea liniilor • Ascultarea și manipularea cablurilor

Sursa: elaborat de autor în baza standardului ISO 27005, IT - Grundschutz Kompendium, rapoartelor de securitate internaționale și a rezultatelor cercetărilor din capitolul 1 al tezei de doctor.

Anexa 4. Sondajul final

CSSCE evaluare experți

Ca rezultat al cercetărilor a fost elaborat un cadru sistemic de securitate a comunicațiilor electronice CSSCE (framework) pentru a contribui la securitatea CE din instituțiile de învățământ superior din Republica Moldova, prin abordarea sistemică a securității serviciilor electronice academice. Este necesar suportul experților pentru a evalua prototipul CSSCE propus și a-l rafina. Pentru aceasta au fost identificate 7 criterii de valoare (cele 7 întrebări din sondaj).

Sunteți rugați să înregistrați nivelul de acord, după studierea materialului de suport atașat la email, pentru fiecare întrebare din sondaj, după calificativele de mai jos:

1 - Dezacord total

2 - Dezacord

3 - Neutru

4 - De acord

5 - Total de acord

În același timp, pentru întrebările cu calificativul 3 și mai mic, rugăm să oferiți o recomandare de îmbunătățire a prototipului CSSCE.

Orice recomandare este binevenită și va reprezenta o resursă valoroasă pentru îmbunătățirea prototipului CSSCE!!!

Adresă de e-mail *

Adresa dvs. de e-mail

Domeniul de expertiză al Dvs *

Implementarea standardelor de securitate informațională

Administrarea rețelelor de comunicații

Elaborarea politicelor și a strategiilor de securitate informațională

Ofițer de securitate informațională

Expert în cadrul organizațiilor guvernamentale

Manager proiecte

Cercetător din mediul academic

Altele:

Instituția sau organizația în care activați*

Răspunsul dvs.

Stagiul de muncă în domeniu*

1-5 ani

5-10 ani

mai mult de 10 ani

1. Este prototipul CSSCE aplicabil în instituțiile de învățământ superior?*

1 - Dezacord total

2 - Dezacord

3 - Neutru

4 - De acord

5 - Total de acord

2. Sunt identificate fazele de implementare a prototipului CSSCE în mediul universitar?*

1 - Dezacord total

2 - Dezacord

3 - Neutru

4 - De acord

5 - Total de acord

3. Este descris profilul specialistului responsabil de securitate CE?*

1 - Dezacord total

2 - Dezacord

3 - Neutru

4 - De acord

5 - Total de acord

4. Prototipul CSSCE recomandă modalitatea prin care managementul riscului poate fi realizată într-o instituție academică?*

1 - Dezacord total

2 - Dezacord

3 - Neutru

4 - De acord

5 - Total de acord

5. Puteți aprecia prototipul CSSCE ca fiind eficient și că poate contribui la îmbunătățirea securității cibernetice a universităților din RM?*

1 - Dezacord total

2 - Dezacord

3 - Neutru

4 - De acord

5 - Total de acord

6. Este prototipul CSSCE scalabil, poate fi aplicat în orice instituție academică, indiferent de dimensiunea sau complexitatea serviciilor electronice?*

1 - Dezacord total

2 - Dezacord

3 - Neutru

4 - De acord

5 - Total de acord

7. Se conformează prototipul CSSCE standardelor din domeniul securității informaționale pe dimensiunile acoperite?*

1 - Dezacord total

2 - Dezacord

3 - Neutru

4 - De acord

5 - Total de acord

Recomandările Dvs. sau sugestiile de îmbunătățire:

Răspunsul dvs.

Anexa 5. Model Proiect de implementare a CSSCE

Proiect de securizare a serviciilor electronice academice					
Departament/Direcție:		**Manager proiect:**	**Aprobat de:**		**No de referință**
Proces academic:		**Membru 1:**			
Locația PA:		**Membru 2:**	**Semnătura**		
Data:		**Membru 3:**	**Nume:**		
Versiunea:		**Membru 4:**	**Funcție:**		

Obiective și Rezultatele Proiectului			
Obiective		**Rezultate**	
O1.		**R1.**	
O2.		**R2.**	
O3.		**R3.**	
O4.		**R4.**	
O5.		**R5.**	

Active de Suport							
Categorie active	**Active de suport**	**Amenințări/Vulnerabilități comune**	**Amenințări/Vulnerabilități specifice**	**ID-ul riscului**	**Controale Implementate**	**Control Anexa A ISO 27001**	**Comentarii**
Echipamente terminale	Server						
Software	Aplicație						
Rețele și Comunicații	Router						
Personal	Personal didactic						
Infrastructură	Camera serverelor						
					Numărul total active de suport implicate în proiect:		

Costul Implementării Proiectului						
Tipul resursei		**Specificații tehnice/cunoștințe**	**Unități necesare**	**Argumentare**	**Cost**	**Preț**
1	Echipamente terminale					
2	Software					
3	Rețele și Comunicații					
4	Personal					
5	Infrastructură					
				Prețul total pentru implementarea proiectului:		

Sursa: elaborat de autor.

Anexa 6. Politica de utilizare acceptabilă a resurselor TIC universitare

Politica de utilizare acceptabilă a resurselor TIC

Versiune	Responsabil	Contact	Data intrării în vigoare	Ultima actualizare
1.0	Direcția TIC	Chișinău, bd.Ștefan cel Mare și Sfânt168	1 septembrie 2022	1 septembrie 2022

Scopul

Scopul acestei politici de securitate este de a informa toți utilizatorii tehnologiei informației și comunicațiilor (TIC) deținute, furnizate sau gestionate în cadrul Universității XXX cu privire la obligația de a respecta politicile instituționale și cadrul normativ în vigoare pentru utilizarea resurselor TIC universitare.

Domeniul de aplicare

Resursele TIC includ, dar nu se limitează la toate resursele hardware și software deținute și gestionate de XXX, rețelele de comunicații electronice cu fir și wireless, servicii de email și serviciile educaționale electronice. Utilizatorii la care se referă această politică includ, dar nu se limitează la angajați (personal didactic și non-didactic), studenți și vizitatori, care accesează resursele TIC ale universității pentru îndeplinirea misiunii universității de a oferi instruire, cercetare și activități administrative.

Definiții

TIC (tehnologia informației și comunicațiilor) se referă la utilizarea computerelor și a altor echipamente electronice pentru stocarea și trimiterea informațiilor.
Comunicații electronice se referă la orice informație transmisă între anumite părți printr-o linie telefonică sau utilizând conexiunea la internet.
Rețele de comunicații electronice reprezintă sistemele de transmisie, indiferent dacă se bazează sau nu pe o infrastructură permanentă sau pe o capacitate de administrare centralizată și, după caz, echipamente de comutare sau de rutare și alte resurse.
Serviciile electronice sunt serviciile care utilizează tehnologiile informației și comunicațiilor.

Cerințele politicii de securitate

În utilizarea acceptabilă a resurselor, utilizatorii vizați de această politică trebuie să:

- Utilizeze resursele TIC doar în scopuri autorizate, resursele TIC universitare reprezintă un privilegiu;
- Protejeze ID-urile de utilizator, alte mecanisme de autentificare și autorizare și sistemele împotriva utilizării neautorizate, deoarece sunt direct responsabili;
- Acceseze doar informațiile la care au acces autorizat sau care sunt disponibile publicului;
- Utilizeze doar versiuni legale ale resurselor software protejate prin drepturi de autor, în conformitate cu cerințele de licență ale furnizorului;
- Fie atenți în utilizarea resurselor partajate, evitarea monopolizării sistemelor, supraîncărcarea rețelelor cu date excesive, degradarea serviciilor computerului, a timpului de conectare, a spațiului pe disc, a hârtiei de imprimantă, a manualelor sau a altor resurse universitare;
- Stocheze datele confidențiale numai în locații securizate aprobate de universitate;
- Utilizeze dispozitivele proprii conectate la rețelele de comunicații electronice universitare doar în scopurile aprobate de universitate;
- Revizuiască parolele și alte mecanisme de autentificare și autorizare suspectate de compromis;
- Raporteze incidentele de securitate identificate sau suspectate către șeful de laborator, profesor.

În utilizarea acceptabilă a resurselor, persoanele vizate de această politică nu trebuie să:

- Obțină acces la sistemul, fișierele sau datele unei alte persoane fără permisiune;
- Dezvăluie o parolă sau alte mijloace de autentificare și autorizare oricărei alte persoane, chiar și celor care pretind că sunt tehnicieni de asistență TIC (la telefon sau în persoană);
- Utilizeze programe de calculator pentru a descoperi parole sau alte informații utilizate pentru controlul accesului;
- Încerce a ocoli sau submina măsurile de securitate a sistemului sau rețelei universitare;
- Să se angajeze în orice activitate care are scopul de a dăuna sistemelor sau oricărei informații stocate pe acestea, inclusiv, dar care nu se limitează la crearea sau propagarea de programe malware, cum ar fi viruși, viermi sau programe „cal troian"; perturbarea serviciilor; fișiere deteriorate sau efectuarea de modificări neautorizate ale informațiilor universității;
- Realizeze sau utilizeze copii ilegale ale resurselor software, protejate prin drepturi de autor, să stocheze astfel de copii în sistemele TIC universitare sau să le transmită prin rețelele de comunicații universitare;
- Utilizeze e-mail-ul, rețelele sociale sau alte servicii de mesagerie pentru încălcarea legilor sau reglementărilor, sau pentru a hărțui sau intimida o altă persoană, de exemplu, prin difuzarea de mesaje nesolicitate, prin trimiterea în mod repetat de e-mailuri nedorite sau prin utilizarea numelui sau a ID-ului unui alt utilizator;
- Utilizeze resursele de calcul sau de rețea partajate, de exemplu, prin plasarea intenționată a unui program într-o buclă nesfârșită, prin imprimarea unor cantități excesive de hârtie sau prin trimiterea de scrisori în lanț sau de corespondență nesolicitată;
- Stocheze date confidențiale pe unități locale, unități flash sau alte medii portabile sau externe.

Excepții

În cazurile foarte rare în care această politică interferează cu îndeplinirea misiunii universității, studenții, facultatea sau personalul pot solicita o derogare scrisă de la persoana desemnată ca fiind responsabilă.

Încălcarea politicii

Dacă se constată că o persoană încalcă Politica de utilizare acceptabilă, universitatea va lua măsuri disciplinare, inclusiv restricționarea și posibila pierdere a privilegiilor de rețea sau consecințe mai grave, până la inclusiv suspendarea, rezilierea sau expulzarea din universitate.

Documente relevante

Politica de securitate privind protecţia datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale gestionate de IP „XXX".

Anexa 7. Depozit cerințe de securitate ruter/switch

DEPOZIT CERINȚE DE SECURITATE RUTER/SWITCH	
Cerințe de securitate	**Conformitatea cu ISO 27001 (2022)**
Cerințe de securitate de bază	
Configurație de bază sigură a unui ruter/switch Protecția interfețelor de administrare Protecție împotriva atacurilor de fragmentare Acces de urgență la ruter/switch Înregistrarea evenimentelor pe ruter/switch Copii de rezervă regulate Documentație operațională	A.5.9 Inventarierea informației și a altor active importante A.5.10 Utilizarea acceptabilă a informației și a altor active importante A.5.15 Controlul accesului A.5.17 Informații despre autentificare A.5.18 Drepturi de acces A.5.37 Documentarea procedurilor operaționale A.7.1 Perimetre fizice de securitate A.7.3 Securitatea oficiilor, camerelor și a facilităților A7.4 Monitorizarea securității fizice A. 7.5 Protecția împotriva amenințărilor fizice și de mediu A.7.8 Protecția echipamentului A.7.12 Securitatea cablurilor A.7.13 Mentenanța echipamentului A.8.5 Autentificare sigură A.8.7 Protecție antimalware A.8.9 Managementul configurațiilor A.8.17 Sincronizarea ceasului A.8.20 Securitatea rețelei A.8.21 Securitatea serviciilor de rețea
Cerințe de securitate standard	
Crearea unei politici de securitate specifice Achiziționarea unui ruter/switch nou Crearea unei liste de verificare de configurare pentru ruter/switch Administrarea printr-o rețea de gestionare separată Protecție împotriva inundării cu mesaje ICMP Filtrarea bogon și spoofing Protecția împotriva atacurilor DoS și DDoS Configurarea listelor de control al accesului Securizarea porturilor switch-ului Securitatea protocoalelor de rutare Gestionarea identității și a autorizațiilor în infrastructura de rețea Planificarea de urgență pentru rutere și comutatoare Teste de revizuire și penetrare	A.5.1 Politici pentru securitatea informației A.5.7 Inteligența amenințărilor A.5.25 Evaluarea şi decizia privind evenimentele de securitate a informaţiei A.5.27 Învăţarea din incidentele securităţii informației A.5.28 Colecții de evidență A.7.11 Utilități de suport A.8.2 Drepturi privilegiate de acces A.8.4 Accesul la codul-sursă A.8.6 Managementul capacității A.8.8 Managementul vulnerabilităţilor tehnice A8.13 Copii de rezervă a informației A.8.15 Înregistrarea evenimentelor A.8.16 Monitorizarea activităților A.8.22 Segregarea rețelelor
Cerințe de securitate sporite	
Utilizarea controalelor de acces la rețea Protecție extinsă a integrității pentru fișierele de configurare Disponibilitate ridicată Managementul lățimii de bandă pentru aplicații și servicii critice	A.8.3 Restricții de acces la informație A.8.14 Redundanța echipamentelor A.8.27 Securitatea arhitecturilor de securitate și a principiilor inginerești

Anexa 8. Varianta inițială a depozitului de securitate

DEPOZIT CERINȚE DE SECURITATE										
Departament/Direcție:		Responsabil DS:						Aprobat de:		No de referință
Locația Depozitului:		Membru DS 1:						Semnătura		
Data:		Membru DS 2:						Nume:		
Versiunea:		Membru DS 3:						Funcție:		
Revizuire planificată:		Membru DS 4:						Data:		
Categorie active	Active de suport	Amenințări generice	Amenințări specifice	Controale de securitate						Probleme identificate
					Implementat			Implementat		
				Controale de Bază	Efectiv	Non-efectiv	Controale Standard	Efectiv	Non-efectiv	
	Server	9, 12, 13, 16, 17, 18, 19, 20, 23, 24, 26, 32, 33, 34, 35, 37, 39, 40	Utilizarea sau administrarea incorectă a dispozitivelor și sistemelor Pierderea datelor Dispozitive sau sisteme nefuncționale Defecțiunea dispozitivelor sau a sistemelor Atacul cibernetic Programe malițioase Negarea serviciilor (Denial of Service)	SYS.1.1.A1Instalare adecvată			SYS.1.1.A11Definirea unei politici de securitate pentru servere			
				SYS.1.1.A2Autentificarea utilizatorului pe servere			SYS.1.1.A12Planificarea utilizării serverelor			
				SYS.1.1.A5Protecția interfețelor			SYS.1.1.A13Achiziție de servere			
				SYS.1.1.A6Dezactivarea serviciilor inutile			SYS.1.1.A15Sursă de alimentare stabilă și neîntreruptibilă			
				SYS.1.1.A9Utilizarea programelor antivirus pe servere			SYS.1.1.A16Configurația de bază sigură a serverelor			
				SYS.1.1.A10Logare			SYS.1.1.A19Configurarea filtrelor locale de pachete			
							SYS.1.1.A21Documentație operațională pentru			
							SYS.1.1.A22Integrarea în Planificarea de urgență			
							SYS.1.1.A23Sisteme de monitorizare și servere			
							SYS.1.1.A24Verificări de securitate pentru servere			
							SYS.1.1.A25Dezafectarea controlată a unui server			
							SYS.1.1.A35Întocmirea și întreținerea unui manual de utilizare			

Sursa: elaborat de autor după modulele IT - Grundschutz Kompendium.

Anexa 9. Întrebări evaluare cantitativă

1. Angajamentul de implementare a CSSCE a fost aprobat de către administrația instituției?
2. Au fost alocate resurse pentru implementarea CSSCE?
3. A fost stabilit contextul și determinate problemele interne/externe ale instituției pe dimensiunea securității comunicațiilor electronice?
4. Au fost determinate părțile interesate/responsabilii pentru implementarea CSSCE?
5. Realizați acțiuni pentru identificarea părților terțe de care depind activitățile instituției?
6. A fost determinat domeniul de aplicare a CSSCE?
7. Ați realizat arhitectura de referință a RCE universitare?
8. Ați implementat și publicat politica de securitate generală a instituției?
9. Actualizați cu o periodicitate determinată conținutul politicii de securitate generală a instituției?
10. Ați determinat serviciile academice electronice pentru care se implementează CSSCE?
11. Ați implementat politici de securitate specifice serviciilor electronice academice pe care le prestați?
12. Actualizați cu o periodicitate determinată conținutul politicilor de securitate specifice ale instituției?
13. Este realizată lista activelor de suport pentru fiecare serviciu academic electronic?
14. Ați implementat politici de securitate bazate pe sistem configurate pe activele de suport universitare?
15. Este realizată lista obiectivelor de securitate și dependența de serviciile electronice academice?
16. Este realizată lista amenințărilor generice pentru fiecare activ de suport important?
17. Este realizată lista amenințărilor specifice pentru fiecare activ de suport important?
18. Realizați activități pentru evaluarea riscului cibernetic?
19. Utilizați registrul riscurilor cibernetice pentru a duce o evidență a activelor ce prezintă riscuri de securitate?
20. Ați clasificat activele de suport conform riscului pe care îl prezintă ca fiind active cu risc redus, mediu sau sporit?
21. Implementați pe toate activele cu risc de securitate redus cerințe de securitate de bază?
22. Implementați pe toate activele cu risc de securitate mediu cerințe de securitate de bază și cerințe de securitate standard?
23. Implementați pe toate activele cu risc de securitate mare cerințe de securitate de bază, standard și sporite?
24. Evaluați periodic eficacitatea cerințelor de securitate implementate?

25. Aveți în instituție aprobat un plan de tratare a riscului de securitate?
26. Ați realizat declarația de aplicabilitate?
27. Ați creat depozitul controalelor de securitate?
28. Actualizați periodic depozitul controalelor de securitate cu noi active de suport utilizate?
29. Actualizați periodic depozitul controalelor de securitate cu noi amenințări de securitate cu care s-a confruntat instituția Dvs.?
30. Actualizați periodic depozitul controalelor de securitate cu noi cerințe de securitate?

Anexa 10. Acte de implementare

MINISTERUL EDUCAȚIEI
ȘI CERCETĂRII AL REPUBLICII
MOLDOVA
**UNIVERSITATEA TEHNICĂ
A MOLDOVEI**

MINISTRY OF EDUCATION
AND RESEARCH OF THE REPUBLIC
OF MOLDOVA
**TECHNICAL UNIVERSITY
OF MOLDOVA**

MD-2004, Chișinău, Bd. Ștefan cel Mare și Sfânt, 168, Tel: 022 23-78-61 | Fax: 022 23-54-41, www.utm.md

07 octombrie 2022

A C T

de implementare a rezultatelor științifice obținute în teza de doctor elaborată de Alexei Arina, în vederea obținerii titlului de doctor în științe tehnice, cu tema:" CADRU SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE PENTRU INSTITUȚIILE DE ÎNVĂȚĂMÂNT SUPERIOR DIN REPUBLICA MOLDOVA"

Rezultatele științifice obținute de către doamna Alexei Arina și prezentate spre analiză către Direcția Tehnologia Informației și Comunicații, UTM, reprezintă valoare aplicativă și au fost implementate pentru a spori securitatea serviciilor academice electronice prestate de către Universitatea Tehnică a Moldovei.

Elementele de noutate științifică obținute în prezenta teză, au fost propuse spre implementare și testare în cadrul rețelei de comunicații UTM, astfel au fost implementate politici de securitate pe tehnologiile de comunicații universitare și verificate cerințele de securitate propuse spre implementare.

Considerăm, că rezultatele, propunerile și recomandările expuse în teza de doctor, au un impact semnificativ pentru securitatea comunicațiilor electronice în Instituțiile de Învățământ Superior, inclusiv Universitatea Tehnică a Moldovei, deoarece se orientează pe specificul rețelelor și serviciile de comunicații electronice universitare, pot servi ca ghid de implementare a propriului sistem de securitate.

Prorectorul Universității Tehnice a Moldovei
pentru digitalizare
Dinu Țurcanu
Maestru în Telecomunicații și Tehnologia Informației

MINISTERUL SĂNĂTĂȚII
AL REPUBLICII MOLDOVA

UNIVERSITATEA DE STAT DE MEDICINĂ
ȘI FARMACIE „NICOLAE TESTEMIȚANU"
DIN REPUBLICA MOLDOVA

MINISTRY OF HEALTH
OF THE REPUBLIC OF MOLDOVA

NICOLAE TESTEMITANU STATE UNIVERSITY
OF MEDICINE AND PHARMACY
OF THE REPUBLIC OF MOLDOVA

MD-2004, Chișinău, bd. Ștefan cel Mare și Sfânt, 165, tel.: (+373) 22 205 701, fax: (+373) 22 242 344, contact@usmf.md, https://usmf.md

09.11.2022

ACT

de implementare a rezultatelor științifice obținute în teza de doctor realizată de Alexei Arina, în vederea obținerii titlului de doctor în științe tehnice, cu tema:

"Cadru Sistemic de Securitate a Comunicațiilor Electronice pentru Instituțiile de Învățământ Superior din Republica Moldova"

Cadrul Sistemic de Securitate a Comunicațiilor Electronice propus de către dr. Alexei Arina prezintă o valoare aplicativă semnificativă pentru mediul universitar și a fost implementat pentru a spori securitatea rețelelor de comunicații electronice, inclusiv ale Universității de Stat de Medicină și Farmacie "Nicolae Testemițanu" din Republica Moldova.

Elementele de noutate științifică, elaborate și prezentate în teza de doctor, ce au prezentat interes sunt:

- Evidențierea problemelor interne și externe cu care se poate confrunta universitatea ca urmare a digitalizării și elaborarea sistemului de securitate;
- Modalitatea de implementarea și evidențierea importanței de a implementa un sistem care să gestioneze centralizat problemele care apar ca urmare a digitalizării;
- Diverse acte de suport: lista de verificare a activelor informaționale universitare; lista amenințărilor generice și specifice mediului universitar; modelul propus pentru managementul riscului cibernetic; depozitul cerințelor de securitate.

Prorector pentru activitate socială

Marcel Abraș

conferențiar universitar, dr. șt. med.

FREE INTERNATIONAL UNIVERSITY OF MOLDOVA

UNIVERSITATEA LIBERĂ INTERNAȚIONALĂ DIN MOLDOVA

52, Vlaicu Pârcălab St., Chişinău, MD-2012, Republic of Moldova

Tel. (37322) 220029, Fax (37322) 205976, e-mail: ulim@ulim.md, office@ulim.md

UNIVERSITATEA LIBERĂ INTERNAȚIONALĂ DIN MOLDOVA
IEȘIRE Nr. 370/A/109
18 octombrie 2022

18.10.2022

ACT

de implementare a rezultatelor ştiinţifice obţinute în teza de doctor realizată de ALEXEI Arina, în vederea obţinerii titlului de doctor în ştiinţe tehnice, cu tema:

"CADRU SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE PENTRU INSTITUȚIILE DE ÎNVĂȚĂMÂNT SUPERIOR DIN REPUBLICA MOLDOVA"

Universitatea Liberă Internaţională din Moldova, ca de altfel şi toate celelalte Instituţii de Învăţământ Superior naţionale şi internaţionale, gestionează cu un volum foarte mare de date sensibile, care necesită protecţie, astfel că abordarea unei strategii care ar permite securizarea datelor şi serviciilor educaţionale electronice, este foarte important în secolul tehnologizării intense. Rezultatele ştiinţifice obţinute de către d-na ALEXEI Arina, au permis conturarea mai clară şi cuprinzătoare totodată a acestei probleme. Astfel că, pentru a securiza informaţia sensibilă, dar şi pentru a asigura disponibilitatea serviciilor academice electronice, Serviciului Control Proces Educaţional din cadrul Universităţii Libere Internaţionale din Moldova a implementat Cadrul Sistemic propus de d-na ALEXEI Arina.

Prezentăm interes sporit pentru:

- Baza de cunoştinţe teoretice şi empirice, care se bazează pe investigaţii şi metode ştiinţifice aplicate pentru a identifica soluţii viabile pentru problema securităţii comunicaţiilor electronice specifice mediului academic;
- Analiza problemelor din domeniu;
- Expunerea clară a etapelor de implementare a cadrului de securitate propus, ca parte aplicativă a tezei de doctor;
- Operaţionalizarea cadrului sistemic de securitate a comunicaţiilor electronice.

Prorector pentru Strategie Academică şi Programe de Studii ULIM
dr. conf. univ. Alexandr CAUIA

MINISTERUL EDUCAȚIEI
ȘI CERCETĂRII AL REPUBLICII
MOLDOVA
**UNIVERSITATEA TEHNICĂ
A MOLDOVEI**

MINISTRY OF EDUCATION
AND RESEARCH OF THE REPUBLIC
OF MOLDOVA
**TECHNICAL UNIVERSITY
OF MOLDOVA**

MD-2004, Chișinău, Bd. Ștefan cel Mare și Sfânt, 168, Tel: 022 23-78-61 | Fax: 022 23-54-41, www.utm.md

04 octombrie 2022

ADEVERINȚĂ

Prin prezenta se confirmă:

Alexei Arina, doctorandă la departamentul Telecomunicații și Sisteme Electronice a Universității Tehnice a Moldovei, a implementat rezultatele obținute în cadrul tezei de doctor cu tema: "CADRU SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE PENTRU INSTITUȚIILE DE ÎNVĂȚĂMÂNT SUPERIOR DIN REPUBLICA MOLDOVA", în procesul de instruire la Universitatea Tehnică a Moldovei:

- Departamentul Telecomunicații și Sisteme Electronice, disciplinele: " Securitatea informației în sistemele de telecomunicații" și "Securitatea Informației" titular de curs lectoră universitară Arina Alexei.
- Departamentul Ingineria Software și Automatică, disciplina " Tehnologii ale securității informaționale", anul de studii 2022-2023, titular de curs lectoră universitară Arina Alexei.

Rezultatele științifice teoretice și practice au fost utilizate în calitate de:

1. Suport de curs pentru temele ce se referă la standardele internaționale de securitate; managementul riscului cibernetic, atacuri și amenințări de securitate, tehnologii pentru asigurarea principiilor fundamentale ale securității;
2. În cadrul orelor de laborator, rezultatele aplicative obținute au fost utilizate ca ghid pentru implementarea sistemelor de securitate și configurarea tehnologiilor de comunicații electronice.

Adeverința este eliberată pentru a confirma importanța rezultatelor științifice teoretice și aplicative, obținute de doctoranda Alexei Arina.

Prim-Prorectorul Universității Tehnice a Moldovei

Rețitca Vladislav,

conf.univ., dr.

Declaraţia privind asumarea răspunderii

Subsemnata, ALEXEI Arina, declar pe răspundere personală că materialele prezentate în teza de doctorat sunt rezultatul propriilor cercetări şi realizări ştiinţifice. Conştientizez că, în caz contrar, urmează să suport consecinţele în conformitate cu legislaţia în vigoare.

ALEXEI Arina_____

Data_____

CURRICULUM VITAE al autorului

INFORMAŢII PERSONALE	**Arina ALEXEI**
	str. Acad. S. Rădăuțanu 9, ap.74, 2045 Chișinău, Republica Moldova +373 060 675 675 arina.alexei@tse.utm.md
EDUCAŢIE ŞI FORMARE	Universitatea Tehnică a Moldovei, 2000-2004 Diplomă de licență în Informatică
	Universitatea de Stat din Moldova, 2007-2009 Diplomă de Master în Business și Administrarea Afacerilor
	Universitatea Tehnică a Moldovei, 2009-2014 Studii de Doctorat, Specialitatea – Sisteme, reţele şi dispozitive de telecomunicaţii redenumită în Ingineria și tehnologia comunicațiilor electronice
EXPERIENŢĂ PROFESIONALĂ	Profesor de informatică Liceul de Limbi Străine și Informatică, Chișinău, Republica Moldova, 2003-2004
	Lector universitar, Departamentul Telecomunicații și Sisteme Electronice, Facultatea Electronică și Telecomunicații, Universitatea Tehnică a Moldovei, Chișinău, Republica Moldova 2006-prezent
Limbi străine	Engleza – foarte bine Franceza – bine Rusa – foarte bine