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

231.02. INGINERIA ȘI TEHNOLOGIA COMUNICAȚIILOR ELECTRONICE

Rezumat științific al tezei de doctor în științe inginerești

CHIȘINĂU, 2023

Teza a fost elaborată în cadrul departamentului ”Telecomunicații și Sisteme Electronice”, facultatea Electronică și Telecomunicații, Universitatea Tehnică a Moldovei.

Conducător științific:

NISTIRIUC Pavel, doctor în științe fizico-matematice, conferențiar universitar, UTM.

Referenți oficiali:

COSTAȘ Ilie, doctor habilitat în tehnică, profesor universitar, ASEM.
CĂPĂŢÂNĂ Gheorghe, doctor în tehnică, profesor universitar, USM.

Componența Consiliului Ştiinţific Specializat:

GUŢULEAC Emilian, **președinte**, doctor habilitat în tehnică, profesor universitar, UTM.
COJUHARI Irina, **secretar științific**, doctor în informatică, conferențiar universitar, UTM.
BOLUN Ion, doctor habilitat în tehnică, profesor universitar, UTM.
ABABII Victor, doctor în tehnică, conferențiar universitar, UTM.
COJOCARU Igor, doctor în informatică, director IDSI.
AVRAM Ion, doctor în tehnică, conferențiar universitar, UTM.

Susţinerea va avea loc la data de 17.11.2023, ora 15.00, în şedinţa Consiliului Ştiinţific Specializat **D 231.02-23-31** din cadrul Universității Tehnice a Moldovei pe adresa: MD-2045, Republica Moldova, Chişinău, str. Studenţilor 9/7, bl. 3, sala 3-208.

Teza de doctor și rezumatul pot fi consultate la biblioteca tehnico-ştiinţifică a Universităţii Tehnice a Moldovei şi pe pagina web a Agenției Naționale de Asigurare a Calității în Educație și Cercetare (www.cnaa.md/www.anacec.md).

Rezumatul ştiinţific a fost expediat la ” 16 ” octombrie 2023.

Secretar ştiinţific
al Consiliului Ştiinţific Specializat,
Dr. în informatică, conf.univ. Cojuhari Irina

Conducător ştiinţific,
Dr. în șt. fizico-matematice, conf. univ. Nistiriuc Pavel

Autor Alexei Arina

CUPRINS

I. REPERE CONCEPTUALE ALE CERCETĂRII

Raționamentele și motivația cercetării

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). Odată cu digitalizarea la nivel internațional și dezvoltarea serviciilor electronice, care devin tot mai cunoscute, cresc și riscurile asociate tehnologiilor comunicaționale. 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.

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 $, 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. Atacuri cu impact major au avut loc asupra infrastructurilor critice de stat, 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.

Conform raportului prezentat de Microsoft și Check Point Software, 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, la fel, și atenția din partea autorităților centrale. 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, 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, 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). Metoda complementară utilizată pentru operaționalizarea cadrului este Ingineria Cerințelor de Securitate SRE (Security Requirements Engineering). 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, 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. Metoda Delphi a fost combinată cu metode calitative, așa ca interviurile semi-structurate, 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 secțiunea a V-a.

II. CONȚINUTUL TEZEI

Capitolul 1, ***SECURITATEA COMUNICAȚIILOR ELECTRONICE***, include 6 componente importante, cum ar fi:

1. ***Considerații generale și termeni specifici domeniului*** în care au fost definiți următorii termeni: comunicații electronice, rețele de comunicații electronice (RCE), servicii de comunicații electronice (SCE), securitatea comunicațiilor electronice, securitatea cibernetică, active bazate pe CE, arhitecturi de securitate. A fost analizată evoluția tehnologiilor comunicaționale și arhitecturile de securitate propuse de către organizațiile internaționale pentru asigurarea securității CE bazată pe trei straturi: stratul de infrastructură care se referă la elementele esențiale ale RCE așa ca dispozitive intermediare de rețea, dispozitive terminale și medii de conexiune; stratul de servicii care se referă la SCE prestate consumatorului final și poate varia de la servicii de bază, precum este accesul la Internet până la servicii cu valoare adăugată; stratul de aplicații care se referă la aplicațiile bazate pe rețea, ce pot fi simple sau colaborative.

2. ***Amenințări de securitate a comunicațiilor electronice*** – 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 [1]. 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* [1]. 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*. Majoritatea atacurilor în RCE au loc începând cu nivelul 2 OSI, nivelul legătură de date, precum ar fi atacurile de tip DoS/DDoS, care au loc prin inundarea cu pachete sau transmiterea pachetelor formatate incorect (în ultimii 20 de ani au înregistrat o creștere majoră a consumului de bandă); atacurile de impersonare prin modificarea adreselor de rețea și a tabelului ARP sau prin falsificarea DNS; atacurile MiTM bazate pe falsificare sau creare de stații false, cât și în baza protocoalelor TLS/SSL sau BGP; atacuri pasive de interceptare a comunicațiilor electronice. Există și câteva tipuri de atacuri care vizează nivelul 1 OSI, după cum este bruiajul frecvențelor radio (RF) în rețelele fără fir [2] sau atacurile intenționate de deteriorare a mediilor

de conexiune. De asemenea, un impact mare asupra RCE au tehnicile de inginerie socială [3], utilizatorul fiind una dintre principalele surse de amenințare pentru comunicațiile electronice.

3. ***Dispozitive de securitate a rețelelor de comunicații electronice*** **–** pot fi analizate prin prisma nivelurilor modelului OSI, care se referă la RCE, și anume, la nivelul 1 al modelului OSI. Dispozitivele electronice utilizate 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 sistemele de detecție și prevenire a intruziunilor (IDPS). Nivelul 3, de 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 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, care controlează procesul de comunicație dintre rețeaua internă și externă, implementând politicile de securitate a rețelei securizate. Firewall-urile pot fi dispozitive electronice, servicii de securitate integrate pe rutere sau aplicații instalate pe sistemul de operare al dispozitivelor terminale. Alte dispozitive de securitate utilizate pentru protecția RCE sunt UTM (Unified Threat Management), considerate a fi firewall de generația următoare și dispozitive multifuncționale.

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 printr-un nivel înalt de dezvoltare a RCE. Astfel, au fost aduse modificări Legii nr. 241 cu privire la comunicațiile electronice, din 15.11.2007, 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 rețelelor și serviciilor de CE; modificări aduse pentru armonizarea legislației Republicii Moldova la prevederile directivelor-cadru ale Uniunii Europene. Așadar, art. 21, punctul 1(a) se referă la totalitatea măsurilor tehnice și organizatorice pentru managementul riscului informațional/cibernetic, 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 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică prevede cerințe minime obligatorii pentru securitatea RCE și a transmisiunilor de date (HG.201). 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. La fel, 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, deoarece sunt impuse noi condiții 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.

5. ***Esența și particularitățile CE ale IÎS*** **–** RCE universitare reprezintă rețelele IP autonome gestionate 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 [4]. Pentru managementul centralizat al rețelelor de CE universitare sunt utilizate conexiunile LAN și WAN [4].

Designul RCE diferă de la IÎS la IÎS [5], de la designul în cascadă la modelul ierarhic de organizare a RCE. 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 pot provoca pierderea conexiunii la Internet în cazul deconectării unui singur comutator [5]. Modelul ierarhic de configurarea a RCE oferă o topologie modulară și scalabilă, care permite rețelelor să evolueze [4] și este divizat pe 3 straturi: acces, distribuție și de bază.

Datorită modelelor de rețea utilizate și a erorilor în configurația dispozitivelor intermediare de rețea apar mai multe probleme, exploatate ulterior de atacurile cibernetice, provocând pierderi financiare importante, indisponibilitatea serviciilor educaționale în IÎS și furtul proprietății intelectuale. 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.

6. ***Studiul empiric al situației actuale în IÎS din Republica Moldova*** la care au participat 9 IÎS naționale (60% din IÎS de stat) 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 participante 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:

a) 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;

b) politicile de acces, educarea utilizatorilor, controlul mediilor amovibile, monitorizarea utilizatorilor, managementul incidentelor sunt aplicate de o mică parte din IÎS;

c) politicile de securitate nu sunt implementate în cea mai mare parte de către IÎS naționale, doar 22,2% au confirmat implementarea acestora;

d) nici o IÎS nu este certificată cu un standard internațional.

Definirea problemei de cercetare s-a bazat pe analiza cadrelor normative, rapoartele de securitate internaționale și alte studii științifice publicate de cercetători, fiind necesare cercetări privind:

- 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.

În capitolul 2, ***METODOLOGIA DE DEZVOLTARE A CADRULUI SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE,*** a fost prezentată principala metodă științifică, metoda DSR, utilizată la identificarea soluțiilor privind problema de cercetare și descrise etapele de implementare a acestei metode, pentru ca să fie reproductibile cunoștințele prescriptive din respectiva teză de doctor. Designul cercetării conform etapelor metodei DSR poate fi analizat în figura 1.

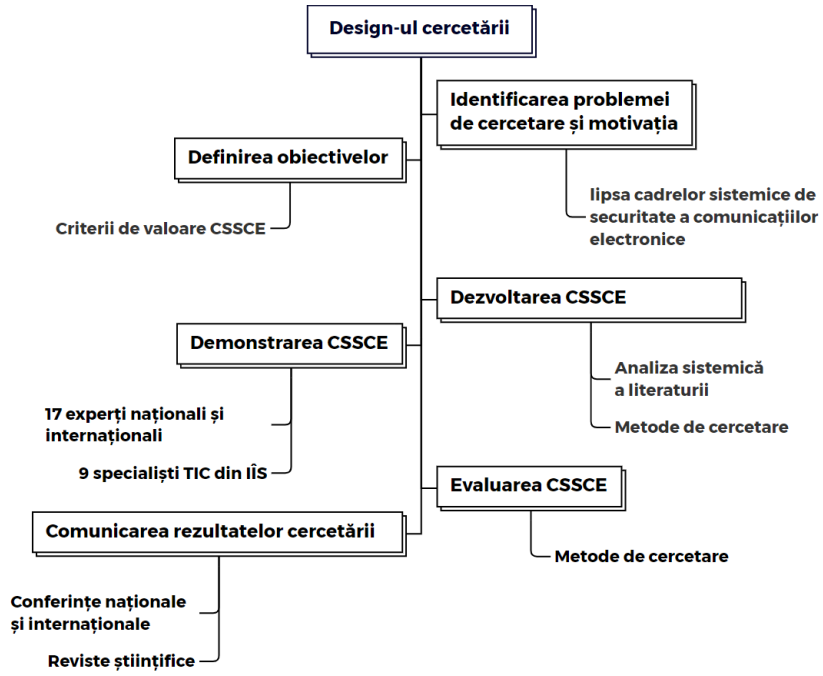

Figura 1. Designul cercetării conform etapelor DSR

Provocarea a fost de a identifica criterii de valoare după care va fi evaluat și confirmat CSSCE. Astfel, au fost studiate lucrările științifice [6, 8] pentru a identifica criteriile de valoare după care pot fi evaluate cadrele de securitate, în baza dovezilor științifice. Criteriile de valoare propuse pentru evaluarea CSSCE și argumentele relevante pot fi analizate în tabelul 1.

Tabelul 1. Criteriile de valoare ale CSSCE

Nr.	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 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	Importanța internațională	IÎS din RM se conformează procesului de la Bologna, care definește importanța implementării cadrelor recunoscute internațional 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.

Dezvoltarea prototipului trebuie să se bazeze pe studiul aprofundat al literaturii de specialitate, componentele funcționale ale sistemului și relațiile predefinite dintre acestea. A fost realizat studiul literaturii, conform metodei propuse de Kitchenham, cu scopul de a identifica, interpreta și evalua cercetările relevante domeniului de securitate a CE în instituțiile de învățământ superior [9] (figura 2).

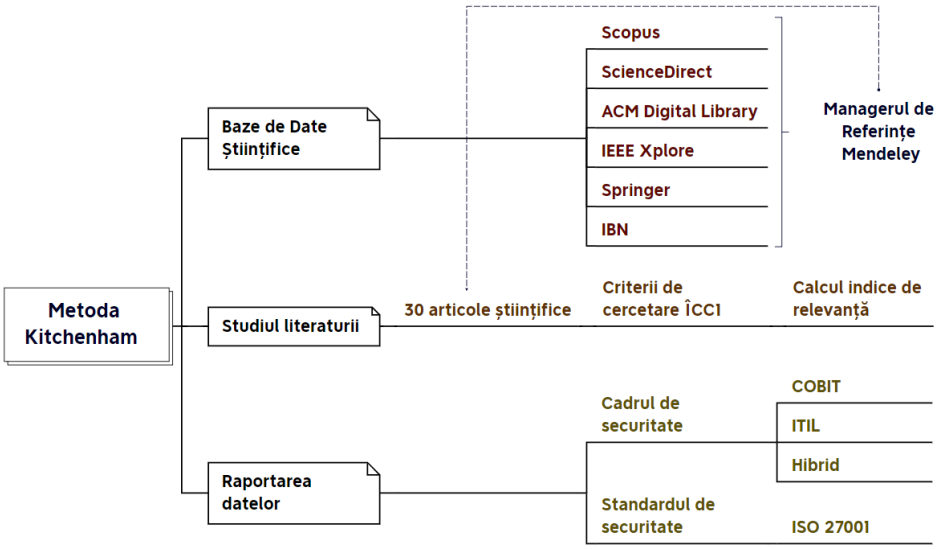

Figura 2. Studiul literaturii în baza metodei lui Kitchenham

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 în 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 [1, 10].

De asemenea, drept contribuție originală a tezei au fost identificate lacune între cerințele minime ale HG 201 și controalele de securitate din anexa A, a standardului ISO 27001 [11], deși cerințele lipsă vizează aspecte importante pentru IÎS [12]. Pentru identificarea lacunelor a fost utilizată analiza decalajului, iar în continuare vor fi prezentate câteva concluzii relevante domeniului academic:

- Este necesar a fi prevăzute proceduri clare pentru eliminarea conturilor înregistrate în sistemele universitare ale studenților care au absolvit IÎS și ale 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 rețea;* 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; în acest sens vor fi utilizate standardele ISO 27001 și ISO 27005.

Tot în acest capitol a fost descrisă metoda SRE, utilizată pentru procesul de operaționalizare a CSSCE în IÎS (figura 3).

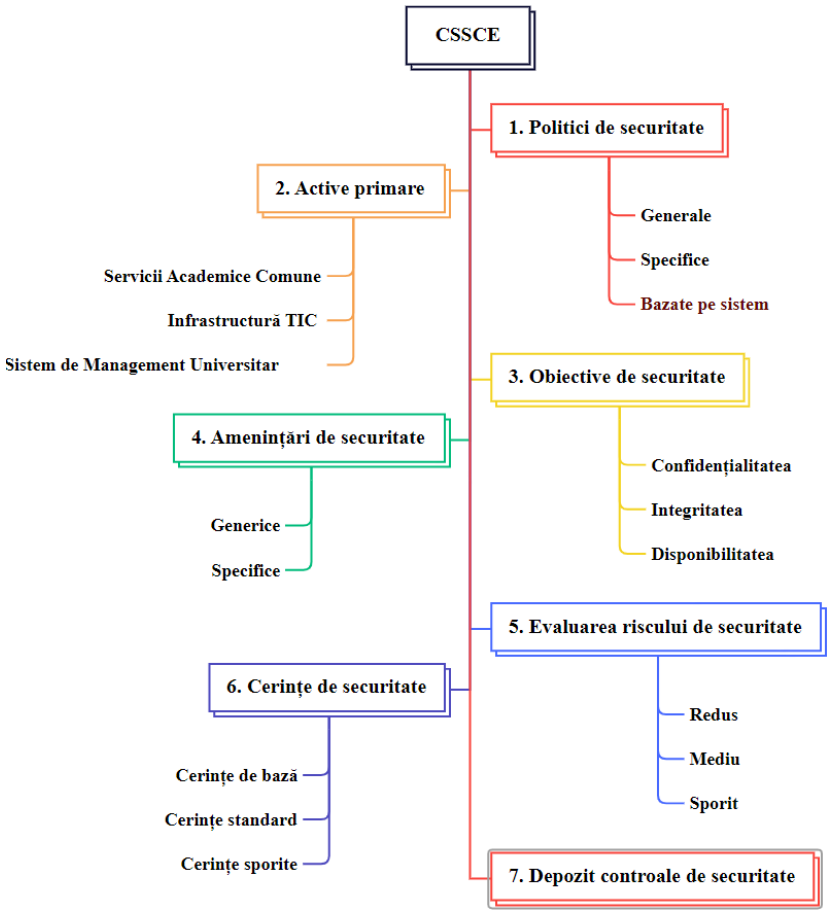

Figura 3. Operaționalizarea CSSCE conform metodei SRE

Capitolul 3, ***CADRUL SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE UNIVERSITARE,*** poate fi divizat în două secțiuni principale, prima dintre care se bazează pe fundamentarea teoretică a CSSCE, iar a doua secțiune pe dezvoltarea CSSCE.

Pentru fundamentarea teoretică a fost definit conceptul de securitate a CE. Totalitatea elementelor-cheie este prezentată prin harta conceptuală din figura 4, în baza elementelor-cheie identificate în definițiile la care s-au referit alți cercetători și organizații specializate expuse în capitolul 1.

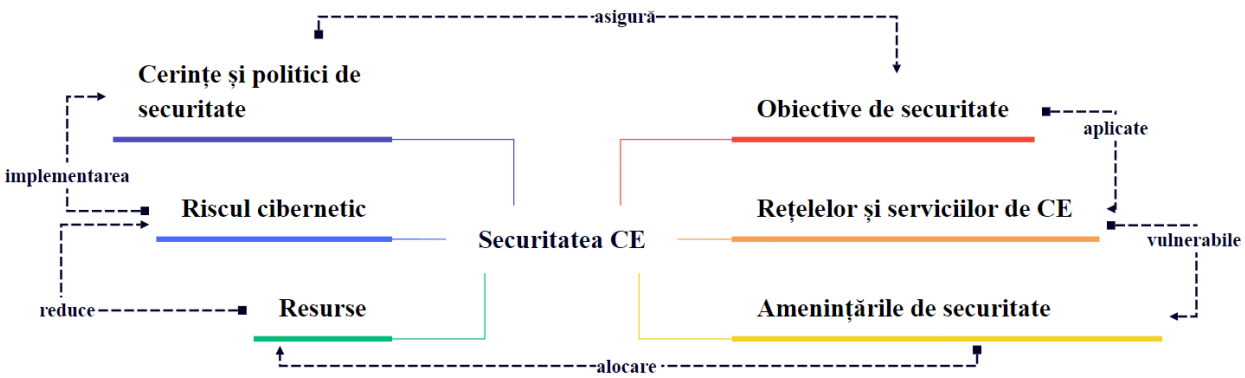

Figura 4. Conceptul de securitate a CE

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***.

La selectarea cerințelor de securitate și implementarea sistemelor de securitate trebuie să se ia în calcul calitatea serviciilor, astfel securitatea devenind unul dintre criteriile constituente ale QoS (Quality of Service), deopotrivă cu viteza, utilizabilitatea, disponibilitatea, fiabilitatea etc. Așadar, securitatea și QoS sunt considerate servicii critice ale RCE, fiind interdependente și necesită a fi luate în calcul când se proiectează infrastructura de rețea.

A fost analizat modelul Clements–Hoffman bazat pe teoria grafurilor, mulțimile fuzzy și teoria probabilității [13, 14]. Teoria mulțimilor fuzzy permite ca obiectele să aparțină unei mulțimi sau cuplurile de obiecte să aparțină unei relații, deținând un anumit grad de apartenență și sunt potrivite pentru evaluarea sistemelor de securitate complexe în care există un anumit nivel de incertitudine. Teoria mulțimilor fuzzy este aplicată în momentul când este necesar a exprima cantitativ anumite mărimi imprecise [15].

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 [13]. 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 [13]. 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. Este important a specifica că relația amenințare-cerință-obiect, conform modelului Clements–Hoffman, nu este una 1-1-1 [16], 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.

Astfel, prin utilizarea modelului Clements–Hoffman pot fi definite următoarele:

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

$$S=\{O,A,C,V,P\}, \quad (1)$$

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 de 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:

$$V=O\times A=\{v_l=(o_i,\ a_j),l=1,L\}; \quad (2)$$

$$P=C\times V=O\times A\times C=\{p_t=(o_i,a_j,c_m),t=1,T\}; \quad (3)$$

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 sistematice, 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 reprezintă un sistem de securitate complet acoperit, compus din 5 seturi de variabile conform formulei 1, poate fi analizat în figura 5.

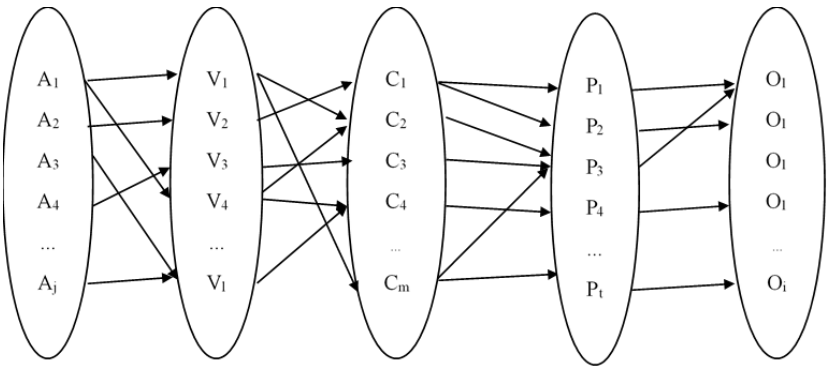

Figura 5. Graful sistemului de securitate (adaptat după [13]**)**

Pentru modelul sistemului de securitate complet protejat se îndeplinește următoarea condiție:

$$\forall(v_l)\in V\ \exists(p_t=(o_i,a_j,c_m))\in P\ ; \quad (4)$$

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 expusă în formula 4, care indică un sistem complet securizat, se poate deduce că un sistem nu este securizat dacă există următoarea condiție:

$$(v_l) \in V \nexists (p_t = \langle o_i, a_j, c_m \rangle) \in P ; \quad (5)$$

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. Astfel, poate fi prezentată următoarea relație:

$$\beta(t) = P\{A(t) \leq 0, R(t) > b_0\}. \quad (6)$$

Un alt indicator propus pentru utilizare poate fi riscul rezidual R_r, adică, valoarea riscului rămasă după tratarea riscului prin implementarea cerințelor de securitate, care se determină după formula (7):

$$Rr_t = P_t C_t (1 - R_t); \quad (7)$$

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 exploatat de a_j pentru care s-a implementat cerința de securitate p_t;

R_t – rezistența căii de penetrare protejate p_t.

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

$$S=\frac{1}{\sum_{t=1}^{T} P_t C_t (1-R_t)}. \quad (8)$$

Așadar, 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.

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.

În partea a doua din capitolul 3 se prezintă procesul după care a avut loc dezvoltarea CSSCE. Cadrul sistemic este format din mai multe componente distincte, eterogene, inseparabile ce îi definesc consistența [17]. Acesta poate fi definit ca o rețea sau un plan de concepte interconectate, care oferă o înțelegere cuprinzătoare a unui fenomen [17]. 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*.

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. Întregul proces care reflectă ciclul de viață al CSSCE, în baza modelului PDCA, poate fi analizat în figura 6.

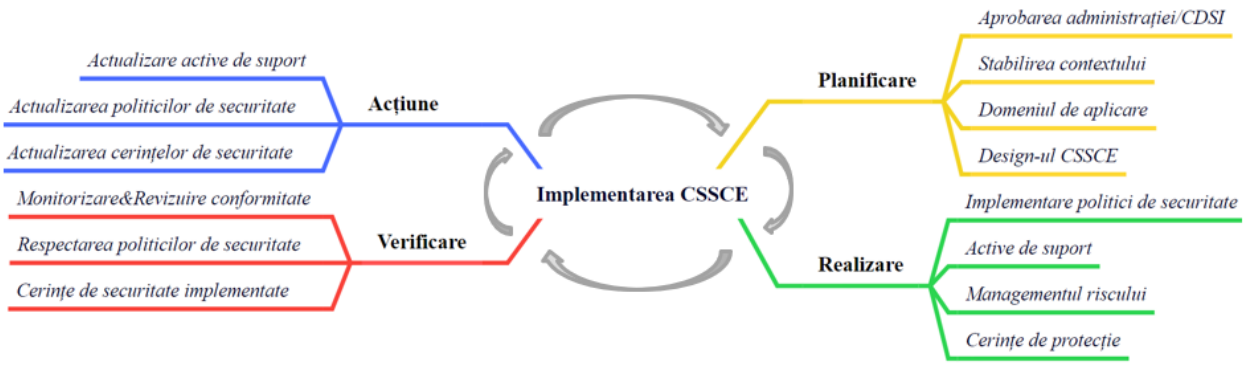

Figura 6. Dezvoltarea CSSCE conform ciclului Deming

Abordarea sistemică a securității CE, în orice organizație, începe cu procesele organizaționale [18, 19], 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 7).

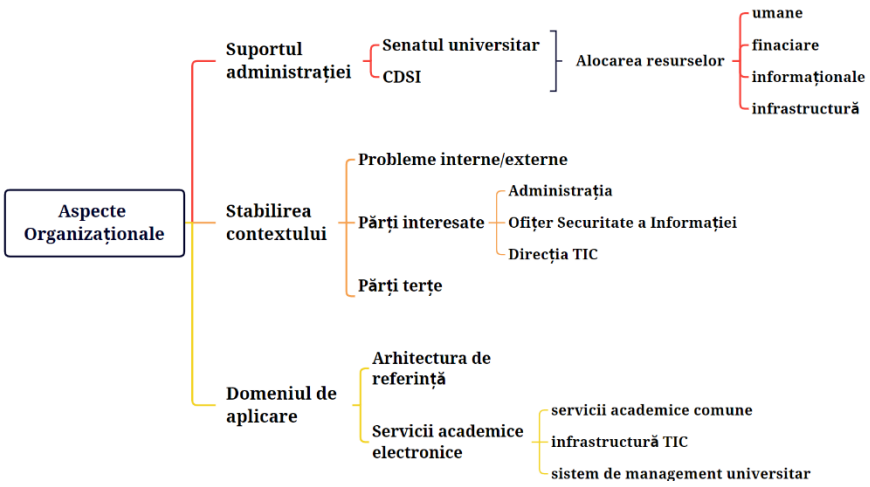

Fig. 7. Dezvoltarea aspectelor organizaționale ale CSSCE

Drept rezultat au fost identificate activele primare ale IÎS pentru care este necesară asigurarea securității CE: ***serviciile academice comune, infrastructura TIC, sistemul de management universitar studenți/angajați***.

Procesul de operaționalizare a CSSCE în etapa inițială presupune determinarea indicatorilor-cheie de performanță. Indicatorii de performanță sunt utilizați pentru a măsura nivelul de securitate în cadrul organizațiilor. Sistemele de securitate sunt compuse din seturi de variabile fuzzy. 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. 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 noi 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 al CE într-un moment dat de timp. Astfel, indicatorii de performanță pot servi ca instrumente utilizate la luarea deciziilor și la stabilirea obiectivelor măsurabile [20]. Indicatorii-cheie ai CSSCE au fost identificați conform etapelor de operaționalizare a cadrului sistemic și reprezintă finalitatea fiecărei etape în parte. Fluxul de lucru prin care activitățile vor fi procesate și obținuți indicatorii de performanță sunt reflectați în tabelul 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 2. Indicatori-cheie de performanță a CSSCE

Nr. d/o	Operaționalizare a 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 - Politică de securitate specifică pentru serviciile electronice academice - Politici de securitate bazate pe sistem implementate pe 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 sistem
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 - Declarația de aplicabilitate

				Continuarea tabelului 2
6	Identificarea cerințelor de securitate	- Depozitul cerințelor de securitate - IT Grundschutz Kompendium - Declarația de aplicabilitate - Standardul ISO 27001 - Standardul ISO 27002	- Sesiuni de brainstorming - Consultări externe - Interviuri	- Lista cerințelor de securitate pentru fiecare activ de suport al unui proces secundar academic - Responsabilii pentru implementare
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

Cele mai semnificative rezultate care se referă la prototipul CSSCE operațional sunt:

1. A fost clar definită necesitatea implementării politicilor de securitate generale, specifice și tehnice în baza standardelor ISO 27001, ISO 27002 și a rezultatelor empirice obținute în teză. Drept contribuție originală a tezei servește cadrul generic și structura-tip, după care pot fi create și implementate de către orice IÎS atât politici de securitate generale, cât și specifice. A fost propus un model-tip de politică de securitate specifică, au fost simulate două politici de securitate tehnice, care constau în configurarea avertismentelor și crearea listelor de control al accesului pe dispozitivele intermediare de rețea pentru accesul la serverele de fișiere.
2. 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.
3. 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.
4. 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.

5. 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.
6. 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.
7. A fost creat și completat depozitul controalelor de securitate care va putea fi utilizat în comun de IÎS.

De asemenea, drept contribuție originală a tezei de doctor este prototipul aplicației i-CSSCE, ce poate fi utilizat pentru a susține procesul de implementare a activităților propuse de CSSCE și de evaluare cantitativă a nivelului de implementare a cadrului de securitate, pentru a minimiza efortul necesar al activităților de management al securității CE. Prototipul aplicației a fost conceput ca o aplicație web scrisă în PHP, HTML5, JavaScript ce 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 bazată pe MySQL. Conform modelului formal Clements–Hoffman, care descrie componentele primare ale unui sistem de securitate, au fost create funcții ce vor permite ulterior a gestiona relațiile dintre activele bazate pe CE, amenințările și cerințele de securitate.

Pentru ca specialiștii din IÎS să poată evalua cantitativ implementarea indicatorilor de performanță ai CSSCE, a fost dezvoltat un modul separat, care în baza chestionarului va calcula nivelul de implementare a cadrului de securitate propus.

În capitolul 4, ***EVALUAREA CADRULUI SISTEMIC DE SECURITATE A COMUNICAȚIILOR ELECTRONICE,*** este descris un studiu de caz pentru a simula implementarea CSSCE în cadrul unei facultăți a UTM și sunt descrise rezultatele sondajului final, pentru care au fost create 2 paneluri de respondenți: experți în domeniu din companiile din RM și străinătate în Panelul 1, specialiștii responsabili din IÎS în Panelul 2. A fost aplicată tehnica Delphi,

prin care a fost evaluat prototipul CSSCE, conform criteriilor de evaluare stabilite în capitolul 2 al tezei. Rezultatele înregistrate au fost prelucrate, prin instrumentul IBM SPSS, utilizând indicatorii ***statistici descriptivi*** așa ca media și deviația standard, deoarece reprezintă baza analizei cantitative și pentru a generaliza rezultatele sondajului; ***statistica inferențială*** cu scopul de a face inferențe între rezultatele sondajului, adică între datele observate și deducțiile ce nu pot fi identificate prin analiza simplă a datelor. A fost calculat coeficientul de concordanță, numit *W al lui Kendall,* care reprezintă un test neparametric al statisticii inferențiale, utilizat pentru a măsura acordul dintre evaluatorii sondajului, care oferă calificative rezultatelor științifice obținute. Valoarea coeficientului *W al lui Kendall = 0,752,* care indică un acord puternic între cele 2 paneluri ale studiului Delphi, ceea ce confirmă că prototipul CSSCE satisface criteriile de valoare după care a fost dezvoltat.

Evaluarea calitativă a prototipului CSSCE a fost realizată prin recomandările și aprecierile date de respondenții la sondaj, dar și de 2 profesori din Germania care au fost rugați să evalueze rezultatele obținute. Au fost înregistrate doar avize pozitive.

Ultima etapă a constat în compararea a 8 cadre de securitate propuse anterior de către cercetători cu CSSCE în baza prevederilor obligatorii ale standardului ISO 27001 și a etapelor metodei SRE după care a fost dezvoltat CSSCE, acțiune ce a demonstrat originalitatea și inovația soluției derivate din rezultatele cercetărilor realizate în teza de doctor.

III. 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 și demonstrată în prezenta teză de doctor.

Așadar, conform problemei de cercetare identificate și a sarcinilor stabilite 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 utilizate 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 utilizate 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 pentru 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 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 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.

IV. BIBLIOGRAFIE

1. *Security in telecommunications and information technology*. ITU-T Technical Report, 2020.
2. 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.
3. **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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. **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.
10. *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.

11. ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT. International Organization for Standardization. Geneva, Switzerland, 2022. [citat 02.03.2023].
12. **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.
13. HOFFMAN, L.J., CLEMENTS, D. *Fuzzy computer security metrics: a preliminary report*. Berkeley, 1977.
14. 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.
15. 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.
16. Черней Г., Охрименко С., Леаху Ф. *Безопасность автоматизированных информационных систем*. Кишинев: Ruxanda, 1996, 186 стр. ISBN 9975-60-767-5M-187-96.
17. 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.
18. **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.
19. **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.
20. 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.

V. LISTA LUCRĂRILOR PUBLICATE LA TEMA TEZEI

În reviste din străinătate recunoscute:

1. **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.
2. **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.
3. **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.

În reviste din Registrul Naţional al revistelor de profil, cu indicarea categoriei:

Categoria B +

4. **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.
5. **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.
6. **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.

Articole în culegeri ştiinţifice:

În lucrările conferinţelor ştiinţifice internaţionale (peste hotare):

7. **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.
8. **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.

În lucrările conferinţelor ştiinţifice internaţionale (Republica Moldova)

9. **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.
10. **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.
11. **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.

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.

ALEXEI Arina

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

231.02. Ingineria și tehnologia comunicațiilor electronice

Rezumatul tezei de doctor în științe inginerești

Aprobat spre tipar: 11.10.23 | Formatul hârtiei 60x84 1/16

Hârtie ofset. Tipar RISO | Tiraj 50 ex.

Coli de tipar: 2,18 | Comanda nr.

U.T.M. 2023. Chișinău, bd. Ștefan cel Mare, 168.

Editura "Tehnica UTM"

MD 2045, mun. Chișinău, str. Studenţilor 9/9.