MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Șef departament:
FIODOROV Ion dr., conf.univ.

_____
„___" _____ 2025

APLICABILITATEA STANDARDULUI ISO/IEC 27014:2020 ÎN SISTEMELE INFORMAȚIONALE DIN DOMENIUL SĂNĂTĂȚII

Teză de master

Student: **Stoica Adrian, SI-231M**

Coordonator: **Bulai Rodica, lect. univ.**

Consultant: **Cojocaru Svetlana, asist.univ.**

Chişinău, 2025

REZUMAT

Într-o lume digitalizată, expunerea la riscuri cibernetice este o realitate inevitabilă, atât în sfera personală, cât și la locul de muncă. Amenințările din mediul online sunt adesea subestimate sau neglijate, iar răspunsurile la incidentele de securitate sunt deseori neadecvate. În domeniul sănătății, unde procesarea și stocarea datelor sensibile ale pacienților reprezintă o componentă esențială, aceste riscuri au implicații majore. Digitalizarea accelerată și interconectivitatea sistemelor informatice aduc nu doar beneficii, ci și o complexitate crescută a vulnerabilităților. Fenomenul este agravat de lipsa de conștientizare și de insuficiența măsurilor preventive, ceea ce face ca instituțiile medicale să fie expuse unor amenințări semnificative, cu potențial de compromitere a datelor și a funcționării sistemelor.

Studiul își propune să analizeze starea actuală a securității informaționale în domeniul sănătății, identificând principalele vulnerabilități și amenințări cibernetice. Un obiectiv central este evaluarea nivelului de criticitate al informațiilor gestionate în acest sector, cu accent pe importanța protecției datelor sensibile ale pacienților. În plus, studiul explorează modalitățile prin care instituțiile medicale pot adopta standarde recunoscute internațional, precum ISO 27001 sau ISO 27014, pentru a dezvolta o cultură a securității și a implementa strategii eficiente de management al riscurilor. Ipoteza fundamentală este că o abordare structurată, bazată pe bune practici, poate reduce semnificativ expunerea la riscuri și impactul acestora asupra sistemelor informatice medicale.

Pentru realizarea cercetării, a fost utilizată o abordare analitică, combinată cu studii de caz și revizuirea literaturii de specialitate. Documentele și standardele internaționale relevante, precum ISO 27001, NIST CSF, și reglementările GDPR și HIPAA, au fost analizate pentru a identifica măsuri și practici aplicabile în contextul instituțiilor medicale. În plus, au fost investigate incidentele de securitate raportate în sectorul sănătății, cu scopul de a evidenția tiparele comune ale atacurilor cibernetice și de a înțelege impactul acestora asupra organizațiilor. Această metodologie a permis formularea unor recomandări concrete, adaptate nevoilor specifice ale instituțiilor din domeniu.

Ca rezultat sa reușit implementarea standardului ISO/IEC 27014 în cadrul IMSP AMT Centru. Această inițiativă a permis instituției să dezvolte un sistem de guvernanță eficient pentru securitatea informațiilor, aliniat cerințelor internaționale. Procesul a inclus identificarea și evaluarea riscurilor, definirea unor politici clare de protecție a datelor sensibile ale pacienților și integrarea unor măsuri proactive pentru prevenirea incidentelor cibernetice. Acest demers nu doar că a redus expunerea la amenințările cibernetice, dar a și crescut încrederea pacienților și partenerilor în capacitatea instituției de a proteja informațiile critice. Modelul implementat la IMSP AMT Centru poate servi drept exemplu pentru alte organizații din domeniul sănătății, oferind un punct de plecare pentru adoptarea standardelor similare în vederea asigurării unei securități cibernetice robuste.

ABSTRACT

In a digitized world, exposure to cyber risks is an inevitable reality, both in the personal sphere and in the workplace. Online threats are often underestimated or neglected, and responses to security incidents are often inadequate. In healthcare, where the processing and storage of sensitive patient data is an essential component, these risks have major implications. Accelerated digitization and the interconnectedness of IT systems bring not only benefits, but also an increased complexity of vulnerabilities. The phenomenon is aggravated by the lack of awareness and the insufficiency of preventive measures, which makes medical institutions exposed to significant threats, with the potential to compromise data and the functioning of systems.

The study aims to analyze the current state of health information security, identifying the main cyber vulnerabilities and threats. A central objective is to assess the level of criticality of the information managed in this sector, with an emphasis on the importance of protecting sensitive patient data. In addition, the study explores how healthcare institutions can adopt internationally recognized standards, such as ISO 27001 or ISO 27014, to develop a culture of security and implement effective risk management strategies. The fundamental assumption is that a structured approach based on best practices can significantly reduce risk exposure and their impact on medical IT systems.

To carry out the research, an analytical approach was used, combined with case studies and literature review. Relevant international documents and standards, such as ISO 27001, NIST CSF, and GDPR and HIPAA regulations, were analyzed to identify measures and practices applicable in the context of healthcare institutions. In addition, security incidents reported in the healthcare sector were investigated to highlight common patterns of cyber attacks and understand their impact on organizations. This methodology allowed the formulation of concrete recommendations, adapted to the specific needs of the institutions in the field. As a result, the ISO/IEC 27014 standard was successfully implemented within the IMSP AMT Center. This initiative allowed the institution to develop an effective governance system for information security, aligned with international requirements. The process included identifying and assessing risks, defining clear policies to protect sensitive patient data, and integrating proactive measures to prevent cyber incidents. This approach not only reduced exposure to cyber threats, but also increased patient and partner confidence in the facility's ability to protect critical information. The model implemented at the IMSP AMT Center can serve as an example for other healthcare organizations, providing a starting point for adopting similar standards to ensure robust cyber security.

CUPRINS

INTRODUCERE

În fiecare zi, suntem supuși, atât acasă, cât și la locul de muncă, la riscuri provenite din mediul online. Adesea, nu suntem conștienți de aceste amenințări, iar atunci când le identificăm, reacția noastră nu este întotdeauna adecvată. Zilnic, apar articole care discută despre incidentele de securitate și efectele lor asupra indivizilor și organizațiilor. Aceste cazuri sunt doar partea vizibilă a unui fenomen mai complex; în realitate, vulnerabilitățile noastre sunt mult mai mari decât ne imaginăm, având în vedere că riscurile din spațiul cibernetic sunt în continuă expansiune.

Mediul digital, care include infrastructurile cibernetice și informațiile care sunt procesate, stocate sau transmise, precum și acțiunile utilizatorilor, este o componentă esențială a vieții noastre. Cu toate acestea, preocuparea pentru securitatea acestuia este adesea insuficientă. Această problemă este amplificată de complexitatea tehnologiilor moderne, care aduc noi provocări ce pot avea un impact major asupra indivizilor și organizațiilor. Acțiunile malefice desfășurate online pot compromite grav funcționarea sistemelor informatice și datele asociate acestora. În contextul evoluției tehnologice rapide și al digitalizării accelerate în domeniul sănătății, securitatea informațiilor a devenit o preocupare esențială pentru toate instituțiile medicale. Studiul privind securitatea informatică în Republica Moldova evidențiază necesitatea unei abordări sistemice și dinamice în asigurarea securității IT, pe fondul intensificării atacurilor cibernetice și a complexității acestora. Deși există un cadru legislativ și standarde internaționale adoptate, monitorizarea securității IT la nivel național este insuficientă. Analiza bazată pe un sondaj arată că nivelul de securitate variază în funcție de dimensiunea organizațiilor, iar performanțele sunt semnificativ mai bune în sectorul TIC comparativ cu alte domenii, însă securitatea rămâne sub nivelul optim pentru majoritatea întreprinderilor[1].

Capitolul 1 analizează situația actuală a securității în medicină, punând accent pe vulnerabilitățile existente, amenințările cibernetice și atacurile frecvente. În continuare sunt prezentate tipurile de informații gestionate în acest sector, precum și despre nivelul lor de criticitate, subliniind importanța protecției datelor sensibile ale pacienților. De asemenea, se examinează și alte sisteme informatice care prelucrează informații critice, evidențiind interconectivitatea și riscurile asociate.

Capitolul 2 analizează și prezintă modelele existente de securitate, precum ISO 27001, NIST SP-800, NIST CSF, CIS Controls, precum și reglementările GDPR și HIPAA. Acest capitol scoate în evidență ISO 27014, subliniind relevanța sa în contextul securității informațiilor în sectorul medical și modul în care poate fi integrat în practicile curente de management al riscurilor.

În final, Capitolul 3 propune un model simplificat de securitate inspirat din standardele menționate anterior, oferind exemple concrete de implementare. Această abordare vine să faciliteze o mai bună înțelegere a modului în care instituțiile medicale pot adopta măsuri eficiente pentru a proteja datele sensibile și a asigura continuitatea serviciilor. Prin analiza detaliată a acestor aspecte, lucrarea își propune să contribuie la dezvoltarea unor strategii eficiente de securitate cibernetică în domeniul sănătății.

BIBLIOGRAFIE

[1] I. Bolun, D. Ciorbă, A. Zgureanu, R. Bulai, R. Călin, și C. Bodoga, „INFORMATICS SECURITY ASSESSMENT IN THE REPUBLIC OF MOLDOVA”, dec. 2020, doi: 10.5281/ZENODO.4288297.

[2] „LP133/2011”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://www.legis.md/cautare/getResults?doc_id=144823&lang=ro

[3] „LP48/2023”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://www.legis.md/cautare/getResults?doc_id=136732&lang=ro

[4] „LP148/2023”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://www.legis.md/cautare/getResults?doc_id=137908&lang=ro

[5] M. D. S. R. Team, „WannaCrypt ransomware worm targets out-of-date systems”, Microsoft Security Blog. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

[6] K. Young, „Cyber Case Study: Anthem Data Breach”, CoverLink Insurance - Ohio Insurance Agency. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://coverlink.com/case-study/anthem-data-breach/

[7] S. Cârlugea, „Peste 100 de spitale, afectate câteva zile de un atac cibernetic. Rețeaua e acum funcțională aproape în totalitate. Învățămintele unui atac”, Europa Liberă România, 16:57:05Z. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://romania.europalibera.org/a/spitale-afectate-de-atac-cibernetic-invatamintele-atacului/32819533.html

[8] S. Rotaru, „Atac cibernetic la Spitalul «Sf. Treime». Ce baze de date au fost blocate și ce cer atacatorii”, Radio Europa Liberă, 12:23:46Z. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://moldova.europalibera.org/a/atac-cibernetic-la-spitalul-sf-treime-ce-baze-de-date-au-fost-blocate-si-ce-cer-atacatorii-/32557221.html

[9] „ALERTĂ: Backmydata Ransomware”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://dnsc.ro/citeste/alert-backmydata-ransomware-spitale-romania

[10] „LP91/2014”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://www.legis.md/cautare/getResults?doc_id=112497&lang=ro

[11] „Cu privire la instituirea Sistemului informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://gov.md/sites/default/files/document/attachments/subiect-22-nu-558-ms-2022.pdf

[12] „Cu privire la instituirea Sistemului informațional „Constatarea medicală a nașterii și a decesului” (eCMND)”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://gov.md/sites/default/files/document/attachments/15._ms_nu-1176_-cu_privire_la_instituirea_sistemului_informational_constatarea_medicala_a_nasterii_si_decesului.pdf

[13] „Ghid de utilizare SIRSM”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: http://old.cnam.md/httpdocs/editorDir/file/Ghiduri/SIRSM/Ghid%20de%20utilizare%20-%20Prescriptor%20v2.pdf

[14] „ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

[15] National Institute of Standards and Technology, „The NIST Cybersecurity Framework (CSF) 2.0”, National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, feb. 2024. doi: 10.6028/NIST.CSWP.29.

[16] „CIS Control 1: Inventory and Control of Enterprise Assets - CIS Controls Self Assessment Tool Document Library”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://cas.docs.cisecurity.org/en/latest/source/Controls1/

[17] „General Data Protection Regulation (GDPR)”. Data accesării: 2 decembrie 2024. [Online]. Disponibil la: https://www.ncsc.gov.uk/information/gdpr

[18] A. Lachi, „IMPLEMENTAREA UNEI POLITICI DE SECURITATE EFICIENTE”.

[19] A. Stoica, „APLICABILITATEA ISO/IEC27014:2020 ÎN SISTEMELE INFORMAȚIONALE DIN DOMENIUL SĂNĂTĂȚII”, 2024.