PROTECȚIA DATELOR ÎN ECOSISTEMUL ACADEMIC DIGITAL PRIN APLICAREA STANDARDELOR ISO PRIVIND SECURITATEA INFORMAȚIEI

DATA PROTECTION IN THE DIGITAL ACADEMIC ECOSYSTEM BY APPLYING ISO STANDARDS ON INFORMATION SECURITY

Elena BORDIAN, șefa Bibliotecii Republicane Tehnico-Științifice, Institutul Național de Cercetări Economice, ASEM

Elena LUPU, șefă de secție Colecții Speciale, Biblioteca Republicană Tehnico-Științifică a INCE, ASEM

Ecaterina COȘLEȚ, bibliotecar principal, secția Colecții Speciale, Biblioteca Republicană Tehnico-Științifică a INCE, ASEM

Elena BORDIAN, head of the library, The Technical-Scientific Republican Library of NIER, Academy of Economic Studies of Moldova
ORCID: 0000-0002-2052-7323
e-mail: bordian.elena@ase.md

Elena LUPU, Head of Special Collections Section, The Technical-Scientific Republican Library of NIER, Academy of Economic Studies of Moldova
ORCID: 0000-0001-9065-4638
e-mail: elenalmd@gmail.com

Ecaterina COȘLEȚ, Principal Librarian, Special Collections Section, The Technical-Scientific Republican Library of NIER, Academy of Economic Studies of Moldova
ORCID: 0000-0003-0965-1208
e-mail: ecaterinacoslet3@gmail.com

CZU: 004.056:006.44:378
DOI: 10.46727/c.v4.19-20-03-2026.p387-396

Abstract. The paper analyzes the conceptual framework of information security, highlighting its main components – confidentiality, integrity, authenticity and availability – as well as the related concepts of risk, vulnerability and threat. At the same time, the legal and ethical obligations regarding the protection of user data are examined, in correlation with the national legislative framework of the Republic of Moldova and with the regulations on access to information and the protection of personal data. The emphasis is placed on the role of international standards from the ISO/IEC 27000 family, which provide a systemic framework for the implementation of information security management in academic institutions. The risks specific to the digital academic ecosystem are analyzed, including cyber attacks, unauthorized access and misuse of information resources. The importance of complying with licensing agreements for access to scientific databases and the role of libraries in protecting intellectual property are highlighted. In this regard, institutional security policies, digital education of users and the implementation of appropriate technical measures become para-

mount for maintaining a secure academic environment. Data protection and information security are strategic components of modern academic governance, and the application of ISO/IEC 27000 standards facilitates the development of a resilient, responsible and sustainable digital ecosystem.

Keywords: information security; academic ecosystem; data protection; ISO standards.

Introducere

Evoluțiile recente în domeniul tehnologiilor informaționale au determinat o reconfigurare profundă a mediului academic, în care procesele educaționale și de cercetare sunt tot mai mult mediate de infrastructuri digitale. Universitățile și bibliotecile academice operează astăzi într-un ecosistem complex, caracterizat prin interconectivitate, volum mare de date și acces distribuit la diverse resurse informaționale. Gestionarea eficientă a informației este inseparabilă de asigurarea securității acesteia. Creșterea dependenței de platforme digitale, servicii cloud și sisteme informatice integrate amplifică expunerea instituțiilor la riscuri cibernetice, breșe de securitate și utilizări neautorizate ale datelor. Prin urmare, protecția datelor devine o dimensiune strategică a funcționării instituțiilor academice, fiind necesară pentru protejarea integrității proceselor educaționale și a rezultatelor cercetării.

În acest context, adoptarea unor cadre normative recunoscute la nivel internațional, precum standardele din familia ISO/IEC 27000, reprezintă o abordare sistemică a managementului securității informației. Aceste standarde oferă principii, metode și controale care permit instituțiilor să identifice vulnerabilitățile, să evalueze riscurile și să implementeze măsuri adecvate de protecție. Astfel, integrarea standardelor ISO în practicile instituționale nu doar că sprijină conformitatea cu reglementările în vigoare, dar și contribuie la consolidarea unui model de guvernanță digitală responsabil, bazat pe prevenție, transparență și reziliență. În mod particular, în cadrul bibliotecilor academice, acest demers capătă o importanță sporită, având în vedere rolul acestora în gestionarea resurselor informaționale și în protejarea datelor utilizatorilor într-un mediu digital dinamic.

Metodele și materialele aplicate

Prezenta cercetare are la bază analiza documentară a principalelor acte normative care reglementează securitatea informației în Republica Moldova. Demersul metodologic adoptat este de natură calitativă, fiind orientat spre interpretarea conținutului legislativ și corelarea acestuia cu practicile instituționale specifice mediului academic. În acest sens, lucrarea integrează următoarele metode și instrumente de cercetare:

– analiza documentară a standardelor relevante elaborate de Organizația Internațională de Standardizare [4];
– analiza cadrului legislativ național din Republica Moldova, în domeniul securității informației și protecției datelor;

– aplicarea unei abordări calitative, bazate pe evaluarea riscurilor și analiza măsurilor instituționale adoptate pentru diminuarea acestora.

Această abordare metodologică permite o înțelegere integrată a relației dintre cadrul normativ, standardele internaționale și practicile instituționale, evidențiind gradul de aliniere a instituțiilor academice la cerințele contemporane de securitate a informației.

Definirea conceptelor cheie

Securitatea informațiilor reprezintă un domeniu fundamental al guvernanței digitale, care include ansamblul măsurilor, politicilor și tehnologiilor destinate protejării informațiilor împotriva accesului neautorizat, utilizării abuzive, modificării sau distrugerii. În conformitate cu principiile promovate de Organizația Internațională de Standardizare, în special prin standardele din familia ISO/IEC 27000 [5], securitatea informațiilor urmărește asigurarea unor proprietăți fundamentale care garantează funcționarea sigură și fiabilă a sistemelor informaționale.

În acest cadru conceptual, principalele proprietăți ale securității informației sunt:

- *Confidențialitatea*, care asigură accesul exclusiv al persoanelor autorizate la informații, prevenind divulgarea sau utilizarea neautorizată;
- *Integritatea*, care garantează menținerea informațiilor în forma lor originală, fără modificări neautorizate pe parcursul stocării sau transmiterii;
- *Autenticitatea*, care confirmă identitatea sursei informației și veridicitatea acesteia;
- *Nerepudierea (apelabilitatea)*, care permite demonstrarea faptului că autorul unei informații nu poate nega ulterior crearea sau transmiterea acesteia.

În contextul sistemelor informatice, aceste caracteristici sunt completate de proprietăți operaționale de bază pentru funcționarea eficientă a infrastructurii digitale. Astfel, *fiabilitatea* reflectă capacitatea sistemului de a funcționa conform așteptărilor în condiții normale și excepționale, iar *precizia* vizează executarea corectă și completă a operațiunilor. *Controlul accesului* asigură aplicarea coerentă a drepturilor diferențiate asupra resurselor informaționale, în timp ce *auditabilitatea* permite verificarea și evaluarea continuă a componentelor sistemului. De asemenea, *controlul identității* garantează autenticitatea utilizatorilor prin mecanisme adecvate de autentificare, iar *toleranța la erori* contribuie la menținerea funcționalității sistemului chiar și în condiții adverse.

Literatura de specialitate și standardele internaționale definesc, totodată, o serie de concepte conexe esențiale pentru managementul securității informației. De exemplu: *amenințarea* reprezintă orice eveniment potențial, intenționat sau accidental, care poate afecta negativ procesele și sistemele organizaționale, în timp ce *vulnerabilitatea* desemnează o slăbiciune ce poate fi exploatată pentru a produce un impact nedorit. *Pierderile* reflectă consecințele negative, de natură financiară sau operaționa-

lă, rezultate din materializarea amenințărilor, iar *riscul* este definit ca o combinație între probabilitatea producerii unui eveniment și impactul acestuia asupra organizației, conform ISO/IEC 27001[4].

În ansamblu, securitatea informațiilor depășește dimensiunea strict tehnologică, presupunând o abordare integrată, care îmbină componente organizaționale, juridice și tehnice, cu scopul de a asigura continuitatea operațională și consolidarea încrederii în sistemele informaționale.

Protecția datelor utilizatorilor – obligație juridică și etică

În contextul transformării digitale a mediului academic, protecția datelor utilizatorilor devine o responsabilitate primordială, cu dublă dimensiune – juridică și etică. Bibliotecile academice nu mai gestionează doar colecții fizice, dar operează cu volume semnificative de date generate prin utilizarea serviciilor digitale, platformelor de acces la resurse electronice și sistemelor informatice integrate. În activitatea curentă, aceste instituții procesează o varietate de date, inclusiv date de identificare (nume, afiliere instituțională, adrese de e-mail), informații privind comportamentul informațional (istoric de împrumut, interogări în catalogul online, acces la baze de date științifice), precum și date statistice utilizate în scopuri de raportare și analiză instituțională. Gestionarea acestor date implică respectarea unor principii fundamentale, precum legalitatea prelucrării, minimizarea datelor colectate, transparența utilizării și asigurarea confidențialității. Din perspectivă juridică, bibliotecile trebuie să se conformeze cadrului normativ privind protecția datelor cu caracter personal, implementând politici și proceduri interne care să reglementeze accesul, stocarea și utilizarea informațiilor. În același timp, dimensiunea etică presupune responsabilitate față de utilizatori, prin protejarea vieții private și evitarea utilizării abuzive sau excesive a datelor colectate.

Riscurile asociate unei gestionări inadecvate a datelor sunt semnificative. Orice breșă de securitate poate conduce la divulgarea informațiilor personale, afectând direct utilizatorii și generând consecințe juridice pentru instituție. În plus, astfel de incidente pot compromite reputația bibliotecii și pot afecta relațiile contractuale cu furnizorii de resurse electronice, care impun standarde stricte privind securitatea accesului și protecția datelor. În acest context, atât protecția datelor personale ale utilizatorilor, cât și protecția resurselor de informare, trebuie abordate ca o componentă strategică a managementului informației, integrată în politicile instituționale și susținută prin implementarea unor măsuri tehnice și organizaționale adecvate. Bibliotecile academice își consolidează, în aceste condiții, rolul de furnizori de servicii informaționale sigure, contribuind la dezvoltarea unui mediu academic bazat pe încredere, responsabilitate și respectarea normelor etice și legale.

Cadrul legislativ național privind siguranța informației în Republica Moldova: în Republica Moldova, siguranța informației este o prioritate strategică la nivel național, acest domeniu fiind reglementat printr-un ansamblu de acte normative care stabilesc principiile, responsabilitățile și mecanismele de protecție a informației. Cadrul legislativ național privind siguranța informației include reglementări care

vizează protecția datelor cu caracter personal, securitatea sistemelor informatice și asigurarea confidențialității, integrității și disponibilității informațiilor. Printre cele mai relevante acte normative se regăsesc:

- Programul național de securitate cibernetică pentru perioada 2026–2030, aprobat prin Hotărârea Guvernului nr. 821 din 29 decembrie 2025 [8]. Acest document strategic stabilește direcțiile principale de dezvoltare în domeniul securității cibernetice, incluzând: consolidarea capacităților instituționale de prevenire și răspuns la incidente; dezvoltarea infrastructurilor critice securizate; creșterea nivelului de educație și conștientizare în domeniul securității informației; alinierea la standarde și practici europene. Programul evidențiază importanța cooperării interinstituționale și a parteneriatelor public-private în gestionarea riscurilor cibernetice.

- Legea nr. 148 din 9 iunie 2023 privind accesul la informațiile de interes public [9], reglementează dreptul cetățenilor de a accesa informații deținute de autoritățile publice. Aceasta stabilește principiile transparenței și deschiderii instituționale, obligațiile autorităților de a furniza informații, limitele accesului, în cazul informațiilor sensibile. Această lege creează pentru biblioteci și instituții academice un echilibru între accesul liber la informație și protecția datelor sensibile.

- Legea nr. 195 din 25 iulie 2024 privind protecția datelor cu caracter personal [11], este un cadru modern, aliniat la standardele europene, pentru gestionarea datelor personale. Aceasta reglementează principiile prelucrării datelor (legalitate, transparență, minimizare), drepturile persoanelor vizate, responsabilitățile operatorilor de date, măsurile de securitate necesare. În mediul academic, aplicarea acestei legi este necesară pentru protejarea datelor studenților, cercetătorilor și utilizatorilor de bibliotecă.

- Legea nr. 299 din 21 decembrie 2017 privind aprobarea Concepției securității informaționale a Republicii Moldova [10], stabilește cadrul strategic general pentru protecția informației la nivel național. Sunt definite obiectivele securității informaționale, amenințările și riscurile majore, mecanismele de protecție instituțională. Concepția rămâne documentul de referință pentru dezvoltarea politicilor în domeniu.

Pentru instituțiile publice din domeniul culturii și educației, elaborarea cadrului legislativ național se bazează pe experiențe și reglementări internaționale, care presupune implementarea politicilor de securitate a informației. protejarea datelor utilizatorilor și a resurselor digitale, controlul accesului la baze de date licențiate, respectarea drepturilor de proprietate intelectuală.

Bibliotecile, în calitate de gestionari ai resurselor informaționale, au un rol primordial în promovarea securității informației și în asigurarea unui acces sigur și legal la cunoaștere. În acest context, un reper conceptual și operațional este **Declarația IFLA (International Federation of Library Associations and Institutions)** privind securitatea cibernetică (2022) [3]. Documentul recomandă bibliotecilor, care dețin control total sau parțial asupra propriilor sisteme informatice, să implementeze politici și măsuri tehnice orientate spre minimizarea riscurilor. Un principiu central îl reprezintă limitarea colectării și stocării datelor, inclusiv prin ștergerea istoricului de utilizare după perioade definite, în conformitate cu principiul minimizării datelor.

Declarația subliniază importanța implementării controalelor de securitate la nivel de infrastructură și puncte finale (stații de lucru, servere), în acord cu bunele practici internaționale reflectate de standarde precum ISO/IEC 27001, ISO/IEC 27002 și ISO/IEC 27032. Deși aceste standarde nu sunt întotdeauna accesibile integral, ele oferă un cadru de referință valoros pentru dezvoltarea sistemelor de securitate informațională.

La nivel instituțional, toate bibliotecile sunt îndemnate să elaboreze și să publice politici clare privind utilizarea acceptabilă a sistemelor informatice, protecția datelor și securitatea informației. Aceste politici trebuie să definească explicit tipurile de date colectate, scopul utilizării acestora, precum și procedurile aplicabile în cazul incidentelor de securitate. De asemenea, este semnificativă formarea continuă a personalului, astfel încât acesta să dețină competențe de bază în domeniul securității cibernetice și să poată aplica practici corecte în activitatea profesională. În Declarație este evidențiat și rolul bibliotecilor în dezvoltarea alfabetizării digitale a utilizatorilor. Prin activități educaționale și de informare, bibliotecile contribuie la creșterea capacității utilizatorilor de a identifica și evita amenințările cibernetice, consolidând astfel reziliența comunității academice.

La nivel macro, guvernele au responsabilitatea de a asigura resursele necesare și cadrul normativ adecvat pentru implementarea măsurilor de securitate, precum și de a promova politici care să combine eficiența protecției cibernetice cu respectarea drepturilor fundamentale, în special a dreptului la viață privată. În ansamblu, Declarația IFLA (2022)[4] promovează o abordare integrată și echilibrată a securității cibernetice în biblioteci, în care protecția datelor, transparența și responsabilitatea instituțională converg spre crearea unui mediu informațional sigur, etic și sustenabil.

Accesul la resursele informaționale științifice în mediul academic contemporan este reglementat prin acorduri de licențiere încheiate între instituțiile de învățământ superior și furnizori internaționali de conținut, precum Elsevier, Springer, EBSCO Information Services, Wiley, Taylor & Francis sau ProQuest. Ele stabilesc în mod explicit condițiile de utilizare a conținutului digital, incluzând limitele de descărcare, interdicția utilizării automate (de tip crawling sau scraping), cerințele de autentificare securizată și obligația protejării credențialelor (date de conectare, nume de utilizator și parolă) instituționale. Respectarea acestor prevederi nu are doar o dimensiune juridică, dar și una etică. Practicile abuzive – precum descărcările masive neautorizate, distribuirea ilegală a materialelor sau partajarea conturilor – pot conduce la suspendarea accesului pentru întreaga comunitate academică, afectând direct activitatea de cercetare și procesul educațional. Mecanismele de control al accesului și securitatea datelor devin instrumente necesare pentru protejarea interesului academic colectiv și pentru asigurarea unei utilizări sustenabile a resurselor informaționale. În paralel, bibliotecile academice gestionează un volum semnificativ de resurse digitale proprii, prin intermediul repozitoriilor instituționale și al platformelor de tip open access, precum DSpace, EPrints sau Fedora Commons. Aceste infrastructuri includ articole științifice, teze de doctorat, rapoarte de cercetare, seturi de date deschise și alte produse academice, a căror gestionare implică responsabilități sporite privind securitatea informației și protecția proprietății intelectuale.

Implementarea politicilor riguroase de securitate contribuie la prevenirea plagiatului, la evitarea modificărilor neautorizate ale metadatelor și conținutului, precum și la respectarea drepturilor morale și patrimoniale ale autorilor. De asemenea, este asigurată conformitatea cu embargourile editoriale și cu reglementările privind accesul deschis[1]. În așa mod, protecția datelor depășește dimensiunea strict tehnologică, fiind incluse într-un cadru mai amplu al politicilor de integritate academică și contribuie la fortificarea încrederii în ecosistemul cercetării și al diseminării rezultatelor științifice.

Ecosistemul academic digital – riscuri și vulnerabilități

Ecosistemul academic digital reprezintă o infrastructură complexă, construită pe interconectarea unor platforme și servicii obligatorii pentru educație și cercetare. Acesta include: *biblioteci electronice*, *repozitorii instituționale*, *baze de date științifice și platforme bibliometrice*, care, împreună, susțin un mediu colaborativ de generare, diseminare și valorificare a cunoașterii. Prin facilitarea accesului rapid la informație și prin integrarea resurselor la nivel global, acest ecosistem contribuie semnificativ la dezvoltarea comunicării academice. Dar, complexitatea și gradul ridicat de interconectare generează o serie de riscuri și vulnerabilități care necesită o gestionare atentă. Printre principalele amenințări se numără accesul neautorizat la datele personale ale utilizatorilor, pierderea sau alterarea informațiilor și atacurile cibernetice, precum phishing-ul sau ransomware-ul, care pot afecta funcționarea sistemelor informatice. De asemenea, există riscuri asociate scurgerilor de date privind rezultatele cercetării sau elemente de proprietate intelectuală, ceea ce poate avea consecințe asupra integrității științifice și competitivității instituționale. Repozitoriile instituționale, în absența unor măsuri adecvate de securitate, pot fi vulnerabile la compromiterea conținutului sau la accesul neautorizat.

Un alt aspect critic îl reprezintă utilizarea necorespunzătoare a credențialelor (date de conectare, nume de utilizator și parolă) academice și a conturilor instituționale, care poate facilita accesul ilegal la resurse licențiate și poate genera încălcări ale politicilor de utilizare. Astfel de situații pot afecta nu doar securitatea informației, dar și relațiile contractuale cu furnizorii de baze de date. În acest context, este necesară implementarea unor măsuri integrate de securitate, care să combine soluții tehnice, politici instituționale și educație digitală a utilizatorilor [1]. Doar printr-o abordare coerentă și preventivă poate fi asigurată protecția resurselor informaționale și menținerea unui mediu academic sigur, credibil și sustenabil.

Relevanța standardelor ISO/IEC 27000 în mediul academic

Organizația Internațională de Standardizare are un rol fundamental în elaborarea standardelor internaționale aplicabile într-o varietate de domenii, inclusiv producție, tehnologie, management și siguranță. Standardele din familia ISO/IEC 27000 [5; 6], oferă un cadru conceptual și metodologic integrat pentru protecția datelor

și gestionarea riscurilor în mediul digital. Aceste standarde promovează o abordare sistemică, bazată pe implementarea unui Sistem de Management al Securității Informației (SMSI), care permite organizațiilor să identifice, să evalueze și să controleze riscurile asociate informației.

Evoluția inițială a SMSI a avut la bază standardul ISO/IEC 27001 [4], în anii 1990, când British Standards Institution a elaborat standardul BS 7799, considerat primul cadru formal dedicat managementului securității informației, fiind supus periodic procesului de revizuire, menit să reflecte dinamica accelerată a tehnologiilor informaționale. În anul 2005, Organizația Internațională de Standardizare, în colaborare cu Comisia Electrotehnică Internațională, a preluat și dezvoltat acest cadru, publicând prima versiune a standardului internațional ISO/IEC 27001:2005. Edițiile ISO/IEC 27001:2013 și ISO/IEC 27001:2022 [4] au introdus cerințe actualizate privind managementul riscurilor, controlul securității și alinierea la noile realități digitale care permit organizațiilor să adopte un sistem de management al securității informației adaptat mediului contemporan, facilitând totodată obținerea certificării conform standardului și consolidarea încrederii în capacitatea lor de a proteja informațiile.

Cele mai relevante standarde din familia ISO/IEC 27000 pentru mediul academic sunt prezentate în Tabelul 1.

Tabelul 1. Standarde din grupul ISO/IEC 27000 pentru mediul academic

STANDARDE DIN GRUPUL ISO/IEC 27000 PENTRU MEDIUL ACADEMIC	
ISO/IEC 27000: 2018	Tehnici de securitate – Sisteme de management al securității informațiilor - Prezentare generală și vocabular
ISO/IEC 27001: 2022	Securitatea informațiilor, securitatea cibernetică și protecția confidențialității – Sisteme de management al securității informațiilor – Cerințe
ISO/IEC 27002: 2022	Securitatea informațiilor, securitatea cibernetică și protecția confidențialității – Controale de securitate a informațiilor
ISO/IEC 27003: 2017	Tehnici de securitate – Sisteme de management al securității informațiilor – Ghid
ISO/IEC 27004: 2016	Tehnici de securitate – Managementul securității informațiilor - Monitorizare, măsurare, analiză și evaluare
ISO/IEC 27005: 2022	Securitatea informațiilor, securitatea cibernetică și protecția confidențialității. Îndrumări privind gestionarea riscurilor de securitate a informațiilor
ISO/IEC 27006-1: 2024	ISO/IEC 27006-1:2024 Securitatea informațiilor, securitatea cibernetică și protecția confidențialității – Cerințe pentru organismele care asigură auditul și certificarea sistemelor de management al securității informațiilor Partea 1: Generalități
ISO/IEC 27032:2023	Securitate cibernetică – Linii directoare pentru securitatea internetului
ISO/IEC 27102: 2019	Securitatea informațiilor, securitatea cibernetică și protecția confidențialității – Linii directoare pentru aplicarea ISO/IEC 27001 și a standardelor conexe în sprijinul asigurărilor cibernetice

Utilizarea standardelor ISO/IEC 27000, oferă o abordare sistematică a protecției datelor în ecosistemul academic digital, inclusiv în biblioteci. Aceste standarde ajută la stabilirea unui sistem eficient de management al securității informațiilor (SMSI), la minimizarea riscului de încălcare a datelor și la respectarea cerințelor legale. Bibliotecile, ca centre pentru prelucrarea a datelor de cercetare, pot utiliza aceste standarde pentru a spori încrederea utilizatorilor, asigurând confidențialitatea, integritatea și disponibilitatea informațiilor. Transformarea digitală a bibliotecilor universitare necesită integrarea unor astfel de cadre de reglementare pentru dezvoltarea durabilă a ecosistemului.

Concluzii. Protecția datelor în ecosistemul academic digital se conturează ca o dimensiune fundamentală a guvernanței instituționale, depășind sfera tehnică și integrându-se în strategiile de dezvoltare organizațională. Standardele elaborate de Organizația Internațională de Standardizare din familia ISO/IEC 27000 oferă un cadru coerent și robust pentru organizarea securității informației și protecția datelor cu caracter personal. Analiza realizată permite formularea unui grup de direcții fundamentale care reflectă principalele priorități în domeniu:

- structurarea unui sistem coerent de management al securității informației, adaptat specificului mediului educațional și de cercetare;
- elaborarea și aplicarea politicilor instituționale de securitate a informației;
- utilizarea criptării pentru datele sensibile și prevenirea accesului neautorizat la informații critice;
- realizarea periodică a auditurilor de securitate;
- identificarea vulnerabilităților infrastructurii IT și adoptarea măsurilor corective bazate pe evaluarea riscurilor;
- dezvoltarea continuă a competențelor personalului și utilizatorilor în domeniul securității informației;
- formarea culturii organizaționale orientate spre prevenție, responsabilitate și utilizare sigură a resurselor digitale.

Implementarea unui Sistem de Management al Securității Informației (SMSI), conform ISO/IEC 27001, în corelație cu cadrul legislativ național contribuie la edificarea unui mediu academic sigur, sustenabil și competitiv la nivel internațional. Respectarea standardelor ISO favorizează dezvoltarea unui model viabil de guvernanță digitală, orientat spre prevenție, securitate și consolidarea rezilienței instituționale.

BIBLIOGRAFIE

1. ALEXEI, Arina. Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. *Journal of Social Sciences*, 2021, vol. 4, nr. 1, pp. 84–94. ISSN 2587-3490, eISSN 2587-3504. Disponibil: https://doi.org/10.52326/jss.utm.2021.4(1).11 [accesat 2026-03-04].
2. EUR-Lex. Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (Text cu rele-

vanță pentru SEE) Disponibil: https://eur-lex.europa.eu/eli/dir/2022/2555/oj [accesat 2026-03-06].

3. INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS. *IFLA Statement on Cybersecurity*. 13 aprilie 2022. Disponibil: https://www.ifla.org/news/ifla-statement-on-cybersecurity/ [accesat 2026-03-11].
4. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Geneva: ISO, 2022. Disponibil: https://www.iso.org/standard/27001 [accesat 2026-03-10].
5. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. Geneva: ISO, 2022. Disponibil: https://www.iso.org/standard/75652.html [accesat 2026-03-12].
6. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27005:2022 Information security risk management*. Geneva: ISO, 2022. Disponibil: https://www.iso.org/standard/80585.html [accesat 2026-03-12].
7. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*. Geneva: ISO, 2025. Disponibil: https://www.iso.org/standard/27701 [accesat 2026-03-12].
8. Hotărâre cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026–2030: nr. 821 din 29-12-2025. *Monitorul Oficial al Republicii Moldova*, 2026, nr. 656–658, art. 838. ISSN 2587-389X, eISSN 2587-3903. Disponibil: https://www.legis.md/cautare/getResults?doc_id=152334&lang=ro [accesat 2026-03-06].
9. Lege privind accesul la informațiile de interes public: nr. 148 din 09.06.2023. *Monitorul Oficial al Republicii Moldova*, 2023, nr. 234, art. 410. ISSN 2587-389X, eISSN 2587-3903. Disponibil: https://www.legis.md/cautare/getResults?doc_id=137908&lang=ro [accesat 2026-03-06].
10. Lege privind aprobarea Concepției securității informaționale a Republicii Moldova: nr. 299 din 21.12.2017. *Monitorul Oficial al Republicii Moldova*, 2018, nr. 48–57, art. 122. ISSN 2587-389X, eISSN 2587-3903. Disponibil: https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro [accesat 2026-03-05].
11. Lege privind protecția datelor cu caracter personal: nr. 195 din 25.07.2024. *Monitorul Oficial al Republicii Moldova*, 2024, nr. 367–369, art. 574 ISSN 2587-389X, eISSN 2587-3903. Disponibil: https://www.legis.md/cautare/getResults?doc_id=144681&lang=ro [accesat 2026-03-02].
12. Lege privind securitatea cibernetică: nr. 48 din 16.03.2023. *Monitorul Oficial al Republicii Moldova*, 2023, nr. 151–153, art. 325 ISSN 2587-389X, eISSN 2587-3903 [online]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=136732&lang=ro [accesat 2026-03-02].