Digital Library Perspectives

Securing digital library services and ensuring data privacy in Ukrainian public libraries

Yurii Horban
Department of Information and Public Relations, Kyiv National University of Culture and Arts, Kyiv, Ukraine

Olena Hryhorevska
Department of Information Communications, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine, and

Tetiana Novalska, Nataliia Kobyzhcha, Vladyslav Kasian, Olena Karakoz, Liudmyla Prokopenko and Viktoriia Pylypiv
Department of Information and Public Relations, Kyiv National University of Culture and Arts, Kyiv, Ukraine

Received 31 December 2025
Revised 12 March 2026
Accepted 25 May 2026

Abstract

Purpose – This study aims to map the specific terrain of prevalent security threats to digital library services, dissect the critical privacy risks associated with patron information and culminate in the proposal of a resilient framework designed to address these multifaceted challenges.

Design/methodology/approach – To ground this analysis in empirical reality, a quantitative survey of 127 Ukrainian public library professionals was conducted. The study synthesizes established cybersecurity best practices, data protection principles and current information science literature to examine vulnerabilities ranging from technical infrastructure to human-factor risks.

Findings – The results reveal a critical governance gap: 70% of surveyed institutions operate without a formal information security policy, and 85% lack full-time information technology (IT) staff (with 60% having no dedicated IT resource at all). These findings replace previous assumptions with concrete data, highlighting the urgency of the issue. The investigation identifies a spectrum of common threats, including malware, phishing and denial-of-service attacks and highlights the profound privacy implications of the Diia.Digital Education initiative.

Originality/value – This research replaces previous assumptions with concrete data regarding the security maturity of libraries in a war zone, specifically analyzing the risks of the Diia ecosystem integration. It proposes a conceptual framework with actionable strategies tailored to empower Ukrainian public libraries to fortify their digital offerings and champion user data privacy.

Keywords Public libraries, Digital libraries, Cybersecurity, Data privacy, Information security, User data protection

Paper type Research paper

1. Introduction

The operational heart of the modern public library has migrated from the physical stacks to the digital infrastructure, a profound shift driven by the ubiquitous nature of internet services. This digital transformation has enabled libraries to extend their mission far beyond their architectural confines, offering citizens unprecedented access to information, learning modules and vast repositories of cultural knowledge through tools like online catalogs, e-

Digital Library Perspectives

2059-5816
DOI 10.1108/DLP-12-2025-0307

resource platforms and virtual reference services (King, 2020; Mojjada, 2025). Within Ukraine, this evolution is not merely a technological upgrade but a vital component of community development, the cultivation of digital literacy and the strengthening of democratic participation, making the enhancement of these digital offerings a matter of strategic national importance (Lukianova and Ovcharuk, 2023).

However, this deepened reliance on networked platforms and internet-based services introduces a parallel and pressing reality: a significant exposure to a complex and evolving landscape of information security threats and data privacy risks. The very systems designed to democratize knowledge can become vectors for sophisticated cyberattacks that target vulnerabilities in software, network configurations and, most frequently, human behavior. At the same time, the responsible stewardship of user data – a necessary component for personalizing services and managing resources effectively – presents profound ethical and legal challenges that must be navigated with the utmost care (Williamson and Prybutok, 2024).

For Ukraine's public libraries, these universal challenges are often amplified by a specific set of contextual factors. These include constrained financial resources for acquiring advanced IT infrastructure, a wide spectrum of digital literacy among both staff and patrons and a volatile geopolitical environment that can directly influence the intensity and nature of cyber threats. Since the escalation of the conflict in 2022, Ukrainian institutions have faced a hybrid threat landscape where cyber aggression parallels kinetic warfare. Libraries, as custodians of national heritage and community hubs, are not exempt from this targeting.

The central aim of this investigation, therefore, is to dissect the security vulnerabilities and data privacy risks that are intrinsically linked to the digital services provided by public libraries in Ukraine. Specifically, this paper sets out to achieve the following objectives:

- *Identify and categorize threats:* To identify and categorize the principal information security threats currently targeting digital library services within the Ukrainian context, leveraging data from the computer emergency response team of Ukraine (CERT-UA) and empirical survey data.
- *Analyze privacy risks:* To analyze the primary data privacy challenges that arise from the collection, processing, storage and dissemination of patron data, with a specific focus on the integration of the Diia government service ecosystem into library terminals.
- *Assess empirical reality:* To present and analyze the results of a survey of 127 library professionals, providing a quantitative baseline for the state of cybersecurity governance in the sector.
- *Propose strategic framework:* To propose a cohesive set of strategies, unified within a conceptual framework, designed to empower Ukrainian public libraries to mitigate these risks, strengthen their overall cybersecurity posture and ensure robust protection for user data privacy.

Effectively confronting these issues is of paramount importance. The task at hand extends beyond the mere protection of institutional assets or user information; it is fundamentally about preserving the deeply-rooted public confidence in libraries as safe, neutral and reliable havens for knowledge and inquiry. This study seeks to furnish librarians, IT professionals and policymakers in Ukraine with insightful analysis and pragmatic, forward-thinking recommendations.

2. Literature review

The scholarly discourse surrounding the fortification of digital library services and the safeguarding of user privacy has evolved from a niche concern into a central pillar of

information science and security studies (Witt, 2017; Broeders *et al.*, 2023). In the pioneering days of digital libraries, the grand mission was focused squarely on universal access and elegant interoperability. The digital locks, reinforced walls and vigilant security guards were often an architectural afterthought. Now, however, as these systems have become the core circulatory system for knowledge in many institutions, the undeniable necessity of robust security protocols has moved from the footnotes to the headline (Nehra and Bansode, 2024).

2.1 The global threat landscape

The digital ecosystem these libraries inhabit is teeming with a diverse threat landscape. The modern repository of threats is vast, ranging from digital plagues like viruses, spyware and the particularly pervasive threat of ransomware, to the cunning social mimicry of phishing schemes designed to trick the unwary and the brute-force digital traffic jams of distributed denial of service attacks (Aslan *et al.*, 2023). As the work of EL Yamani *et al.* (2024) highlights, the nature of these network assaults is in constant flux, demanding proactive and adaptive defense mechanisms.

For a digital library, the consequence of such a breach is not merely an institutional inconvenience; it can mean a catastrophic disruption of service, significant financial loss, a tarnishing of public trust and, most critically, the exposure of sensitive user information (George *et al.*, 2024). The targeting of academic and public institutions has become a global trend, but the intensity varies by region.

2.2 Cyber humanities and cognitive warfare in conflict zones

In the context of armed conflict, the destruction or manipulation of digital archives is not merely collateral damage but a deliberate tactic. Recent scholarship in "cyber humanities" emphasizes that securing digital cultural heritage is deeply intertwined with national identity and resilience (Bellini, 2024; Bellini and Degl'Innocenti, 2025). During the Russo-Ukrainian war, the targeting of cultural institutions represents a form of "cultural cleansing" and "cognitive warfare," wherein cyber operations are designed to destabilize public trust, erase historical memory and manipulate the information environment (Alcala, 2022; Deppe and Gary, 2024; Nguyen, 2024). Consequently, public libraries are no longer passive repositories; they are active frontline defenders of digital cultural property. This elevated threat requires institutions to transition from basic IT hygiene to comprehensive "cyber resilience," focusing on the ability to anticipate, withstand and rapidly recover from sophisticated cyber-physical disruptions (Alhidaifi *et al.*, 2024).

2.3 Data privacy and regulatory frameworks

Beyond fending off external attacks, a more profound ethical challenge lies in navigating the complex currents of data privacy, a domain now governed by a sophisticated Web of regulations. The European Union's (EU) general data protection regulation (GDPR) has effectively set a global standard, championing principles that are vital for library ethics: data minimization (the notion that one should not collect a user's entire life story just to check out a digital book), purpose limitation and the fundamental right of individuals to understand and control their own digital footprint (Schütz, 2022).

Although Ukraine is not an EU member, its own data protection legislation is on a trajectory of harmonization with these European standards, making the principles of GDPR a vital framework for best practice (Dudyk *et al.*, 2024). In the sacred context of a library, where intellectual freedom is paramount, the confidentiality of user data – encompassing everything from names and contact details to borrowing histories and search queries – is an

ethical cornerstone (Velmurugan, 2024). The rise of "surveillance capitalism," as noted by Sedrati and Sidi Athmane (2024), only amplifies the societal risks of unchecked data analysis, making the library's role as a guardian of privacy more critical than ever.

To operationalize these legal requirements, institutions typically look to domain-specific frameworks. The International Federation of Library Associations and Institutions (IFLA) and the American Library Association (ALA) provide robust privacy guidelines that emphasize the ethical imperative of protecting patron data. Still, translating these library-specific ethics into technical reality requires integration with broader cybersecurity standards, such as the ISO/IEC 27001 framework for Information Security Management Systems (ISMS). Unfortunately, existing literature shows a significant gap in adapting complex frameworks like ISO 27001 for under-resourced cultural institutions, a gap this study aims to address practically.

2.4 The gap between theory and practice

When researchers examine the on-the-ground reality of implementing these security and privacy ideals, a consistent picture emerges. Studies frequently point to a classic institutional struggle: the noble mission of open access clashing with the pragmatic need for security controls, often waged with limited budgets, a shortage of dedicated IT security personnel and a gap in security awareness among staff who are, first and foremost, information professionals, not cybersecurity experts (Khan *et al.*, 2021; Ulven and Wangen, 2021; Kotoroi, 2023).

While research into Ukraine's broader digital transformation has often highlighted the need for infrastructural development and policy alignment (Kniazieva *et al.*, 2023), a specific scholarly focus on the unique intersection of digital library services, information security and data privacy within the context of Ukrainian public libraries remains largely uncharted territory. This paper contributes to filling this gap by situating these universal security principles within the specific operational realities and contemporary challenges faced by these vital community institutions.

3. Methodology

To move beyond theoretical assumptions and ground this study in the specific reality of Ukrainian public libraries, a primary data collection exercise was undertaken.

3.1 Survey design, distribution and response rate

A structured questionnaire was developed to assess the current state of cybersecurity governance, technical infrastructure and threat awareness in Ukrainian public libraries (see Appendix). The survey was distributed digitally via Google Forms through professional networks, including the Ukrainian Library Association's (ULA) mailing lists and specific regional library consortia groups, targeting library directors, department heads and IT specialists. The data collection period spanned two months in early 2024.

Based on the membership counts of the targeted distribution channels at the time of deployment, the survey link was delivered to a calculable population of 642 active library professionals. A total of 127 valid responses were collected, yielding a precise response rate of 19.8%. In the context of specialized professional surveys, particularly in a region experiencing active conflict and infrastructural disruptions, a response rate nearing 20% is considered highly robust. It provides a robust descriptive and empirical baseline for assessing the sector's cybersecurity maturity while allowing us to confidently evaluate potential trends without significant non-response bias.

3.2 Sample characteristics

To mitigate non-response bias, the distribution strategy deliberately encompassed a diverse cross-section of institutions. While the use of convenience sampling via professional networks introduces a potential for self-selection bias, the sample achieves robust regional representation. The 127 respondents reflect a broad geographic spread across Ukraine: approximately 45% from Central and Northern regions, 35% from Western regions and 20% from the heavily impacted Eastern and Southern regions. Administratively, the sample includes:

- regional universal scientific libraries;
- city public libraries; and
- amalgamated territorial community libraries (rural/small town).

This diverse sample size provides a representative snapshot of the sector, allowing for the reliable extrapolation of broader trends regarding the "security maturity" of the Ukrainian public library system.

4. Empirical findings: the state of security in Ukrainian libraries

The analysis of the survey data reveals a concerning landscape characterized by a lack of formal governance and scarce technical resources. The findings replace previous assumptions with concrete evidence of the vulnerabilities facing these institutions.

4.1 The human resource deficit

One of the most critical components of a robust cybersecurity posture is the presence of qualified personnel. The survey results indicate a severe shortage in this area (Table 1).

As indicated in Table 1, 60% of surveyed libraries operate without any dedicated IT specialist. In these institutions, technical responsibilities often fall to general library staff who may lack the specific expertise required to manage complex security configurations, monitor network traffic or respond effectively to cyber incidents. Only 15% of libraries, primarily larger regional institutions, maintain full-time IT staff. The quantitative breakdown of IT personnel availability across the surveyed institutions is illustrated in Figure 1.

This "human firewall" gap significantly lowers the barrier for potential attackers.

4.2 The governance gap

Beyond human resources, the survey sought to establish the prevalence of formal security governance (Table 2).

The data presented in Table 2 reveals a profound governance gap: 70% of respondents reported that their library does not have a written information security policy. This finding allows us to definitively state that the majority of Ukrainian public libraries lack the

Table 1. IT Staffing in Ukrainian public libraries ($n = 127$)

Category (IT staffing status)	%	No. of libraries (abs.)
Full-time IT specialist	15	19
Part-time / outsourced	25	32
No IT specialist	60	76
Total	*100*	*127*

Source(s): Compiled by the authors based on 2024 survey data

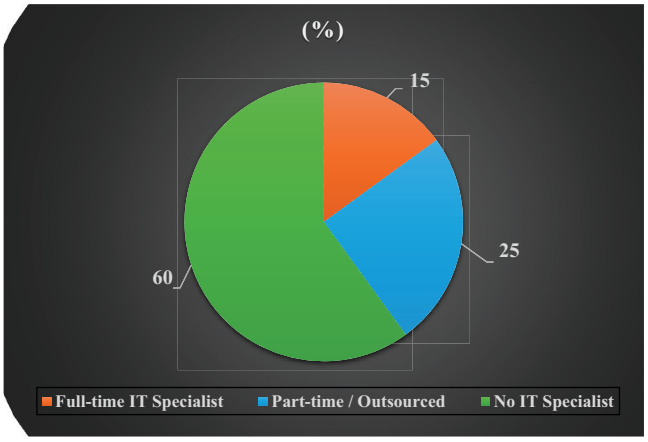

Figure 1. Distribution of IT staffing models in surveyed institutions
Source: Compiled by the authors based on 2024 survey data

Table 2. Existence of information security policies ($n = 127$)

Policy status	%	No. of libraries (abs.)
Written policy exists	30	38
No written policy	70	89
Total	*100*	*127*

Source(s): Compiled by the authors based on 2024 survey data

foundational documentation necessary to guide staff behavior, define data handling procedures and ensure legal compliance. Without a policy, security measures are likely to be ad-hoc, inconsistent and dependent on individual initiative rather than institutional mandate.

4.3 Technical hygiene and threat exposure

The survey also probed the operational realities of software maintenance and the prevalence of social engineering attacks (Figure 2. Part A: software update frequency; Part B: phishing encounters).

Figure 2 highlights a dangerous correlation. While 60% of libraries report encountering phishing attempts, a staggering 57% report that software updates occur rarely or never. This combination creates a high-risk environment: staff are being actively targeted by social engineering attacks (a primary vector for malware delivery) while operating on systems that likely contain unpatched vulnerabilities. The low rate of automated updates (12%) suggests that even when IT staff are present, they may be overwhelmed or lack the tools for centralized patch management.

Further cross-tabulation of the survey data reveals a compounding vulnerability: libraries operating without dedicated IT staff were disproportionately represented among those reporting irregular software updates, demonstrating a direct analytical link between the human resource deficit (Section 4.1) and technical exposure (Section 4.3).

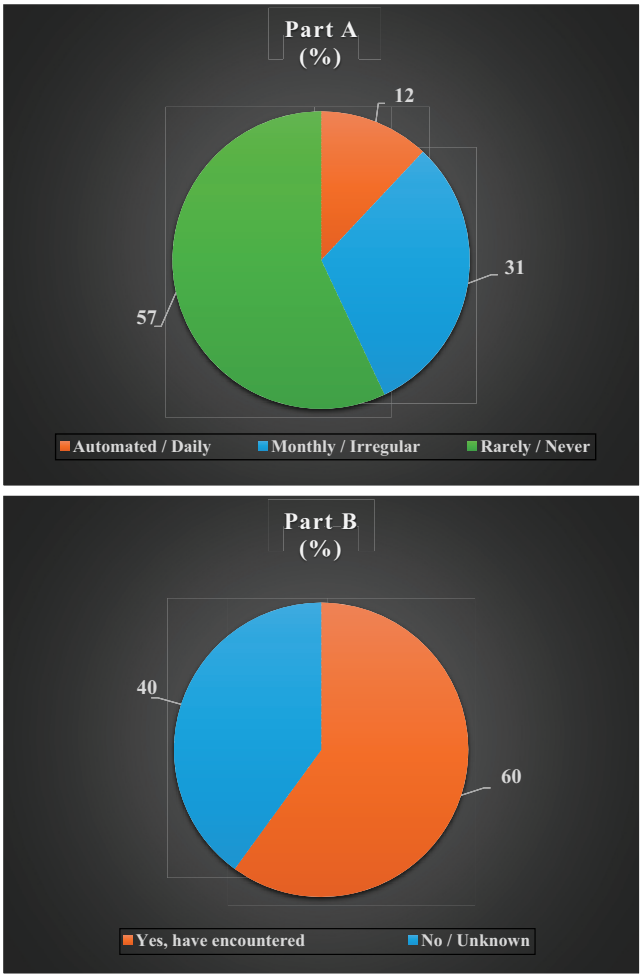

Figure 2. Survey results on technical hygiene and threat exposure ($n = 127$). Part A: software update frequency. Part B: frequency of phishing encounter incidents
Source: Compiled by the authors based on 2024 survey data

5. The main issues in securing digital library services and ensuring data privacy in Ukraine

The survey results provide a quantitative foundation for understanding the systemic challenges. However, these statistics must be contextualized within the specific operational realities of Ukraine. The challenges are not merely technical; they are deeply intertwined with the socio-political context of the country.

5.1 The technological inheritance: navigating with outdated equipment

A primary and deeply entrenched technological challenge is the reliance on an aging and patchwork IT infrastructure. Many institutions operate on a digital foundation built with

hardware from a bygone era. This issue is critically compounded by the persistence of legacy software. Much like a beautifully crafted but antiquated vehicle, these older systems may still function, but they no longer receive vital security patches from their developers, leaving them with known vulnerabilities that act as open invitations for digital intrusion (Otieno *et al.*, 2023).

The prohibitive cost of a comprehensive system-wide overhaul often remains an insurmountable barrier. This is further exacerbated by a limited capacity to deploy modern defensive tools such as next-generation firewalls or intrusion detection systems, which demand significant financial investments. The internal network design within many libraries also presents a risk; "flat" network architectures, where staff and public computers share the same segment, allow malware to spread laterally with ease.

5.2 Context-specific challenges: the "Diia" ecosystem and privacy

To justify the focus on the Ukrainian context, it is essential to analyze the specific role libraries play in the state's digital infrastructure.

5.2.1 Libraries as Diia.Digital education hubs. To comprehend the unique privacy risks in Ukrainian libraries, one must understand the role of "Diia" (Action). Diia is Ukraine's comprehensive national e-governance platform, which centralizes digital passports, biometric data, tax records and over 70 critical state services into a single portal and mobile application (Diia, 2026). Recognizing the digital divide, the Ministry of Digital Transformation designated public libraries as official "Diia.Digital Education" hubs (UNDP, 2023). This initiative mandates libraries to assist citizens – especially the elderly and internally displaced persons – in accessing these highly sensitive government services via public library terminals. While socially vital, this integration fundamentally alters the library's threat profile. Public access computers are transformed into critical national infrastructure access points.

Citizens visit libraries to learn how to use digital services, often logging into the Diia portal – which grants access to sensitive government records, tax data and digital passports – on public library computers (EUMP, 2022). This creates a high-value target for attackers. If a library's public computer is infected with a keylogger or info-stealer malware (a common tool in the arsenal of groups targeting Ukraine), the sensitive personal data of citizens could be compromised. The survey finding that 57% of libraries rarely update software suggests that many of these "hubs" may be operating with significant vulnerabilities, putting user data at risk of interception.

5.2.2 Privacy risks on public terminals. The integration of Diia necessitates a higher standard of privacy protection than traditional library services. Users may be entering passport numbers, tax IDs and biometric data. The risk of "session persistence" – where a user forgets to log out and the next user accesses their account – is acute. Without automated "deep freeze" software that resets the computer state after every session, libraries cannot guarantee the privacy of the next patron (EUMP, 2022).

5.3 The impact of kinetic warfare: blackouts and infrastructure degradation

The ongoing full-scale invasion has introduced physical threats that have direct digital consequences. Since October 2022, systematic attacks on Ukraine's energy infrastructure have led to widespread, rolling blackouts (Congressional Research Service, 2023).

Disruption of IT integrity: Sudden power cuts cause improper shutdowns of servers and workstations. For databases used in library management systems (LMS) (typically SQL-based), an ungraceful shutdown can corrupt the file system or transaction logs, leading to irreversible data loss (Center for Infrastructure Protection, 2016). Furthermore, the

irregularity of power supply makes the scheduling of automated updates (typically set for night-time) impossible, directly contributing to the 57% "irregular update" statistic found in our survey.

Equipment damage: Voltage spikes upon power restoration frequently damage sensitive IT equipment. For libraries with limited budgets, the loss of a server or network switch due to a power surge can result in weeks or months of service unavailability.

5.4 Real cyberattacks on cultural institutions

The threat of targeted cyberattacks is not theoretical. Reports from CERT-UA indicate a sustained campaign against Ukrainian institutions. In January 2023, CERT-UA reported a cyberattack on the national news agency Ukrinform using "CaddyWiper" malware (CERT-UA, 2024). This type of malware is designed to destroy data irrecoverably. Libraries, as repositories of digital heritage, are logical targets for such "cultural cleansing" operations.

Groups like UAC-0050 and APT28 (Fancy Bear) have been observed using mass phishing emails disguised as official correspondence from government bodies to infiltrate networks (RNBO, 2024). The survey finding that 60% of library staff have encountered phishing aligns with these national-level threat intelligence reports.

Attacks often target the software supply chain. For example, the compromise of the "M.E.Doc" accounting software served as patient zero for the devastating NotPetya attack in 2017, underscoring the cascading risks of third-party software in Ukrainian networks (Greenberg, 2019).

6. Strategies for enhancing digital library security and data privacy in Ukraine

To directly address the vulnerabilities identified in the previous sections – namely, legacy infrastructure (Section 5.1), Diia privacy risks (Section 5.2) and physical blackout impacts (Section 5.3) – the following framework maps specific mitigation strategies to each challenge. Given the severe budget and staffing constraints highlighted in our empirical findings, these recommendations deliberately move beyond theoretical ideals. They prioritize feasible, open-source and policy-driven solutions that can be implemented by under-resourced institutions.

6.1 Technological strategies

Technological measures serve as the primary defense and given the resource constraints identified in the survey, these strategies must prioritize cost-effectiveness and automation (Table 3).

A critical first step is the hardening of infrastructure through the automation of patch management for both operating systems and LMS. This approach directly mitigates vulnerabilities arising from irregular manual updates, a significant risk factor identified in our findings. In addition, the implementation of "Deep Freeze" or similar software on public terminals is essential; this ensures that computers are reset to a clean state after every session, thereby effectively protecting user data, particularly for citizens accessing *Diia* services.

Network security can be significantly enhanced through segmentation and filtering. Implementing network segmentation virtual local area network (VLANs) allows libraries to isolate public Wi-Fi and terminals from staff administrative networks, preventing the lateral spread of threats. To further secure the perimeter, libraries should deploy domain name system (DNS) filtering services, such as Quad9 or Cisco Umbrella. This relatively low-cost measure can block access to malicious domains and known phishing sites, adding a layer of defense that does not require expensive hardware firewalls.

Table 3. Technological strategies for enhancing security and data privacy

Strategy area	Specific strategy/action	Objective/benefit	Considerations for Ukrainian libraries
Infrastructure and systems hardening	(1) Automate patch management for OS and Library Management Systems (LMS)	(1) Mitigate vulnerabilities from irregular manual updates	(1) Schedule updates during likely "power-on" windows or use battery-backed management servers
	(2) Implement "Deep Freeze" software on public terminals	(2) Ensure public computers reset to a clean state after every session, protecting Diia user data	(2) Essential for Diia hubs to prevent session hijacking
Network security	(1) Implement network segmentation (VLANs)	(1) Isolate public Wi-Fi/terminals from staff administrative networks	(1) Collaborate with ISPs to implement basic filtering at the router level
	(2) Deploy DNS filtering (e.g. Quad9, Cisco Umbrella) to block malicious domains	(2) Prevent users from accessing known phishing sites	(2) Low-cost, high-impact measure for libraries with no firewall budget
Data protection and resilience	(1) Establish off-site, immutable backups (3-2-1 rule)	(1) Protect against ransomware and physical destruction (missiles)	(1) Use cloud backup solutions (now permitted under martial law) to ensure data survives physical damage to the library
	(2) Use Uninterruptible Power Supplies (UPS) for critical servers	(2) Prevent database corruption during blackouts	(2) Prioritize UPS for the LMS database server
Threat intelligence	(1) Subscribe to CERT-UA alerts and indicators of compromise (IoCs)	(1) Proactive blocking of known threats targeting Ukraine	(1) Collaborate with CERT-UA regarding threat intelligence and reporting procedures

Source(s): Compiled by the authors

Ensuring data protection and resilience is vital in the context of physical threats. Libraries should establish off-site, immutable backups following the 3–2–21 rule, using cloud solutions to protect against ransomware and the physical destruction of servers. To safeguard against data corruption during frequent blackouts, critical servers must be supported by uninterruptible power supplies (UPS). Besides, subscribing to CERT-UA alerts and indicators of compromise (IoCs) enables libraries to move from a passive stance to proactive blocking of known threats targeting Ukraine.

6.2 Organizational and policy strategies

Technology alone is insufficient without a robust organizational structure to guide its implementation. To bridge the governance gap identified in the survey, libraries must develop and approve a standardized information security policy (Table 4).

This framework should clearly define roles, establish acceptable use guidelines and enforce rigorous password standards. In compliance with data laws and GDPR principles, the appointment of a data protection officer (DPO) is crucial to oversee data handling practices, ensuring that privacy is not compromised in the pursuit of digital service delivery.

Sustainable security requires dedicated resources. Therefore, library administration must actively advocate for specific cybersecurity funding within their budgets to cover essential licenses and hardware upgrades. Beyond local funding, libraries should seek international grants for IT modernization, ensuring that cybersecurity requirements are integral components of any digital transformation project.

Preparedness for potential breaches is as important as prevention. Libraries need to develop a “Break-Glass” incident response plan (IRP) that outlines clear steps for staff to take during an attack. This includes knowing whom to contact – such as CERT-UA – and establishing clear reporting lines to national bodies. Such planning ensures that when incidents occur, the response is swift and coordinated, minimizing downtime and data loss.

Besides, to tailor the framework to the Ukrainian operational context, the ISP must elevate immutable off-site backups from a mere best practice to a mandatory governance requirement, given the high risk of kinetic destruction. For public terminals, the ISP must mandate strict, post-session data-wiping protocols to mitigate the identified Diia privacy risks. Finally, the IRP must specifically outline non-digital communication channels (e.g. landlines or satellite messengers) and procedures for reporting incidents to CERT-UA during scenarios involving total blackouts or telecommunication failures.

6.3 Human-centric and context-specific strategies

The human element remains the most critical variable in the security equation. With a high percentage of staff reporting phishing encounters (60%), education is paramount (Table 5).

Libraries should implement mandatory anti-phishing workshops for all staff to reduce the likelihood of successful social engineering attacks. These should be complemented by regular “Cyber Hygiene” drills to cultivate a culture of skepticism and vigilance, transforming staff from potential targets into active defenders. Specific attention must be paid to user education regarding the *Diia* ecosystem. Libraries should create and display visual guides for safe *Diia* usage on public computers, educating patrons on how to protect their digital identities. Enforcing strict log-out procedures is also critical to prevent credential theft on shared devices, ensuring that one user’s session does not become the next user’s vulnerability.

The unique geopolitical context necessitates strategies for resilience against kinetic and cognitive threats. The concept of “Digital Shelters” must be operationalized: libraries should be equipped not only with physical safeguards (generators, Starlink terminals) but with

Table 4. Organizational and policy strategies

Strategy area	Specific strategy/action	Objective/benefit	Considerations for Ukrainian libraries
Governance framework	(1) Develop and approve a standardized Information Security Policy (2) Appoint a Data Protection Officer (DPO)	(1) Define clear roles, acceptable use and password standards (2) Ensure compliance with data laws and GDPR principles	(1) Adapt templates provided by the Ukrainian Library Association (ULA) to reduce administrative burden (2) In small libraries, this role can be shared regionally
Funding and resource allocation	(1) Advocate for dedicated cybersecurity funding in library budgets (2) Seek international grants for IT modernization	(1) Ensure resources for licenses (antivirus, backup) and hardware	(1) Include security requirements in all grant applications for digital transformation
Incident response	(1) Develop a “Break-Glass” Incident Response Plan (IRP) (2) Establish clear reporting lines to national bodies	(1) Ensure staff know who to call during an attack (e.g. CERT-UA) (2) Minimize downtime and data loss	(1) Include non-digital communication channels (e.g. landlines) in the IRP for total blackout scenarios

Source(s): Compiled by the authors

Table 5. Human-centric and context-specific strategies

Strategy area	Specific strategy/action	Objective/benefit	Considerations for Ukrainian libraries
Staff awareness	(1) Mandatory anti-phishing workshops for all staff (2) Regular "cyber hygiene" drills	(1) Reduce the click rate on malicious emails (2) Build a culture of skepticism toward unsolicited requests	(1) Use the Diia.Digital Education platform's own cybersecurity modules for staff training
User education (Diia)	(1) Create visual guides for safe Diia usage on public computers (2) Enforce strict log-out procedures	(1) Empower patrons to protect their own digital identity (2) Prevent credential theft on shared devices	(1) Place physical posters near terminals reminding users: "Did you log out of Diia?"
Geopolitical resilience	(1) Digitization of rare collections with cloud redundancy (2) "Digital Shelters" concept (3) Integrate with distributed preservation networks (e.g. LOCKSS, CLOCKSS, SUCHO)	(1) Preserve cultural heritage against physical destruction (2) Ensure libraries remain information hubs during crises	(1) Partner with international projects like Saving Ukrainian Cultural Heritage Online (SUCHO) (2) Equip libraries with Starlink terminals and generators

Source(s): Compiled by the authors

robust data continuity protocols. To prevent the "cultural cleansing" described in cognitive warfare literature, institutions must integrate with distributed, decentralized preservation networks such as Lots of Copies Keep Stuff Safe (LOCKSS) and controlled lots of copies keep stuff safe (CLOCKSS) to ensure access continuity even if local servers are obliterated. The Saving Ukrainian Cultural Heritage Online (SUCHO) initiative exemplifies this crucial strategy, demonstrating how international crowdsourced archiving can successfully back up vulnerable local library databases to secure servers abroad, ensuring the survival of digital cultural property under conflict conditions.

7. Discussion

The preceding analysis has charted a complex terrain of interconnected obstacles that Ukrainian public libraries must navigate. The findings from the survey provide a sobering quantitative validation of the theoretical risks. This disparity creates a "security debt" that malicious actors are actively exploiting. The technological deficits, such as the inheritance of aging infrastructure and legacy software, represent a common struggle for public institutions globally. However, within Ukraine's current environment, marked by significant economic constraints and a heightened geopolitical threat level, this challenge is cast in a much starker light. It transforms from a problem of managed obsolescence into one of critical vulnerability.

The specific context of the *Diia.Digital Education* project introduces a complex variable. While the initiative successfully positions libraries as vital centers for digital inclusion, it simultaneously aggregates high-value targets (citizens' digital identities) in low-security environments. The risk is not theoretical; a compromise of a library computer could theoretically serve as a collection point for credentials used to access state services, bridging the gap between a local library breach and national security.

Overlaying these technological realities are the organizational gaps. A library might possess a firewall, but if it lacks a clear policy and dedicated personnel, the technology is merely a fortress with unguarded gates. The strategies proposed in this paper, advocating for dedicated funding and collaborative models of expertise (such as regional IT support teams), aim to address these systemic shortfalls.

Perhaps the most pervasive vulnerability lies in the human-centric dimension. An expensive technological defense can be bypassed by a single, well-crafted phishing email clicked by well-intentioned but inadequately trained staff. The survey's 60% phishing encounter rate underscores this reality. This elevates the proposed strategies for continuous, engaging training and user education from a "nice-to-have" to a mission-critical imperative.

8. Conclusion

The journey to fortify Ukraine's public libraries against the complexities of the digital age is not a simple task of installing new software, but a profound and ongoing voyage of strategic adaptation. This paper has navigated the intricate challenges these vital institutions face, charting a course through a landscape marked by technological vulnerabilities, organizational inertia, the ever-present human element and the unique pressures of Ukraine's socio-political context.

The central thesis of this work is a call to move beyond a reactive, "patch-and-pray" posture toward cybersecurity and privacy. Such an ad-hoc approach is no longer sustainable in a world of ever-more-sophisticated threats. Instead, what is required is the cultivation of a proactive culture where security and privacy are woven into the very fabric of library services, by design and by default.

The survey data presented here serves as a wake-up call: with a vast majority of libraries lacking basic security policies, the sector is currently exposed. However, the resilience of Ukrainian librarians, who continue to serve their communities amidst war and blackouts, suggests that this challenge can be met. By adopting the proposed framework – integrating automated technical controls, standardized governance and rigorous human education – Ukrainian public libraries can not only navigate the diverse threat landscape but also proudly uphold their deep-rooted ethical commitment to user privacy. In doing so, they reinforce their standing as trusted pillars of the community, preserving not just books, but the digital sovereignty of the citizens they serve.

References

Alcala, R. (2022), "Cultural evolution: protecting "digital cultural property" in armed conflict", *International Review of the Red Cross*, Vol. 104 No. 919, pp. 1083-1119, doi: 10.1017/S181638312200008X.

Alhidaifi, S.M., Asghar, M.R. and Ansari, I.S. (2024), "A survey on cyber resilience: key strategies, research challenges, and future directions", *ACM Computing Surveys*, Vol. 56 No. 8, pp. 1-48, doi: 10.1145/3649218.

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E. (2023), "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions", *Electronics*, Vol. 12 No. 6, p. 1333, doi: 10.3390/electronics12061333.

Bellini, E. (2024), "Cyber humanities for heritage security", *Communications of the ACM*, Vol. 68 No. 12, pp. 112-117.

Bellini, E. and Degl'Innocenti, E. (2025), "Building the foundations of cyber humanities: cultural Cyber-Critical ecosystem conceptualization", *2025 IEEE International Conference on Cyber Humanities*.

Broeders, D., Cristiano, F. and Kaminska, M. (2023), "In search of digital sovereignty and strategic autonomy: normative power Europe to the test of its geopolitical ambitions", *JCMS: Journal of Common Market Studies*, Vol. 61 No. 5, pp. 1261-1280, doi: 10.1111/jcms.13462.

Center for Infrastructure Protection and Homeland Security (2016), "Lessons learned from the power outage in Ukraine and how the electric grid of the future will reduce cybersecurity risk". [Online], available at: https://cip.gmu.edu/2016/05/24/lessons-learned-power-outage-ukraine-electric-grid-future-will-reduce-cybersecurity-risk/ (accessed 10 November 2025).

CERT-UA (2024), "On the situation in the cyber sector as at february 23–24, 2024". [Online], available at: https://cert.gov.ua/article/6277840 (accessed 4 October 2025).

Congressional Research Service (2023), "Attacks on Ukraine's electric grid: insights for U.S. Infrastructure security and resilience". [Online], available at: www.congress.gov/crs-product/R48067 (accessed 2 December 2025).

Deppe, C. and Gary, S. (2024), "Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept", *Frontiers in Big Data*, Vol. 7, doi: 10.3389/fdata.2024.1452129.

Diia (2026), "Digital state". [Online], available at: https://expo.diia.gov.ua/ (accessed 15 November 2025).

Dudyk, I., Rezvorovych, K., Melnyk, V., Gayevaya, O. and Tumalavičius, V. (2024), "Strategies for Ukraine's legal integration into the EU: learning from the experience of Central and Eastern Europe", *Evropský Politický A Právní Diskurz*, Vol. 6, pp. 13-21, doi: 10.46340/eppd.2024.11.6.2.

EL Yamani, Y., Baddi, Y. and Kamoun, N. (2024), "A survey on the contribution of ML and DL to the detection and prevention of botnet attacks", *Journal of Reliable Intelligent Environments*, Vol. 10 No. 4, pp. 431-448, doi: 10.1007/s40860-024-00226-y.

EUMP (2022), "What's wrong with Diia?". [Online], available at: https://eump.org/media/2022/whats_wrong_with_diia.pdf (accessed 26 November 2025).

George, A.S., Baskar, T. and Srikaanth, P.B. (2024), *Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors*, Vol. 2, pp. 51-75, doi: 10.5281/zenodo.10639463.

Greenberg, A. (2019), *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Vintage Books, New York, NY.

International Federation of Library Associations and Institutions (IFLA) (2022), "Guidelines on privacy in the library environment".

Khan, A., Ibrahim, M. and Hussain, A. (2021), "An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries", *International Journal of Information Management Data Insights*, Vol. 1 No. 2, p. 100015, doi: 10.1016/j.jjimei.2021.100015.

King, D.L. (2020), "Transforming the library", In Rubin, R.E. and Rubin, R.G. (Eds), *Foundations of Library and Information Science*, 5th ed., ALA Neal-Schuman, Chicago, IL, p. 197.

Kniazieva, T.V., Kazanska, O.O., Orochovska, L.A., Tsymbalenko, Y.Y. and Dergach, A.V. (2023), "Analysis of the impact of digitalization on the quality and availability of public services in Ukraine – a comparative approach with insights from Estonia", *Statistics, Politics and Policy*, Vol. 14 No. 3, pp. 375-398, doi: 10.1515/spp-2023-0012.

Kotoroi, G. (2023), "Constraints facing African academic libraries in applying electronic security systems to protect library materials", *International Journal of Librarianship*, Vol. 8 No. 1, pp. 31-48, doi: 10.23974/ijol.2023.vol8.1.272.

Lukianova, L. and Ovcharuk, O. (2023), "Information literacy and digital inclusion: challenges of the modern information educational environment in Ukraine", In Tomczyk, Ł., Guillén-Gámez, F.D., Ruiz-Palmero, J. and Habibi, A. (Eds), *From Digital Divide to Digital Inclusion*, Springer, Singapore, pp. 541-565, doi: 10.1007/978-981-99-7645-4_25.

Mojjada, M.H. (2025), *ICT in Libraries: A Theoretical Approach*, Chyren Publication.

Nehra, S.S. and Bansode, S.Y. (2024), "Exploring the prospects and perils of integrating artificial intelligence and ChatGPT in academic and research libraries (ARL): challenges and opportunity", *Journal of Web Librarianship*, Vol. 18 No. 3, pp. 111-132.

Nguyen, C.D. (2024), "Digital cultural heritage in the crossfire of conflict: cyber threats and cybersecurity perspectives", *Insights: The UKSG Journal*, Vol. 37 No. 1, p. 7.

Otieno, M., Odera, D. and Ounza, J.E. (2023), "Theory and practice in secure software development lifecycle: a comprehensive survey", *World Journal of Advanced Research and Reviews*, Vol. 18 No. 3, pp. 053-078.

RNBO (2024), "Review of cybersecurity news in Ukraine, tendencies, and world events related to the first world cyber war". [Online], available at: www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest%2002_2024/Feb_2024_fin.pdf (accessed 3 December 2025).

Schütz, P. (2022), "Data protection authorities under the EU general data protection regulation-a new global benchmark", *Handbook of Regulatory Authorities*, Edward Elgar Publishing, Cheltenham, pp. 128-145, doi: 10.4337/9781839108990.00018.

Sedrati, Y. and Sidi Athmane, M.W. (2024), "The cookies' quest: towards digital totalitarian landscape", *Journal of Studies in Language, Culture and Society (JSLCS)*, Vol. 7 No. 2, pp. 182-199.

Ulven, J.B. and Wangen, G. (2021), "A systematic review of cybersecurity risks in higher education", *Future Internet*, Vol. 13 No. 2, p. 39.

UNDP (2023), "Digital education hubs: over 3000 libraries now teaching Ukrainians digital literacy". [Online], available at: www.undp.org/ukraine/press-releases/digital-education-hubs-over-3000-libraries-now-teaching-ukrainians-digital-literacy (accessed 13 November 2025).

Velmurugan, V.S. (2024), "The changing role of libraries in the digital age of intellectual freedom", *International Journal of Information Library and Society*, Vol. 13 No. 2.

Williamson, S.M. and Prybutok, V. (2024), "Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare", *Applied Sciences*, Vol. 14 No. 2, p. 675.

Witt, S. (2017), "The evolution of privacy within the American library association, 1906–2002", *Library Trends*, Vol. 65 No. 4, pp. 639-657.

Further reading

American Library Association (ALA) (2020), "Privacy: an interpretation of the library bill of rights". [Online], available at: www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

CERT-FR (2024), "Cyber threat overview 2023". [Online], available at: www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-002.pdf (accessed 12 October 2025).

CERT-UA (2023), "CERT-UA processed 2,543 cyber incidents in 2023. State service of special communications and information protection of Ukraine". [Online], available at: https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti (accessed 28 September 2025).

Freedom House (2023), "Ukraine: freedom on the net 2023 country report". [Online], available at: https://freedomhouse.org/country/ukraine/freedom-net/2023 (accessed 4 October 2025).

ISO/IEC (2022), "ISO/IEC 27001:2022 information security, cybersecurity and privacy protection – information security management systems – requirements".

Mueller, G.B., Jensen, B., Valeriano, B., Maness, R.C. and Macias, J.M. (2023), *Cyber operations during the Russo-Ukrainian War: from strange patterns to alternative futures*, Center for Strategic and International Studies (CSIS), Washington, DC.

Nair, S.S. (2024), "Securing against advanced cyber threats: a comprehensive guide to phishing, XSS, and SQL injection defense", *Journal of Computer Science and Technology Studies*, Vol. 6 No. 1, pp. 76-93.

Scientific Library of Ivan Franko National University of Lviv (2026), "Informational technology department". [Online], available at: www.lnulibrary.lviv.ua/en/lb-it-en/ (accessed 19 October 2025).

Appendix. Survey on information security in Ukrainian public libraries

Survey methodology: This survey was conducted in Q1 2024 via a Google Form distributed to professional library networks in Ukraine.

Total respondents: 127

Key questions and aggregated results:

IT staffing:

- *Question:* "Does your library have a full-time, staff IT specialist?"
- *Results:* Yes (15%), No (85%).

Security policy:

- *Question:* "Does your library have a written, approved information security or data privacy policy?"
- *Results:* Yes (30%), No (70%).

Phishing awareness:

- *Question:* "Have you or your colleagues encountered phishing attempts (suspicious emails asking for passwords or containing strange links) at your workplace?"
- *Results:* Yes (60%), No/I don't know (40%).

Software updates:

- *Question:* "How often is the software (OS, Library System, Antivirus) on your library computers updated?"
- *Results:* Automatically/daily (12%), monthly (31%), irregularly/never (57%).

Corresponding author
Viktoriia Pylypiv can be contacted at: viktoriia.pylypiv@proton.me