Modern approaches to cybersecurity requirements management for software implementation

Sergiy Gnatyuk[1,*,†], Viktoriya Sydorenko[1,†], Artem Polozhentsev[1,†], Anatolii Skurativskyi[1,†], Kamila Kluczewska-Chmielarz[2,†] and Gabit Shuitenov[3,†]

[1] *State University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine*
[2] *University of the National Education Commission, Podchorazych Str., 2, Krakow, 30-084, Poland*
[3] *Esil University, Astana, A. Zhubanov Str., 7, 010000, Kazakhstan*

Abstract

This paper examines modern approaches to managing cybersecurity requirements during software implementation. It analyzes the regulatory and legal framework, as well as the scientific sources that govern the protection of information systems. Particular attention is given to classifying cybersecurity requirements as functional or non-functional, formulating them, documenting them, and integrating them into the software development process. The article concludes that cybersecurity requirements management encompasses technical, organizational, and legal aspects, necessitating a systematic approach. The article also considers the role of policies, procedures, technical solutions, and regulations in forming a secure digital environment. The importance of continuous monitoring and updating requirements in consideration of the dynamics of cyber threats is emphasized. Furthermore, it presents best practices for managing cybersecurity requirements, along with recommendations for improving the security level of information systems. These results can be used to improve cybersecurity risk management practices, implement security standards, and develop secure software in the public and private sectors.

Keywords

cybersecurity, cybersecurity requirements, requirements management, information systems, data protection, cyber threats, functional requirements, non-functional requirements, ISO/IEC 27001, NIST, security policy, governance policy, requirements documentation

1. Introduction

In today's digital world, cybersecurity is a critical aspect of any organization's operations. A systematic approach to cybersecurity requirements management is necessary to ensure cybersecurity. This approach includes identifying, analyzing, documenting, and implementing necessary security measures. This study presents the core processes of cybersecurity requirements management, defines key stages and methods, and discusses best practices in this field.

2. Analysis of research and problem statement

The rapid development of digital technologies, the growing number of cyber threats, and the tightening regulatory requirements present new challenges to ensuring reliable cybersecurity in information systems. One key element of an effective protection system is managing cybersecurity requirements, which encompasses identifying, formalizing, documenting, implementing, and enforcing requirements.

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

s.gnatyuk@kai.edu.ua (S. Gnatyuk); v.sydorenko@ukr.net (V. Sydorenko); artem.polozhentsev@gmail.com (A. Polozhentsev); a.skurativskyi@gmail.com (A. Skurativskyi); kamila.kluczewska-chmielarz@uken.krakow.pl (K. Kluczewska-Chmielarz); shuitenov.g@esil.edu.kzl (G. Shuitenov)

0000-0003-4992-0564 (S. Gnatyuk); 0000-0002-5910-0837 (V. Sydorenko); 0000-0003-0139-0752 (A. Polozhentsev); 0000-0000-0566-2394 (A. Skurativskyi); 0000-0003-4301-7438 (K. Kluczewska-Chmielarz); 0000-0002-9905-7247 (G. Shuitenov)

In today's world, where information security is a critical component of an organization's strategic resilience, high-quality requirements management is essential for minimizing risk and ensuring regulatory compliance.

Organizations frequently face difficulties in managing cybersecurity requirements in practice, such as a lack of clear criteria for identifying requirements, inconsistencies in regulatory sources, difficulties integrating requirements into software development processes, and inadequate support during monitoring and maintenance. Additionally, international and national practices demonstrate significant variability in their approaches, ranging from formalized methodologies, such as NIST RMF and ISO/IEC 27001, to flexible, adaptive models applied in specific industries. The lack of systematic generalization of scientific contributions in this field complicates the selection of optimal solutions for various types of organizations.

Therefore, a comprehensive analysis of modern approaches to cybersecurity requirements management is necessary to identify the most effective practices and recommendations. This analysis is particularly relevant in the context of software implementation, where cybersecurity requirements must be technically justified and integrated into all phases of the system life cycle.

This article aims to analyze modern approaches to cybersecurity requirements management in the context of software implementation.

To achieve this aim, the following objectives must be achieved:

1. Identify existing cybersecurity requirements, their main sources, and methods of identification.
2. Analyze methods, tools, key steps, and recommendations for documenting cybersecurity requirements.
3. Explore the stages of implementation, monitoring, and maintenance, as well as recommendations for implementing cybersecurity requirements.
4. Identify best practices in cybersecurity requirements management.
5. Examine the current state of scientific approaches to cybersecurity requirements management.

3. Definition of cybersecurity requirements

Cybersecurity requirements are defined as the conditions and constraints that must be met to protect information systems from unauthorized access, modification, disclosure, or destruction. The first and most important stage in ensuring an organization's security is defining cybersecurity requirements. Mathematical methods and algorithms, as presented in works [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11], can be used to formally represent these requirements.

3.1. Key Sources of cybersecurity requirements

Cybersecurity requirements may originate from various sources, including:

1. **Legislative and regulatory acts of Ukraine:**
   - Law of Ukraine *"On the Basic Principles of Ensuring Cybersecurity of Ukraine"*: This law establishes the core principles, objectives, and directions of the state policy in the field of cybersecurity.
   - Law of Ukraine *"On Information Protection in Information and Telecommunication Systems"*: a law that defines the principles of information protection in information and telecommunication systems.
   - DSTU ISO/IEC 27001: The national Ukrainian standard aligned with the international ISO/IEC 27001 standard that establishes requirements for an Information Security Management System (ISMS).
2. **Standards and best practices:**

- **ISO/IEC 27001**: An international standard that defines the requirements for an Information Security Management System (ISMS). It includes provisions for establishing, implementing, maintaining, and continuously improving the ISMS [12].
- **GDPR** (General Data Protection Regulation): the General Data Protection Regulation of the European Union sets requirements for the protection of personal data and privacy for all organizations processing the data of EU residents [13].
- **NIST** (National Institute of Standards and Technology) Cybersecurity Framework: a cybersecurity framework developed by NIST that provides guidance on managing cybersecurity risks. It is widely used in the U.S. and internationally [14].
- **CISA** (Cybersecurity Information Sharing Act): a U.S. law encouraging the sharing of cybersecurity threat information between the government and the private sector to enhance cybersecurity [15].
- **HIPAA** (Health Insurance Portability and Accountability Act): a U.S. law that defines requirements for protecting the privacy and security of electronic health information [16].
- **FISMA** (Federal Information Security Management Act): A U.S. law that establishes requirements for protecting information systems in federal agencies [17].
- **NIS Directive**: an EU directive that establishes measures to achieve a high level of security for networks and information systems across the Union [18].
- **ePrivacy Directive**: a directive that regulates the processing of personal data and the protection of privacy in the electronic communications sector [19].

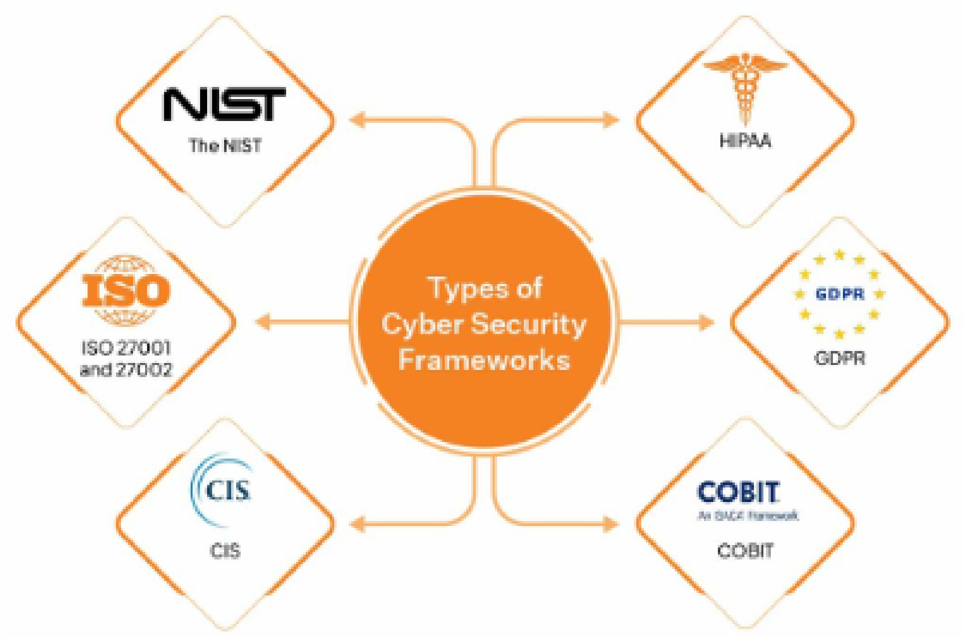

Figure 1: Types of cybersecurity frameworks.

3. **Organizational policies and procedures:**
   Organizational policies and procedures are essential for defining and ensuring cybersecurity requirements. These policies and procedures create a framework for managing cyber risks, ensuring compliance with regulatory requirements, and implementing effective security measures (see Figure 1).
   The following are the main policies and procedures that can be implemented in an organization to ensure cybersecurity:
   a) **Information Security Policy**

This policy outlines the fundamental principles and strategies for protecting the organization's information assets. It addresses aspects such as the confidentiality, integrity, and availability of information [12]. Key elements:

- Defining responsibility for ensuring information security
- Classification of information assets and definition of access levels
- Ensuring network and system security
- Protection against malicious software

b) **Risk Management Policy**
This policy aims to identify, assess, and manage cybersecurity risks [14]. Key elements:

- Risk assessment procedures
- Identification and implementation of risk mitigation measures
- Regular review and updating of risk assessments

c) **Access Control Policy**
This policy regulates access to the organization's information systems and data, ensuring that only authorized users can access them. Key elements:

- Requirements for authentication and authorization
- Management of roles and permissions
- Access monitoring and audit procedures

d) **Incident Response Policy**
This policy outlines the procedures for responding to information security incidents, including cyberattacks, data breaches, and other security violations. Key elements:

- Defining incident types and classification criteria
- Incident reporting procedures
- Response actions and recovery procedures

e) **Change Management Policy**
This policy ensures control over changes to information systems, guaranteeing their security and stability [20, 22]. Key elements:

- Change request and approval procedures
- Security impact assessment of changes
- Testing and documentation of changes

f) **Training and Awareness Policy**
This policy aims to increase employee awareness of cybersecurity and prepare them to comply with security policies and procedures. Key elements:

- Regular cybersecurity training sessions
- Awareness campaigns on emerging threats
- Evaluation of training program effectiveness

g) **Data Retention and Disposal Policy**
This policy defines the requirements for retaining and disposing of data, ensuring the protection of confidential information throughout its life cycle [13, 21]. Key elements:

- Defining data retention periods
- Secure data disposal procedures
- Backup storage requirements

The following table (Table 1) presents the results of the study on organizational policies and procedures for ensuring cybersecurity requirements, based on the following criteria:

- Risk Management (RISK) — if the policy aims to identify, assess, and mitigate cyber risks.
- Access Control (ACCN) — if the policy defines rules for authentication, authorization, and user roles.

- Incident Response (RESP) — if the policy covers the detection, response, and recovery of cyber incidents.
- Data Handling (DATA) — if the policy includes provisions for data retention, backup, and disposal.
- Awareness & Training (TRNG) — if the policy includes educational programs, training sessions, and staff knowledge assessments.
- Change Management (CHNG) — if the policy establishes rules for making secure changes to systems and processes.

The analysis shows that the Information Security Policy is the most comprehensive because it addresses most of the criteria, at least partially. The Risk Management and Incident Response Policies provide targeted support in specific areas, but none of them take into account important components such as staff training or access control. These findings underscore the necessity of a holistic approach to developing cybersecurity policies that consider interrelated requirements.

Table 1
Cybersecurity Policy Comparison

Policy	RISK	ACCN	RESP	DATA	TRNG	CHNG
Information Security Policy	+/-	+	+/-	+/-	−	−
Risk Management Policy	+	−	+/-	−	−	−
Access Control Policy	−	+	+/-	−	−	−
Incident Response Policy	+/-	−	+	+/-	−	−
Change Management Policy	+/-	+/-	−	−	−	+
Training and Awareness Policy	−	−	−	−	+	−

3.2. Technical specifications and architectural solutions

Technical specifications and architectural solutions play a critical role in ensuring cybersecurity by defining and implementing the technical mechanisms required to protect systems, data, and communications. This section outlines key specifications and architectures that support cybersecurity requirements implementation in organizations.

1. Technical Specifications

a. Data Encryption
Encryption safeguards data confidentiality both in transit and at rest.

- **AES (Advanced Encryption Standard):** A symmetric encryption algorithm widely adopted for securing sensitive information due to its strength and speed.
- **TLS (Transport Layer Security):** A cryptographic protocol that ensures secure communication over networks, particularly the Internet.

b. Authentication and Authorization
These mechanisms control access to systems and data, ensuring that only authorized individuals can perform actions.

- **MFA (Multi-Factor Authentication):** Combines two or more independent credentials (e.g., password, phone verification, biometric) for user identity verification.
- **OAuth:** A widely used open standard for access delegation, enabling secure authorization without exposing user credentials.

c. Vulnerability Management
Timely identification and mitigation of vulnerabilities is vital for reducing the risk of exploitation.

- **CVSS (Common Vulnerability Scoring System):** A standardized method for evaluating the severity of software vulnerabilities.
- **Nessus:** A robust vulnerability scanner used to identify weaknesses across systems and applications.

2. Architectural Solutions

a. Network Security
Protecting the integrity and confidentiality of network communications is fundamental.

- **DMZ (Demilitarized Zone):** A network segment that isolates internal systems from untrusted external networks, adding an extra layer of protection.
- **VPN (Virtual Private Network):** Encrypts data transmission across public or untrusted networks, maintaining confidentiality and integrity.

b. Endpoint Protection
Endpoints such as laptops, servers, and mobile devices must be secured against malware and unauthorized access.

- **EDR (Endpoint Detection and Response):** Provides continuous monitoring and response capabilities to detect and counteract endpoint threats.
- **Antivirus Software:** Prevents, detects, and removes malicious software from endpoint devices.

c. Application Security
Secure development practices and application-level controls are essential to prevent exploits.

- **OWASP (Open Web Application Security Project):** Provides a framework and tools for developing secure web applications.
- **SAST (Static Application Security Testing):** Analyzes source code or binaries to identify security vulnerabilities without executing the code.

d. Monitoring and Logging
Effective monitoring and centralized logging are essential for detecting and investigating security events.

- **SIEM (Security Information and Event Management):** Aggregates and correlates security data to identify anomalies and generate alerts.
- **Syslog:** A standard protocol used for forwarding log messages, enabling centralized logging and analysis.

e. Cloud Cybersecurity Solutions
Securing cloud-based infrastructure, applications, and data requires specialized solutions.

- **CASB (Cloud Access Security Broker):** Enforces security policies between users and cloud applications to monitor usage and enforce controls.
- **MSS (Managed Security Services):** Outsourced security services that monitor and protect cloud environments through continuous threat management.

3.3. Requirements identification

After identifying the requirements, they must be thoroughly analyzed to detect potential conflicts, duplications, or gaps. The analysis includes evaluating the requirements' practicability, clarity, verifiability, and priority.

4. Analysis and documentation of requirements

Once the requirements have been identified, they should be thoroughly analyzed to identify possible conflicts, overlaps, and gaps. Analyzing requirements includes assessing their feasibility, clarity, verifiability, and prioritization.

4.1. Categorization of requirements

Requirements can be classified into various categories, such as functional and non-functional requirements.

4.1.1. Functional requirements

Functional cybersecurity requirements define the specific features and capabilities that must be implemented in systems to ensure security. These requirements encompass a wide range of measures aimed at protecting confidentiality, integrity, and availability. The key functional cybersecurity requirements are listed below [23].

1. **Authentication and Authorization**
    - *Authentication:*
        - Multi-factor authentication (MFA): Use of multiple authentication methods (e.g., password and biometric data or token).
        - Single Sign-On (SSO): Single login for access to multiple systems.
    - *Authorization:*
        - Role-Based Access Control (RBAC): Access based on user roles.
        - Attribute-Based Access Control (ABAC): Access based on user attributes like location or time.
2. **Data Protection**
    - *Encryption:*
        - Data at Rest Encryption
        - Data in Transit Encryption (e.g., TLS)
    - *Data Masking:* Masking sensitive data to protect confidentiality.
3. **Incident Detection and Response**
    - *Intrusion Detection Systems (IDS):*
        - Network IDS (NIDS)
        - Host-based IDS (HIDS)
    - *Intrusion Prevention Systems (IPS):*
        - Network IPS (NIPS)
        - Host-based IPS (HIPS)
4. **Access Management**
    - Identity Lifecycle Management
    - Access Auditing
    - Password Policies
5. **Endpoint Protection**
    - Antivirus Software
    - Anti-spam Filters
    - Firewalls
6. **Application Security**

- Secure Software Development
- Security Testing
- Web Application Firewalls (WAF)

7. **Configuration and Change Management**
    - Configuration Change Tracking
    - Configuration Compliance
    - Change Procedures
    - Security Impact Assessment

4.1.2. Non-functional requirements

Non-functional cybersecurity requirements describe the system's characteristics and attributes that are not directly related to its functionality, yet critical to its overall security, reliability, performance, and usability [12].

1. **Performance and Scalability**
    - Response Time
    - Throughput
    - Horizontal and Vertical Scalability
2. **Reliability and Recoverability**
    - Fault Tolerance
    - Operational Continuity
    - Recovery Procedures
    - Backup and Restore
3. **Security Assurance**
    - Confidentiality: Data Encryption
    - Integrity: Data Integrity Control
    - Availability: DDoS Protection, High Availability
4. **Usability**
    - Ease of Use: Interface, Documentation, Training
    - Automation: Automatic Updates, Automated Detection and Response

4.2. Documentation of requirements

Documenting requirements is essential for ensuring clarity and successful implementation. The key steps and recommendations for documenting cybersecurity requirements within an organization are outlined below.

4.2.1. Steps for documenting cybersecurity requirements

The following step-by-step approach offers a practical way to organize and formalize these requirements within an organization:

Step 1: Requirements identification

The first step in documenting cybersecurity requirements is collecting all relevant requirements from various sources:

- *Legislative and regulatory acts*: Requirements established by government authorities and industry standards (e.g., GDPR, ISO/IEC 27001).
- *Organizational policies and procedures*: Internal documents that define the organization's approach to information security management.

- *Technical specifications and architectural solutions*: Requirements derived from technical and system architecture decisions.

Step 2: Requirements analysis and alignment
After gathering the requirements, they must be analyzed and aligned with all stakeholders:

- *Conflict and duplication detection*: Identify and resolve potential conflicts or overlaps between requirements.
- *Requirements prioritization*: Determine the priority of the requirements based on their importance and impact on security.

Step 3: Requirements structuring
Structure cybersecurity requirements to facilitate ease of use and management:

- *Categorization*: Group requirements into categories (e.g., authentication, authorization, encryption, and access control).
- *Hierarchical structure*: Define a hierarchy to track dependencies between requirements.

Step 4: Requirements documentation
Documenting requirements involves creating detailed descriptions that contain all the necessary information:

- *Requirement title*: A short name reflecting the essence of the requirement.
- *Requirement description*: A detailed explanation of the requirement, its purpose, and the expected outcome.
- *Acceptance criteria*: The conditions under which the requirement is considered fulfilled.
- *Priority*: An indication of the requirement's priority (e.g., high, medium, or low).
- *Responsible parties*: The designation of the individuals or departments responsible for implementation and monitoring.

Step 5: Requirements review and approval
After the documentation is complete, the requirements must be reviewed and formally approved:

- *Stakeholder review*: Coordinate the documents with all relevant stakeholders, including the IT department, management, and the legal team.
- *Approval*: The organization's leadership must officially approve the documents.

4.2.2. Recommendations for documenting cybersecurity requirements

To effectively communicate, implement, and maintain cybersecurity requirements, organizations should follow a set of practical documentation principles:

1. **The usage of standards and templates:**
    - Use standardized templates to ensure consistency and clarity in requirement documentation.
    - Follow international standards, such as ISO/IEC 27001, to maintain high-quality documentation.
2. **Transparency and accessibility:**
    - Ensure documents are accessible to all relevant stakeholders.
    - Maintain a centralized repository for easy access to and updates of the requirements.
3. **Regular updates:**
    - Periodically review and update cybersecurity requirements in response to changes in legislation, technology, and business processes.

- Implement mechanisms for rapid updates in case of newly identified threats or vulnerabilities.

4. **Training and awareness:**
    - Conduct staff training on the importance and content of cybersecurity requirements.
    - Ensure that all employees understand their responsibilities regarding compliance with these requirements.
5. **Use requirements management tools:**
    - Use specialized tools for requirements management that enable effective tracking, analysis, and reporting on implementation progress.

5. Implementation, monitoring, and maintenance of cybersecurity requirements

The implementation of cybersecurity requirements involves developing, testing, and integrating security measures into an organization's information systems. This includes:

- Developing technical solutions that meet the defined requirements;
- Conducting tests to verify fulfillment of requirements;
- Integrating the solutions into existing systems and processes.

Monitoring and maintaining cybersecurity requirements are ongoing processes that include:

- Ongoing system monitoring to detect and respond to emerging threats;
- Updating requirements and solutions in response to changes in the technological environment and threat landscape;
- Conducting regular audits and security assessments.

Implementing cybersecurity requirements is a critical step in reliably protecting the organization's information systems and data. This process involves developing and integrating appropriate technical and organizational measures to fulfill documented requirements. The following are key steps and recommendations for implementing cybersecurity requirements (see Fig. 2).

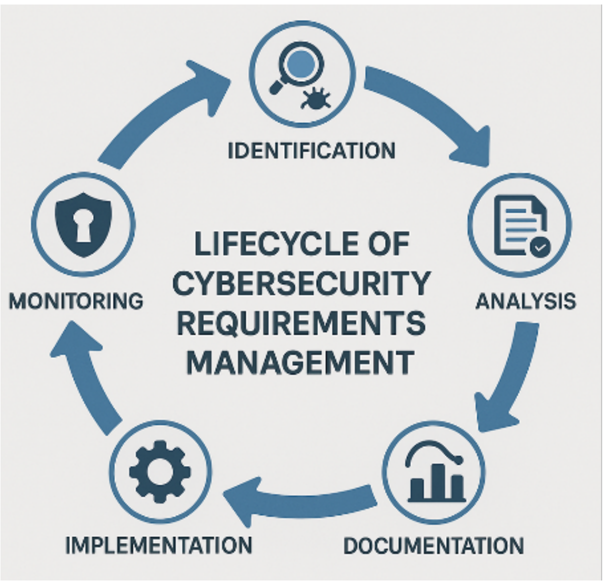

Figure 2: Lifecycle of cybersecurity requirements management.

5.1. Recommendations for implementing cybersecurity requirements

The following recommendations outline the key actions necessary for the effective execution of cybersecurity policies and technical controls:

1. **Integrate security across all stages of the system lifecycle:** Ensure that cybersecurity requirements are incorporated at every stage of system development and operation, from initial planning to decommissioning.
2. **Adopt best practices and standards:** Follow established best practices and frameworks such as NIST, ISO/IEC 27001 to achieve a high level of security assurance.
3. **Conduct regular assessments and improvements:** Perform periodic evaluations of the effectiveness of implemented controls and adjust them in response to emerging threats and new technologies.
4. **Engage stakeholders:** Involve management, IT personnel, and end users in the implementation and monitoring of cybersecurity measures to ensure understanding and support.
5. **Use automated tools:** Leverage automation for monitoring, analysis, and incident response to improve efficiency, accuracy, and timeliness.

6. Best practices in cybersecurity requirements management

6.1. Best practices in cybersecurity

1. **The use of standardized methodologies and tools for managing cybersecurity requirements.**
   These methodologies are key to ensuring process effectiveness and consistency within an organization. They provide structured approaches through systematic planning, transparency, and regulatory compliance. Tools automate and optimize processes, thereby increasing efficiency.
   Standardized methodologies include:
   - ISO/IEC 27001
   - NIST Cybersecurity Framework (CSF)
   - COBIT (Control Objectives for Information and Related Technologies)
   - ITIL (Information Technology Infrastructure Library)
2. **Active engagement with all stakeholders.**
3. **Regular training and upskilling of personnel.**
4. **Ensuring transparency and documentation of all processes.**

6.2. Overview of tools for managing cybersecurity requirements

1. **Jira** is a popular tool for project and requirements management that allows effective tracking of tasks and cybersecurity requirements.
   Functionality: Task tracking, project management, integration with other tools.
   Advantages: Flexibility, customization, support for Agile and Scrum methodologies.
2. **Confluence** is used to create, share, and manage documentation, including cybersecurity requirements.
   Functionality: Collaborative documentation, structured information storage, integration with Jira.
   Advantages: Ease of use, real-time collaboration, centralized documentation storage.
3. **ServiceNow** supports IT service management, including cybersecurity and requirements management.
   Functionality: Incident management, change management, configuration management.
   Advantages: Process integration, automation, analytics, and reporting.

4. **RSA Archer** is a risk management platform that enables organizations to manage risks and regulatory compliance.
   Functionality: Risk management, compliance, audits, security incident tracking.
   Advantages: Broad functionality, scalability, integration with other systems.
5. **Tenable** provides tools for vulnerability management and ensuring compliance with security requirements.
   Functionality: Vulnerability scanning, security monitoring, reporting.
   Advantages: Detailed vulnerability analysis, integration with other security systems, regularly updated threat databases.

A detailed analysis of these cybersecurity requirements management tools was also conducted by the authors (see Table 2) based on the following criteria:

- **FUNC**: Functionality for cybersecurity requirements management;
- **INTG**: Integration with external systems;
- **USAB**: Usability;
- **CYBO**: Cybersecurity-specific functionality;
- **CONF**: Configuration flexibility;
- **ANRE**: Analytics and reporting.

Table 2
Requirements Management Tools Comparison

Tools	FUNC	INTG	USAB	CYBO	CONF	ANRE
Jira	+	+	+	+/-	+	+/-
Confluence	+/-	+	+	-	+	+/-
ServiceNow	+	+	+/-	+	+/-	+
RSA Archer	+	+	+/-	+	+	+
Tenable	+/-	+	+/-	+	-	+

Based on the comparative analysis, it can be concluded that none of the tools under consideration fully cover cybersecurity management requirements. Jira and ServiceNow stand out for their flexibility, integration capabilities, and suitability for an Agile environment. However, they have a limited focus on security aspects. RSA Archer and Tenable have a clear focus on risk and vulnerability management, but are less convenient for Agile requirements management and team collaboration. Confluence, on the other hand, is a convenient documentation tool, but it lacks extensive capabilities for automating cybersecurity processes. Therefore, the choice of tool should be based on project specifics, risk level, and organizational needs — often, a combination of several platforms is advisable.

7. Analysis of modern scientific approaches to cybersecurity requirements management

Let us take a closer look at the current state of scientific research in this field.

Syrovatchenko's work [24] analyzes the legal aspects of ensuring cybersecurity in Ukraine, including an assessment of statistical data on the cyber environment and the role of national and international legislation in countering cyber threats. The author emphasizes the need to improve the legislative framework and international cooperation in cybersecurity.

In [25], Khudolii examines current challenges in Ukraine's cybersecurity landscape, including threats arising from digitalization and hybrid warfare. The author analyzes the Ukrainian government's measures to improve cybersecurity and proposes recommendations to enhance the protection system.

Tsvilii [26] investigates the cybersecurity certification system for ICT as a key element in securing the digital economy and public administration. The author analyzes existing certification standards and procedures and proposes improvements.

Trofymenko et al. [27] identify political, scientific, technical, organizational, and educational issues that must be addressed as part of a comprehensive response to cyber threats. The authors analyze the current state of cybersecurity in Ukraine and offer recommendations for improvement.

Admass, Munaye, and Diro [28] provide a review of the global cybersecurity landscape, including challenges, tactics, conditions, and trends. They highlight threats such as deepfake-based attacks and the need to adapt requirements management strategies accordingly.

Kim, Park, and Lee [29] present a Cybersecurity Requirements Management System (CRMS) as a framework for analyzing security requirements in the automotive industry. The system supports early-stage identification and implementation of security measures.

In [30], Cremer, Sheehan, and Smith explore the limitations of existing cyber risk management approaches, emphasizing the lack of accessible cyber risk data, which hampers effective decision-making and policy development.

Nguyen, Tran, and Le [31] provide an overview of cybersecurity in emerging technologies. They underline the need to integrate requirements management into early phases of tech implementation and identify associated risks.

Summary: The analysis of recent publications shows that current approaches to cybersecurity requirements management emphasize the need to improve regulatory frameworks, adopt industry-specific standards, integrate cyber risk management, and standardize security processes. Studies from Ukraine and globally highlight the importance of interdisciplinary strategies, international alignment, and the use of threat intelligence to ensure informed decision-making. Effective cybersecurity management is recognized as a multifaceted process involving legal, technical, and organizational elements.

8. Conclusions

This study analyzed modern approaches to cybersecurity requirements management in the context of software implementation. Cybersecurity requirements management is crucial for reliably protecting organizational information systems. Effectively identifying, analyzing, documenting, and implementing such requirements helps minimize risk and ensure regulatory compliance.

Legislative and regulatory acts play a key role in shaping secure digital ecosystems by providing clear organizational obligations. Compliance with these laws reduces risks and strengthens cybersecurity.

Developing and enforcing cybersecurity policies and procedures is vital for effective cyber risk management and alignment with legal requirements. Regularly updating these policies ensures adaptation to an evolving threat landscape.

Technical specifications and architectural solutions provide foundational tools for protecting systems from cyber threats. Their continuous improvement is necessary to meet changing conditions and address emerging risks.

Functional cybersecurity requirements target specific technical and organizational measures to safeguard systems and data. Their implementation improves risk posture, enhances security, and ensures regulatory compliance.

Non-functional cybersecurity requirements define performance and reliability attributes such as availability, scalability, and maintainability. These characteristics are essential for the secure and stable operation of systems.

Documenting cybersecurity requirements supports structured implementation and monitoring. Adopting best practices and using modern tools ensures consistency, traceability, and compliance.

Implementing cybersecurity requirements involves multiple phases: designing, testing, integrating solutions, staff training, and ongoing monitoring. Following best practices and continuously improving implemented measures allows organizations to respond effectively to threats and maintain a high level of protection.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] L. Li, et al., Logicedu: Enhancing computational logic understanding through web-based boolean logic simplification tool, in: 2024 21st International SoC Design Conference (ISOCC), 2024, pp. 390–391. doi:10.1109/ISOCC62682.2024.10762040.

[2] S. Deepak, J. A. Shah, N. Chetan, H. Sharda, New decision-making process based on set theory: Towards application of set theory, in: 2023 IEEE Int. Conf. on ICT in Business Industry & Government (ICTBIG), 2023, pp. 1–6. doi:10.1109/ICTBIG59752.2023.10456045.

[3] H. Wang, Network graph theory and organization model analysis based on mathematical modeling with the dynamic systematic data perspective, in: 2022 6th Int. Conf. on Trends in Electronics and Informatics (ICOEI), 2022, pp. 915–919. doi:10.1109/ICOEI53556.2022.9776767.

[4] Q. Yu, Z. Li, A bayesian model averaging method for software reliability assessment, in: 2020 Asia-Pacific Int. Symp. on Advanced Reliability and Maintenance Modeling (APARM), 2020, pp. 1–5. doi:10.1109/APARM49247.2020.9209504.

[5] O. Okoro, M. Zaliskyi, S. Dmytriiev, O. Solomentsev, O. Sribna, Optimization of maintenance task interval of aircraft systems, International Journal of Computer Network and Information Security 14 (2022) 77–89. doi:10.5815/ijcnis.2022.02.07.

[6] B. Yang, et al., A critical and comprehensive handbook for game theory applications on new power systems: Structure, methodology, and challenges, Protection and Control of Modern Power Systems (2024). doi:10.23919/PCMP.2024.000297.

[7] P. Shukla, S. K. Singh, A. Khamparia, A. Goyal, Nature-inspired optimization techniques, in: Nature-Inspired Optimization Algorithms, De Gruyter, 2023, pp. 137–152.

[8] R. Beniwal, V. Kumar, V. Sharma, Metaheuristics approaches towards secure and optimized routing in iot: A systematic literature review, in: 2024 Int. Conf. on Electrical Electronics and Computing Technologies (ICEECT), 2024, pp. 1–6. doi:10.1109/ICEECT61758.2024.10739076.

[9] T. T. Zin, A. S. T. Moe, C. N. Phyo, P. Tin, Fusion of strategic queueing theory and ai for smart city telecommunication system, in: 2024 IEEE 21st Int. Conf. on Mobile Ad-Hoc and Smart Systems (MASS), 2024, pp. 653–657. doi:10.1109/MASS62177.2024.00104.

[10] N. Zhang, Y. Chen, W. Yang, Z. Zhang, Y. Liu, W. Mao, Application of fault tree analysis for reliability evaluation and weak link identification..., in: 2021 IEEE Sustainable Power and Energy Conf. (iSPEC), 2021, pp. 4209–4214. doi:10.1109/iSPEC53008.2021.9735815.

[11] D. Kim, B. Jeon, K. C. Koo, Addressing timely ai technology standardization challenges through a hierarchical analysis approach, in: 2023 14th Int. Conf. on ICT Convergence (ICTC), 2023, pp. 1431–1433. doi:10.1109/ICTC58733.2023.10393654.

[12] ISO/IEC, Information security, cybersecurity and privacy protection — isms — requirements, 2022. doi:10.3403/30514785, iSO/IEC 27001:2022.

[13] European Parliament and Council, General data protection regulation (gdpr), 2016. Regulation (EU) 2016/679.

[14] National Institute of Standards and Technology, Cybersecurity framework 2.0, 2024. doi:10.6028/NIST.CSWP.02022024.

[15] U.S. Congress, Cybersecurity information sharing act (cisa), 2015. Public Law No: 114-113.

[16] U.S. Dept. of Health and Human Services, Health insurance portability and accountability act (hipaa), 2024. Amended 2024.

[17] U.S. Congress, Federal information security modernization act (fisma) of 2014, 2014.

[18] European Parliament and Council, Directive (eu) 2022/2555 on a high common level of cybersecurity, 2022.

[19] European Parliament and Council, Directive on privacy and electronic communications (eprivacy directive), 2002. Consolidated 2009.

[20] M. Zaliskyi, et al., Heteroskedasticity analysis during operational data processing of radio electronic systems, in: S. Shukla, A. Unal, J. V. Kureethara, D. Mishra, D. Han (Eds.), Data Science and Security, volume 290 of *Lecture Notes in Networks and Systems*, Springer, 2021, pp. 168–175. doi:10.1007/978-981-16-4486-3_18.

[21] Y. Averyanova, et al., UAS cyber security hazards analysis and approach to qualitative assessment, in: S. Shukla, A. Unal, J. V. Kureethara, D. Mishra, D. Han (Eds.), Data Science and Security, volume 290 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2021, pp. 258–265. doi:10.1007/978-981-16-4486-3_28.

[22] I. Ostroumov, et al., Relative navigation for vehicle formation movement, in: IEEE 3rd KhPI Week on Advanced Technology, 2022, pp. 1–4. doi:10.1109/KhPIWeek57572.2022.9916414.

[23] QATestLab, Non-functional requirements: Examples, types, approaches, n.d. URL: https://training.qatestlab.com/blog/technical-articles/non-functional-requirements-examples-types-approaches.

[24] O. Syrovatchenko, Legal aspects of ensuring cybersecurity in ukraine, Law Herald (2024) 78–85.

[25] A. Khudolii, Cybersecurity: Current challenges facing ukraine, Acta De Historia & Politica: Saeculum XXI (2019) 138–146.

[26] O. O. Tsvilii, Cybersecurity certification system for ict, Scientific Works of O.S. Popov ONAZ (2020) 121–126.

[27] O. H. Trofymenko, Y. V. Prokop, N. I. Lohinova, O. V. Zadereiko, Cybersecurity in ukraine: Analysis of the current state, Information Protection 21 (2019) 3–12.

[28] W. S. Admass, Y. Y. Munaye, A. A. Diro, Cyber security: State of the art, challenges and future directions, Cyber Security and Applications 2 (2024). URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=129715, article ID: 100031.

[29] H. Kim, J. Park, S. Lee, A framework for cybersecurity requirements management in the automotive industry, Sensors 23 (2023) 4979. doi:10.3390/s23104979.

[30] S. Cremer, B. Sheehan, J. Smith, Cyber risk and cybersecurity: A systematic review of data availability, Global Policy and Public Risk 47 (2022) 123–139.

[31] T. T. Nguyen, M. H. Tran, D. H. Le, Managing cybersecurity risks in emerging technologies, Journal of Emerging Technologies 5 (2023) 89–102.