DOI: 10.32347/2412-9933.2025.64.177-184
UDC 004.056.5:004.41

Tkachenko Vitalii
Postgraduate Student at the Department of Theory and Technology of Programming,
https://orcid.org/0009-0004-5812-5313
Taras Shevchenko National University of Kyiv, Kyiv
Dolhopolov Serhii
Postgraduate Student at the Department of Information Technologies,
https://orcid.org/0000-0001-9418-0943
Kyiv National University of Construction and Architecture, Kyiv

TECHNOLOGICAL SOLUTIONS FOR THE APPLICATION OF THE REGULATORY FRAMEWORK FOR TECHNICAL INFORMATION PROTECTION

Abstract. *In modern conditions of rapid digitalization of management processes and data processing, the issue of ensuring reliable information protection in automated systems becomes critically important for state and private institutions of Ukraine. The regulatory framework of Technical Protection of Information (TPI), formed in the late 90s, lays down fundamental security principles; however, its practical implementation in the context of modern architectural solutions and dynamic threats often causes difficulties for specialists. The relevance of the study is driven by the necessity to harmonize the classic requirements of regulatory documents with modern technological approaches to building information systems, as well as the need to develop clear algorithms for implementing Complex Information Protection Systems (CIPS). The article is devoted to solving the problem of adapting theoretical legislative provisions to practical cases of deploying security systems. A comprehensive analysis of legal and regulatory acts in the field of TPI, particularly the classic requirements of regulatory documents 1.1-003-99, 2.5-004-99, and 2.5-005-99, was conducted. Based on this analysis, a complex of technological solutions and a practical method for implementing protection measures have been developed and presented. A step-by-step algorithm is proposed, covering all stages of CIPS creation: from information categorization based on confidentiality, integrity, and availability properties to the selection and configuration of functional protection profiles. Special attention is paid to the methodology for determining the class of an automated system depending on its architecture (local, distributed) and data processing mode. The process of integrating security requirements into the Software Development Life Cycle (SDLC) is investigated, allowing a transition from «superimposed» security to a «Security by Design» model. Recommendations regarding the implementation of administrative and discretionary confidentiality, integrity, and observability services are developed. A method for evaluating the effectiveness of implemented measures, based on a combination of documentation analysis, personnel interviewing, and instrumental testing of protection mechanisms, is also proposed. The results of the study confirm that the universality of the classic regulatory framework allows for its effective application in protecting modern systems, provided adapted approaches are used. The proposed approach enables organizations of various ownership forms and scales (from small enterprises to large distributed corporations) to build an economically justified and reliable protection system. The practical application of the developed technological solutions contributes to minimizing information security risks, ensuring compliance with legislative requirements, and increasing the general level of cyber resilience of the state's information infrastructure.*

Keywords: Technical Protection of Information; Complex Information Protection System; protection profile; categorization of processed information; System Development Life Cycle

Problem Statement

Global trends in the development of the information society are unequivocally directed towards the total digitalization of management processes, economy, and social interaction. The implementation of e-government, the transition of business to digital ecosystems, and the use of cloud technologies create an environment where information becomes the most valuable asset. In parallel with the growth of data processing volumes, the level of cyber threats is growing exponentially, making information security a critical factor for the survival of any organization.

In this context, the construction of reliable protection systems in Ukraine relies on the regulatory framework of Technical Protection of Information (TPI),

the foundation of which was laid by the classic requirements of regulatory documents. These documents contain universal principles that remain relevant. However, in practice, a significant contradiction arises: modern information system architectures (distributed, microservice, virtualized) require flexible approaches, while regulatory requirements are often perceived by specialists as static and dogmatic.

Today's realities require cybersecurity specialists not just to formally comply with regulator prescriptions, but to have a deep understanding of how to transform requirements for confidentiality, integrity, and availability into specific technical settings of modern hardware and software. Most organizations face a «competence gap» problem: lawyers and managers operate with categories of regulatory acts, while technical specialists deal with configuration parameters. The absence of a clear algorithm for translating regulatory requirements into the language of engineering solutions leads to protection systems being either imitated («paper security») or redundant and economically unjustified.

Tasks that need to be solved in the process of creating a Complex Information Protection System (CIPS) include: correct categorization of processed information; adequate selection of a protection profile corresponding to real threats; integration of security mechanisms without disrupting business processes; ensuring real, not declarative, compliance with standards.

Based on this, the urgent task is to create applied technological solutions that would step-by-step describe the process of implementing the TPI regulatory framework in modern conditions. The paper proposes to consider a practical approach to applying the classic requirements of regulatory documents, which allows systematizing the process of building secure systems from the design stage to commissioning.

Aim of the Study

The aim of the work is to develop practical technological solutions for applying the classic requirements of regulatory documents on technical protection of information through a detailed description of system categorization procedures, justified selection and configuration of protection profiles, as well as the integration of security measures into the system development life cycle to ensure effective information protection in organizations of various types.

Analysis of Key Studies and Publications

The normative foundation of Technical Protection of Information (TPI) in Ukraine is based on a complex of regulatory documents developed in the late 1990s, which still remain valid for state information resources. Fundamental principles and the conceptual apparatus in this area are defined in the classic requirements of regulatory documents 1.1-003-99, which establishes unified terminology for all subjects of the protection system [1]. The security assessment methodology, based on the criteria of confidentiality, integrity, availability, and observability, is detailed in the classic requirements of regulatory documents 2.5-004-99 [2]. The classification of automated systems (AS) depending on the data processing mode and architecture is enshrined in the classic requirements of regulatory documents 2.5-005-99 [3]. These documents have formed a classic protection paradigm based on strictly defined profiles and trust levels.

The current state of state policy in the field of TPI and the challenges associated with the need for its transformation are explored in the works of domestic scientists. In particular, Sadkovyi V. P., Klochko A. M., et al. consider the regulatory and legal aspects of regulating cybersecurity in the context of public administration, emphasizing the need to harmonize national legislation with European standards [4]. Dosenko S. D. in his research focuses on technical problems of information protection, analyzing the shortcomings of outdated approaches in the context of modern cyber threats [5].

An important area of research is the integration of security measures directly into system creation processes. In this context, the work of Shirtz D. et al., dedicated to the concept of «Security by Design» (SbD), deserves attention [6]. The authors propose a holistic methodology for increasing the resilience of critical infrastructure, which goes beyond purely technical solutions and covers «soft» factors such as security culture and personnel awareness. The key idea of the study is that SbD is a continuous discipline that begins at the requirements definition stage and lasts throughout the entire System Development Life Cycle (SDLC), allowing vulnerabilities to be detected at early stages [6].

Developing the theme of proactive protection, Soundararajan B. emphasizes the cost-effectiveness of implementing security principles (such as «least privilege» and «defense in depth») in the early stages of software development. The author argues that investing in secure coding and automated testing (Static/Dynamic Analysis) during design costs significantly less than fixing vulnerabilities after system deployment [7].

A comprehensive approach to security is impossible without considering the operational stage. In his work, Gao Y. expands the protection methodology, covering both development and Operations. The author details technical measures to counter modern threats (SQL injection, XSS, CSRF) and emphasizes the critical importance of continuous monitoring using SIEM systems, IDS/IPS, and vulnerability analysis tools. The study confirms the need to combine secure environment configuration (Environment Security Configuration) with regular audits and disaster recovery plans, which is

a practical implementation of availability and observability requirements in modern conditions [8].

Particular attention in the context of modern distributed systems is paid to issues of cryptographic protection and cloud environment security. Shashank S. and Venkata G. M. in their study analyze the integration of encryption protocols (TLS 1.3, AES-256) into CI/CD processes and containerization (Kubernetes) [9]. The authors emphasize that for compliance with NIST and ISO 27001 standards, the transition to «crypto-agility» – the ability of systems to quickly adapt to new algorithms, in particular Post-Quantum Cryptography (PQC), is critical, which is a new challenge for long-term information protection planning.

Furthermore, modern protection strategies increasingly rely on intelligent data analysis technologies. Dolhopolov S. et al. investigate the use of neural network systems for threat detection to prevent data breaches [10]. This confirms the trend of shifting from signature-based methods to heuristic analysis using Machine Learning, which is a necessary component of the «Observability» subsystem in high-class systems to detect anomalies that cannot be identified by standard means.

A separate challenge for modern protection methodology is the rapid implementation of Generative Artificial Intelligence (GenAI) tools. Kenchi P. V., Kondhalkar P., and Kharat S. in their study analyze the dual nature of AI assistants (GitHub Copilot, ChatGPT) in development [11]. The authors point out that although GenAI significantly increases productivity and automates testing, it creates new risks: «hallucinations», generation of insecure code, and intellectual property issues, which requires the mandatory implementation of human oversight mechanisms and ethical checks in secure development processes.

However, technical means cannot guarantee security without a proper organizational component. In a comprehensive review of the theory and practice of secure development, Odera D., Otieno M., and Ounza J. E. emphasize that software security is a socio-technical problem. The authors identify «human factor» and «Security Culture» as critical elements that are often ignored [12]. The study highlights the importance of Security Governance – managing security through compliance with standards (ISO 27001, NIST) and regular staff training, without which even the most advanced protection algorithms become vulnerable due to configuration errors or social engineering.

A critically important element of modern methodology is the automation of auditing and ensuring data privacy (Privacy by Design). Baldassarre M. T., Barletta V. S., et al. in their study propose specialized tools for improving privacy in software development [13]. The authors demonstrate how automated tools can help developers comply with regulatory requirements (such as GDPR) directly during the coding process, which is a modern alternative to traditional paper compliance checks. At the same time, Hu W. and Wang Z. in their study raise the critical issue of the performance of security audit tools [14]. The authors developed a methodology for load testing (performance testing) for audit products, proving that without checking the speed of data collection and event logging under load, it is impossible to guarantee the completeness of audit logs, which is a direct requirement of the classic requirements of regulatory documents regarding observability.

Analysis of current sources indicates a gap between the theoretical requirements of the TPI regulatory framework and technological realities. While foreign researchers [6–14] offer advanced mechanisms (DevSecOps, AI-coding, Performance Auditing), and domestic authors [4–5] point to the need for reforms, there is no single applied methodology. It is necessary to develop an algorithm that would allow Ukrainian organizations to meet the strict requirements of the classic requirements of regulatory documents [1–3], integrating modern technical solutions and verification methodologies into a single CIPS construction process.

Main Research

The first and fundamental step in building a Complex Information Protection System is to determine the criticality category of the processed information and, based on it, the class of the automated system (AS). Instead of intuitively selecting protection means, it is proposed to use the procedure of inventory and qualitative assessment of assets.

The categorization process begins with forming a complete list of information types circulating in the system (e.g., employee personal data, technological information, financial reporting, etc.). Requirements for ensuring three basic security properties are defined for each type of information: Confidentiality (C) – the need to prevent unauthorized access; Integrity (I) – the need to protect against unauthorized modification or destruction; Availability (A) – the need to ensure access to information at the required time for authorized users.

The criticality level for each property is assessed on a graduated scale of possible consequences resulting from a security breach. This assessment considers various impact factors, ranging from no significant consequences to critical losses that could entail catastrophic outcomes for the organization, such as bankruptcy, severe legal penalties, or threats to national security.

Determining the general category of the information system is carried out according to the «principle of maximum requirements» (often referred to as the high-water mark principle). Accordingly, the system categories for confidentiality, integrity, and availability properties are set equal to the highest values

assigned among all types of processed information. Such a conservative strategy guarantees that the entire system will receive the level of protection necessary for the most valuable and critical asset, effectively leveling the risk of underestimating potential threats and ensuring that the security perimeter is as strong as its most sensitive component requires.

The subsequent stage involves determining the specific class of the AS, which depends not only on the established information category but also on the technological and architectural features of the system's construction. This classification takes into account factors such as the presence of connections to external global networks (Internet), the number of users, the geographical distribution of components, and the mode of data processing. Generalized characteristics of classes, strictly adhering to the classic requirements of regulatory documents (specifically ND TZI 2.5-005-99) and adapted to modern network realities [3], are presented in Table 1.

Table 1 – ***Matrix for Determining the Class of an Automated System***

Characteristic	AS-1	AS-2	AS-3
Architecture	Single-machine, isolated (Stand-alone)	Local Area Network (LAN) within a controlled zone	Distributed network (WAN), presence of remote branches
Users	One user at a time (Single-user)	Multi-user, shared access	Multi-user, access from external networks
Communication Channels	Absent or local interfaces	Physically or organizationally protected within the facility	Use of unprotected channels (Internet, Public Network)
Threat Level	Low (threats mainly of physical access)	Medium (insiders, local attacks)	High (external attacks, traffic interception, DDoS)
Typical Example	Workstation for processing classified information (air-gapped)	Corporate office network, internal ERP server	Cloud system, web portal, interdepartmental system

After determining the class of the system, it is necessary to select a Standard Functional Protection Profile (SFPP). However, standard profiles are often redundant or insufficient for specific conditions. Therefore, an algorithm for adaptive profiling is proposed (Figure 1), which allows modifying the basic set of security services.

Stage 1. Selection of the Basic Profile. For the most common Class 2 systems (Local Area Networks), a profile is selected depending on the information classification level. For example, profile 2.C.1 (original «2.K.1») provides minimal protection (basic authentication), while 2.C.6 (original «2.K.6») provides maximum protection (mandatory access control, protection against covert channels).

Stage 2. Risk and Threat Analysis. H At this stage, the basic profile is checked for compliance with real threats. Using threat analysis methodologies (e.g., STRIDE), the need to strengthen specific protection functions not covered by the standard set is determined.

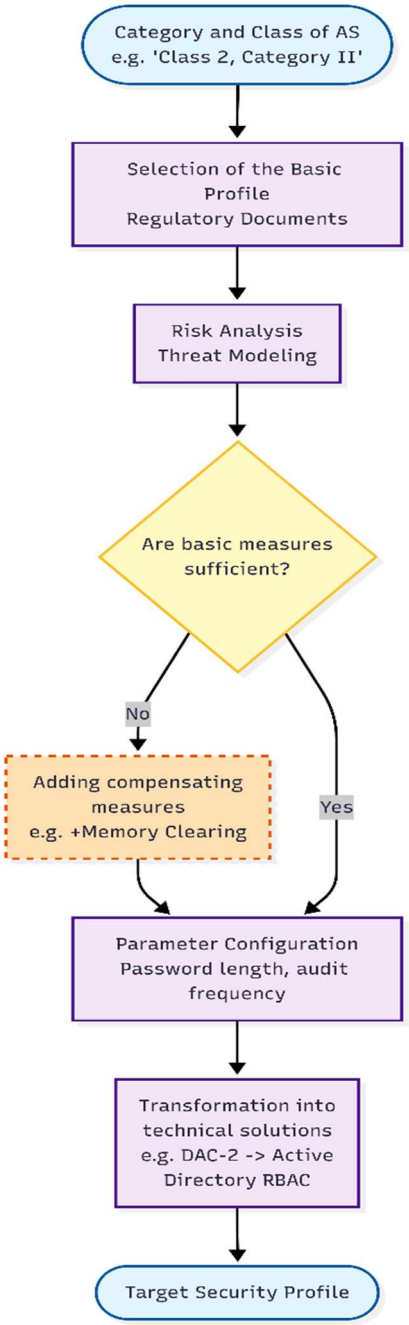

Figure 1 – Algorithm for Adaptive Selection and Configuration of the Protection Profile

Stage 3. Customization (Configuration). The process of adding or excluding security services. For example, if the system processes personal data, it is advisable to add the RAM clearing service (Object Reuse) to profile 2.C.3 (original «2.К.3»), even if it is not mandatory for this level, in order to minimize data leakage risks.

Stage 4. Technical Implementation. Abstract requirements of regulatory documents (e.g., service codes АС-2 (original «КА-2»), СС-1 (original «НК-1») are transformed into specific technical solutions. The connection between regulatory requirements and modern technologies is presented in Table 2.

The proposed Table 2 demonstrates the practical value of the methodology: it serves as a «translation dictionary» for engineers, allowing the implementation of outdated terminological requirements through modern industrial standards.

Effective implementation of the selected protection profile is impossible without integrating security requirements directly into development and operation processes (Security by Design). The traditional approach, where a protection system is «superimposed» on an already finished infrastructure, is economically inefficient and leaves architectural vulnerabilities.

Considering the specified system challenges, a model for synchronizing the stages of creating a Complex Information Protection System with the stages of the Software Development Life Cycle (SDLC) is proposed. The correspondence of stages and necessary measures is presented in Table 3.

The visualization of the model for synchronizing CIPS stages with SDLC stages is presented in Figure 2. Such an approach allows identifying discrepancies with regulatory requirements at the design and coding stages, reducing the cost of error correction.

The final stage of the methodology is evaluating the effectiveness of the implemented measures. Unlike the classic approach, which is often limited to checking the availability of documentation, we propose a three-level verification model that combines organizational and technical methods. The iterative nature of this process, which ensures a closed cycle of security improvement, is schematically shown in Figure 3.

Table 2 – ***Transformation of Security Services from Regulatory Documents into Modern Technical Solutions***

Criteria Group	Service Code (Original)	Requirement Essence	Modern Technical Implementation
Confidentiality (C)	IA (НИ)	User authentication	MFA (Multi-Factor Authentication), Kerberos, X.509 certificates, biometrics
	DAC (КД)	Discretionary access control	ACL (Access Control Lists), RBAC (Role-Based Access Control) in Active Directory
	CE (КВ)	Data protection during transmission	TLS 1.3 protocols, IPsec, SSH, VPN tunneling
Integrity (I)	DI (ЦД)	Protection against modification	Electronic signatures (Digital Signature), hash functions (SHA-256), Blockchain registries
	RB (ЦО)	Ability to roll back to state	Snapshots (Veeam, VMware), transactional DB logs, Git versioning
Observability	REG (НР)	Event registration (audit)	Centralized SIEM systems (Splunk, ELK Stack), Syslog servers
Availability	FT (ДС)	Fault tolerance	Clustering (Kubernetes), Load Balancers, RAID arrays, geo-redundancy

Table 3 – ***Matrix of Integrating TPI Measures into DevSecOps Processes***

SDLC Stage	Security Task (TPI)	Practical Implementation and Tools
Plan	Determination of category and class of AS. Formation of Security Policy.	Threat Modeling, determining the budget for protection means.
Design	Development of CIPS architecture. Selection of protection profile.	Designing network segmentation, selection of cryptographic protocols, design of authentication scheme.
Build	Implementation of functional security services (authentication, logging).	SAST (Static Application Security Testing) – automatic code analysis at the writing stage (Secure Coding).
Test	Preliminary testing of CIPS. Verification of settings.	DAST (Dynamic Application Security Testing), functional testing of protection mechanisms, load testing of audit.
Deploy	Pilot operation. Fixing checksums of software.	Automated configuration deployment (Infrastructure as Code), configuration of perimeter protection means.
Operate	Administration of protection means, log analysis, incident response.	Continuous monitoring (SIEM), Vulnerability Management, regular updating (Patching).

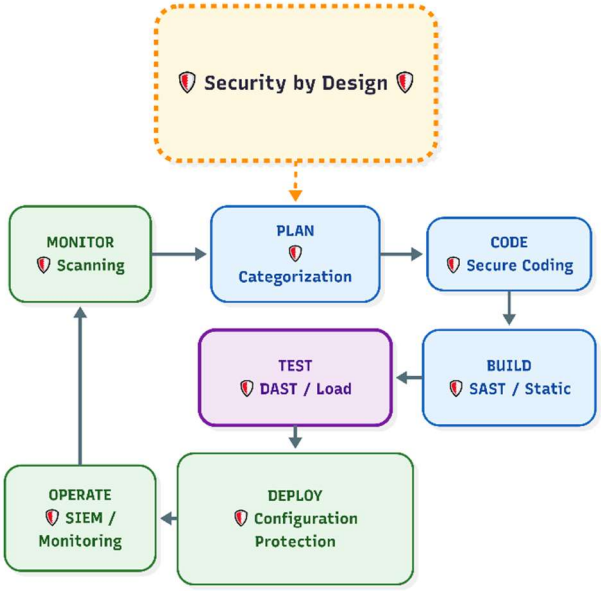

Figure 2 – Model of Integrating TPI Measures into the Life Cycle (DevSecOps)

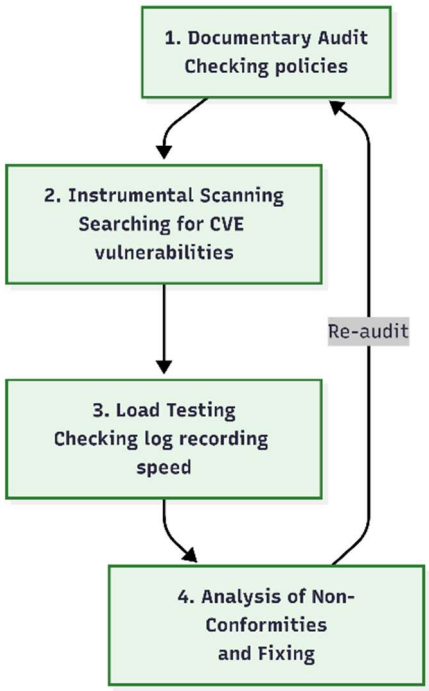

Figure 3 – Iterative Process of Assessment and Verification of CIPS

Level 1. Expert-Documentary Analysis. This initial stage involves a meticulous review of the organizational and administrative foundation of the security system. Experts assess the availability, relevance, and quality of regulatory documentation, including the Security Policy, Protection Plan, administrator instructions, and user guidelines. Beyond merely checking for the existence of these documents, the analysis evaluates their alignment with current business processes and regulatory requirements. Furthermore, personnel interviewing is conducted to verify the real awareness of employees regarding security rules and their adherence to established protocols. This «human-centric» verification is crucial for minimizing the risks of «paper security», where formal compliance exists only in documentation but not in actual practice.

Level 2. Instrumental Vulnerability Analysis. At this technical stage, the system undergoes a comprehensive examination using specialized software. Automated scanning tools, such as OpenVAS, Nessus, or similar enterprise-grade solutions, are deployed to scan the entire infrastructure for known Common Vulnerabilities and Exposures (CVE). The scan covers operating systems, application software, network services, and configurations. It identifies critical issues such as incorrect port configurations, usage of weak or default passwords, unpatched software versions, and insecure encryption settings. The outcome of this phase is a detailed technical report that provides an objective assessment of the system's current state and its compliance with the technical requirements of the selected protection profile.

Level 3. Load Testing of Security Functions (Stress Testing). This is a critically important, yet often overlooked, stage of verification. It goes beyond standard functionality testing to check the resilience of security subsystems under extreme conditions. Specifically, it involves testing the ability of the audit and event logging subsystem to operate correctly under peak loads, such as during a massive DDoS attack or a high-intensity brute-force attempt. The goal is to ensure that the system does not drop audit logs or fail to register security events when the flow of data exceeds standard operational parameters, thereby guaranteeing the «observability» requirement is met even during critical incidents. The universality of the proposed methodology allows for adapting protection strategies to the unique specifics and scale of any organization.

Organizations operating medium-class local area networks require a more comprehensive strategy focused on centralized access control and detailed auditing. Essential technical measures include implementing directory services (like Active Directory) for unified authentication, logical network segmentation (VLANs) to isolate critical assets, and automated log collection systems. Given that the human factor remains the primary attack vector in this segment, establishing regular staff training programs to counter social engineering and phishing attacks becomes a critical component of the defense strategy.

Large third-class systems with distributed architectures require complex, high-end technical solutions. This includes mandatory cryptographic protection of traffic (VPN tunnels) for inter-branch communication, deployment of Intrusion Detection/Prevention Systems (IDS/IPS), and centralized Security Information and Event Management (SIEM) or Security Operations Centers (SOC) for real-time incident

response. Industry specifics are also deeply integrated: the banking sector prioritizes transaction integrity and non-repudiation; medical institutions focus on strict data confidentiality through mandatory access controls; and manufacturing enterprises prioritize the high availability and fault tolerance of technological processes (OT/SCADA security).

Conclusions

The study developed and substantiated practical technological solutions for applying the regulatory framework of technical protection of information, which allows adapting the fundamental requirements of state standards to the operating conditions of modern information and telecommunication systems. The proposed approach solves the urgent problem of the gap between static regulatory prescriptions and the dynamics of technological development, offering tools for building flexible and effective protection systems. The systematization of asset categorization and system classification procedures made it possible to move away from subjective assessments, ensuring an objective determination of the required security level based on the analysis of real consequences of a violation of confidentiality, integrity, or availability of information.

A key scientific and practical result of the work is the creation of an adaptive algorithm for selecting and configuring protection profiles. This mechanism allows transforming abstract requirements of regulatory documents into specific technical solutions, such as multi-factor authentication, cryptographic protection of communication channels, and centralized event auditing. Implementing such an approach ensures the construction of an economically justified protection system that not only formally complies with legislation but is also capable of countering current cyber threats without excessive spending of resources on redundant security measures.

An important achievement of the study is the development of a model for integrating technical protection requirements into the software development life cycle. Synchronizing the stages of creating a comprehensive protection system with DevSecOps processes allows implementing the principle of proactive security, identifying and eliminating vulnerabilities at the design and coding stages, which significantly reduces the cost of fixing errors compared to the traditional approach of imposing protection measures on already finished infrastructure.

The final element of the proposed methodology was a comprehensive effectiveness assessment model that combines organizational checks with instrumental analysis and load testing. This approach guarantees the transition from declarative security to confirmed functional stability of the system, ensuring reliable logging of security events even under peak loads. The practical application of the developed recommendations will allow state and commercial organizations to increase the level of cyber resilience of their information systems, while ensuring full compliance with the requirements of current Ukrainian legislation in the field of information protection.

References

1. Department of Special Telecommunication Systems and Protection of Information of the Security Service of Ukraine. (1999). *Terminology in the field of information protection in computer systems from unauthorized access* (ND TZI 1.1-003-99). DSTSZI SBU.

2. Department of Special Telecommunication Systems and Protection of Information of the Security Service of Ukraine. (1999). *Criteria for evaluating information security in computer systems from unauthorized access* (ND TZI 2.5-004-99). DSTSZI SBU.

3. Department of Special Telecommunication Systems and Protection of Information of the Security Service of Ukraine. (1999). *Classification of automated systems and standard functional profiles of protection of processed information from unauthorized access* (ND TZI 2.5-005-99). DSTSZI SBU.

4. Sadkovyi, V. P., Klochko, A. M., Borysova, L. V., Nikitina, L. O., & Kolomiiets, V. S. (2023). State policy in the field of technical protection of information. *Bulletin of the National University of Civil Protection of Ukraine. Series: Public Administration*, 2 (19), 429–436.

5. Dosenko, S. D. (2021). Technical protection of information: Main problems and ways to solve them. *Herald of Lviv University of Trade and Economics. Technical Sciences*, 27, 27–32. https://doi.org/10.36477/2522-1221-2021-27-04

6. Shirtz, D., Koberman, I., Elyashar, A., Puzis, R., & Elovici, Y. (2024). Enhancing energy sector resilience: Integrating security by design principles. *ArXiv*, 2402.11543. https://doi.org/10.48550/arXiv.2402.11543

7. Soundararajan, B. (2019). Proactive software development using secure by design principles. *International Journal for Multidisciplinary Research*, 1 (3), 1–12. https://doi.org/10.36948/ijfmr.2019.v01i03.39048

8. Gao, Y. (2024). Analysis of software development and operation measures from the perspective of security technology. *Journal of Electronic Research and Application*, 8 (6), 145–151. https://doi.org/10.26689/jera.v8i6.9024

9. Shashank, S., & Venkata, G. M. (2025). Secure software development: Integrating encryption protocols from design to deployment. *International Journal of Applied Mathematics*, 38 (2s), 1190–1213. https://doi.org/10.12732/ijam.v38i2s.714

10. Dolhopolov, S., Honcharenko, T., Fedusenko, O., Khrolenko, V., Hots, V., & Golenkov, V. (2024). Neural network threat detection systems for data breach protection. *Proceedings of the 2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)*, 415–421. https://doi.org/10.1109/SIST61555.2024.10629526

11. Kenchi, P. V., Kondhalkar, P., & Kharat, S. (2025). Role of generative AI in software development. *International Journal of Scientific Research in Engineering and Management*, 9(11). https://doi.org/10.55041/IJSREM53791

12. Odera, D., Otieno, M., & Ounza, J. E. (2023). Theory and practice in secure software development lifecycle: A comprehensive survey. *World Journal of Advanced Research and Reviews*, 18(3), 053–078. https://doi.org/10.30574/wjarr.2023.18.3.0944

13. Baldassarre, M. T., Barletta, V. S., Caivano, D., Dimauro, G., & Piccinno, A. (2022). A tool for improving privacy in software development. *Sensors*, 22(23), 9196. https://doi.org/10.3390/s22239196

14. Hu, W., & Wang, Z. (2025). Network security audit product performance testing methodology and practice. *Proceedings of the 2025 5th International Conference on Computer Network Security and Software Engineering (CNSSE 2025)*, 14–19. https://doi.org/10.1145/3732365.3732368

The article has been sent to the editorial board 10.12.2025

Ткаченко Віталій Андрійович
Аспірант кафедри теорії та технології програмування,
https://orcid.org/0009-0004-5812-5313
Київський національний університет імені Тараса Шевченка, Київ
Долгополов Сергій Юрійович
Аспірант кафедри інформаційних технологій,
https://orcid.org/0000-0001-9418-0943
Київський національний університет будівництва і архітектури, Київ

ТЕХНОЛОГІЧНІ РІШЕННЯ ЗАСТОСУВАННЯ НОРМАТИВНОЇ БАЗИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. *У сучасних умовах стрімкої цифровізації процесів управління та обробки даних питання забезпечення надійного захисту інформації в автоматизованих системах набуває критичного значення для державних та приватних установ України. Нормативна база технічного захисту інформації (ТЗІ), сформована наприкінці 90-х років, закладає фундаментальні принципи безпеки, проте її практична імплементація в умовах сучасних архітектурних рішень та динамічних загроз часто викликає труднощі у фахівців. Актуальність дослідження зумовлена необхідністю гармонізації класичних вимог нормативних документів (НД) із сучасними технологічними підходами до побудови інформаційних систем, а також потребою у розробці чітких алгоритмів впровадження комплексних систем захисту інформації (КСЗІ). Стаття присвячена вирішенню проблеми адаптації теоретичних положень законодавства до практичних кейсів розгортання систем безпеки. Проведено комплексний аналіз нормативно-правових актів у сфері ТЗІ, зокрема НД ТЗІ 1.1-003-99, 2.5-004-99 та 2.5-005-99. На основі цього аналізу розроблено та представлено комплекс технологічних рішень та практичний метод впровадження заходів захисту. Запропоновано покроковий алгоритм, який охоплює всі стадії створення КСЗІ: від категоризації інформації за властивостями конфіденційності, цілісності та доступності до вибору та налаштування функціональних профілів захищеності. Особливу увагу приділено методиці визначення класу автоматизованої системи залежно від її архітектури (локальна, розподілена) та режиму обробки даних. Досліджено процес інтеграції вимог безпеки в життєвий цикл розробки програмного забезпечення (SDLC), що дозволяє перейти від «накладеної» безпеки до моделі «безпека через дизайн» (security by design). Розроблено рекомендації щодо реалізації послуг адміністративної та довірчої конфіденційності, цілісності та спостереженості. Також запропоновано метод оцінювання ефективності впроваджених заходів, який базується на комбінації аналізу документації, інтерв'ювання персоналу та інструментального тестування механізмів захисту. Результати дослідження підтверджують, що універсальність класичної нормативної бази дає змогу ефективно застосовувати її для захисту сучасних систем за умови використання адаптованих підходів. Практичне застосування розроблених технологічних рішень сприятиме мінімізації ризиків інформаційної безпеки, забезпеченню відповідності законодавчим вимогам та підвищенню загального рівня кіберстійкості інформаційної інфраструктури держави.*

Ключові слова: технічний захист інформації; комплексна система захисту інформації; профіль захищеності; категоризація оброблюваної інформації; життєвий цикл розробки системи; НД ТЗІ

Link to publication

APA Tkachenko, V., & Dolhopolov, S. (2025). Technological Solutions for Practical Application of the Regulatory Framework of Technical Protection of Information. *Management of Development of Complex Systems*, 64, 177–184, dx.doi.org\10.32347/2412-9933.2025.64.177-184.

ДСТУ Ткаченко В. А., Долгополов С. Ю. Технологічні рішення застосування нормативної бази технічного захисту інформації. *Управління розвитком складних систем.* Київ, 2025. № 64. С. 177 – 184, dx.doi.org\10.32347/2412-9933.2025.64.177-184.