KAPITEL 5 / *CHAPTER 5* [19]
STANDARDIZATION AND CERTIFICATION OF SOFTWARE IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES

DOI: 10.30890/2709-2313.2025-42-04-048

5.1 General provisions on standards, their classification. Activities of national and international organizations

In the field of quality, standardization and certification of information technology (ICT), the general provisions on standards and their classification constitute a fundamental basis for understanding the processes that ensure the interoperability, reliability and efficiency of digital systems. In 2025, as the global digital transformation accelerates due to artificial intelligence, cloud computing and the Internet of Things (IoT), standardization becomes not just a technical tool, but a strategic mechanism for integrating technology into everyday life, business and government. It helps reduce risks such as cyber threats or system incompatibility, and stimulates innovation by allowing developers and organizations to rely on common norms. The activities of national and international organizations in this field ensure the harmonization of standards, reflecting global trends such as the emphasis on sustainability and the ethical use of AI. This section examines key aspects of standardization, from its concept to the role of organizations, highlighting their relevance for the ICT sector.

Standardization as a concept is a systematic process of establishing and applying uniform norms, rules and requirements for objects, processes or services in order to regulate activities in a certain area. In the context of ICT, it covers everything from software algorithms to network protocols and is based on consensus among stakeholders, including experts, manufacturers and regulators. The characteristics of standardization are that it is voluntary in many cases (although for critical systems such

[19]***Authors:*** *Antonenko Artem Vasylovych, Tolok Galina Arsenivna, Brovenko Tetiana Viktorivna, Vostrikov Sergii Oleksandrovych, Chechyk Serhii Viktorovych, Tkachenko Oleksandr Viktorovich, Didovets Vladyslav M., Kozhemiakin Oleksandr V., Borodavko Maksym I., Nazarenko Dmitry O.*
Number of characters: *68637*
Author's sheets: ***1****,72*

as cybersecurity it may be mandatory), universal (applicable to different levels of technology) and dynamic (continuously updated, for example in 2025 to take into account new standards for AI). This process not only unifies technical parameters, but also contributes to economic efficiency by reducing adaptation and testing costs. The goal of standardization is to achieve harmonization and optimization of processes, improve the quality of products and services, ensure safety and environmental friendliness, and facilitate trade in the global market. In the ICT field, this means creating conditions for interoperability of systems, such as software compatibility across platforms, or data protection in accordance with cybersecurity norms. Standardization methods include peer review (committee work), scientific research (data analysis and modeling), consensus decision-making (voting within organizations), and pilot testing (implementation of prototypes). These methods are characterized by their scientific validity, inclusiveness (participation of various parties), and adaptability to technological change, such as the integration of agile approaches in standards development to respond quickly to innovations.

The main outcomes of standardization activities are the creation of normative documents, such as standards, recommendations and technical reports, which become the basis for certification and implementation. In 2025, for example, the outcomes include updated standards such as ISO/IEC/IEEE 32430:2025 for measuring the non-functional size of software, which helps to assess the performance of software. Other outcomes are increased competitiveness (through international recognition), reduced trade barriers and stimulating innovation (for example, standards on AI for ethical use). The characteristics of the outcomes are their practicality (application in real projects), measurability (through quality metrics) and long-term viability (standards serve as a basis for further developments).

The levels of standardization implementation vary in scale: international (global norms, such as ISO/IEC), regional (e.g., European EN standards), national (state DSTU in Ukraine), industry (ICT-specific, such as telecommunications) and enterprise (internal standards of companies). Each level is interconnected: for example, the national level adapts international standards to local needs. The characteristics are

hierarchy (higher levels affect lower ones) and flexibility (possibility of combination, as in hybrid systems for IoT). Normative documents on standardization include laws (e.g., the Law of Ukraine "On Standardization" of 2014 with updates to 2025), technical regulations (for mandatory compliance), standards (DSTU, ISO) and methodological recommendations. They regulate processes from development to application, providing a legal basis. The characteristics are mandatory (for regulations) and detailed (include terms, testing methods).

Types of standards include fundamental (terminology, like ISO/IEC 2382 for IT vocabulary), products (software requirements, like ISO/IEC 25010 for quality), processes (lifecycle, like ISO/IEC 12207), services (IT services, like ISO/IEC 20000) and test methods (testing). Characteristics include specialization (by object) and universality (applicability). The purpose of internal company standards is to optimize processes within the company, ensure quality and innovation. Classification: by function (development, production, control), by object (software, equipment) and by level (corporate, departmental). Characteristics include confidentiality (not public) and adaptability (to business strategy, like Google or Microsoft).

The classification of standards in the field of software is based on features such as object (software as a product or process), level (international, national), purpose (quality, security) and life cycle stage (development, testing). The features of the classification are: functional (requirements definition), non-functional (performance), organizational (management). In 2025, updates, such as for SaMD (software as medical device), emphasize stability and trust. The features are complexity (multi-features) and evolutionary (updates for AI).

"De facto" standards are norms adopted in practice without formal approval (e.g., PDF format from Adobe), while "de jure" are officially recognized by organizations (such as HTTP from IETF). The characteristics of de facto are rapid diffusion through the market, de jure - legal force and stability.

International organizations that develop standards include ISO, IEC and ITU. ISO is an independent organization with a mission to create standards for a better life; structure: general assembly, technical committees (like JTC 1 for IT, developing

standards on AI and information security); focus: from quality to AI, with an annual meeting in Kigali on 6-10 October 2025. IEC focuses on electrical engineering and ICT; structure: technical committees; focus: standards for IoT, AI, energy efficiency, like IEC 62368-1:2023 for the security of ICT equipment. ITU is for telecommunications; structure: sectors like ITU-T (standardization); focus: AI in education, WTDC-25 in Baku on 17-28 November 2025, space sustainability. Characteristics are globality, consensus and a focus on innovation.

National standards development organizations in Ukraine are represented by SE "UkrNDNC" (UkrNDNC) – the leading body recognized at the national and European levels; structure: committees, registries; activities: ISO/IEC adaptation, harmonization with the EU. Other countries: ANSI in the USA, BSI in the UK. Characteristics are local adaptation and cooperation with international. Technical committees for standardization are working groups in organizations, such as TC-20 "Information Technologies" in Ukraine (in the International Center), which develops standards for ICT, including the implementation of European norms. In ISO – JTC 1 for IT; in ITU – study groups in ITU-T. Characteristics are expertise, thematic and contribution to global standards, as in 2025 for AI and green reconstruction.

5.2 Technical regulation and standardization in the field of ICT

Technical regulation and standardization in the field of information and communication technologies (ICT) are the basis for ensuring the security, interoperability and efficiency of digital systems in the context of rapid digitalization. In 2025, when Ukraine continues its integration with the European legal framework in accordance with the Association Agreement with the EU, these processes will take on particular importance, encompassing the regulation of artificial intelligence, cybersecurity and cloud technologies. Technical regulation is not limited to norms alone, but includes a set of measures for the harmonization of standards, conformity assessment and consumer protection, contributing to the development of the ICT sector. It is based on the principles of transparency, non-discrimination and

proportionality, adapted to the dynamics of technologies, where rapid updates, such as the introduction of 5G or IoT, require constant updating of norms. Standardization here becomes a tool for innovation, reducing barriers to the export of ICT products and ensuring the interoperability of systems, from software to telecommunications networks.

Regulatory and legal acts and technical regulations in the field of ICT form the legal framework that regulates the development, implementation and use of technologies, ensuring their security and compliance with international standards. The key acts are the Law of Ukraine "On Information Protection in Information and Communication Systems" dated July 5, 1994 No. 80/94-BP (as amended as of April 20, 2025), which establishes requirements for data protection in networks, including cryptographic methods and incident response. Resolution of the Cabinet of Ministers of Ukraine dated February 21, 2025 No. 205 "Some Issues of Creation, Administration and Ensuring the Functioning of Information Means" defines procedures for state ICT systems, focusing on administration and security. Technical regulations, such as the Technical Regulation on Radio Equipment (approved by Resolution of the Cabinet of Ministers of Ukraine No. 355 of 2017, as amended), regulate the requirements for telecommunications equipment, including electromagnetic compatibility and spectral efficiency. In 2025, regulations harmonized with the EU are relevant, for example, on electronic trust services (according to the eIDAS Regulation) and personal data protection (GDPR-compliant rules in the draft Law No. 8153 on the Protection of Personal Data). The characteristics of these documents are their mandatory nature for critical sectors, their focus on risk management (e.g. in cybersecurity), and their integration with national DSTU standards, such as DSTU ISO/IEC 27035-3:2024 for security incident management. They contribute to digital transformation by reducing the risks of data leaks and ensuring the interoperability of ICT products on the market.

Technical regulation as standardization activities, development and application of technical regulations and conformity assessment activities appear as a comprehensive system aimed at establishing uniform rules for the ICT sector. Standardization here includes the development of norms, such as DSTU EN 301 549:2021 for the

accessibility of ICT products, ensuring inclusion for people with disabilities. The development of technical regulations involves harmonization with European directives, such as RED (Radio Equipment Directive) for radio equipment, with an emphasis on safety and efficiency. The application of regulations is carried out through mandatory or voluntary certification, where bodies accredited by the National Accreditation Agency of Ukraine (NAAU) conduct assessment. Conformity assessment activities include auditing, testing and inspection, for example, for software according to ISO/IEC 12207:2017, with the issuance of declarations or certificates. The characteristics of this regulation are its systematic nature (integration of standards, regulations and assessments), preventiveness (focus on preventing risks such as cyberattacks) and flexibility (adaptation to new technologies, such as AI, according to the draft Open Data Strategy for 2025-2027). It contributes to economic growth by facilitating access to the EU market for ICT companies and increasing consumer confidence.

The analysis of Ukrainian legislation in the field of technical regulation reveals its evolution from post-Soviet norms to European harmonisation, with an emphasis on digitalisation and security in ICT. The main framework was formed after 2014, with reforms to align with the EU acquis, including over 300 technical regulations, of which about 20% are ICT-related (e.g. regulations on low-voltage equipment and EMC for telecommunications). The analysis shows progress in digitalization: the Information Society Development Strategy for 2025-2027 focuses on open data and AI, with legal aspects in draft laws on the digitalization of administrative services. However, challenges include implementation lags (e.g. full harmonization with the NIS2 Directive for cybersecurity is expected by 2026) and a lack of resources for small businesses. The legislation is characterized by its complexity (combination of laws, regulations and standards), innovation orientation (incorporation of AI into regulation) and international interoperability, which facilitates the export of ICT services, but requires increased monitoring, as noted in the 2025 Institute for Democracy and Human Rights analyses.

The Law "On Standardization" of June 5, 2014 No. 1315-VII (as amended on

April 20, 2025) defines the legal framework for standardization in Ukraine, promoting harmonization with international norms. Its main purpose is to create a unified system of standards to improve the quality of products, services and processes, including ICT. The Law consists of sections: I - General provisions (definitions of terms, principles); II - National standardization system (roles of bodies, such as the national standardization body - SE "UkrNDNC"); III - Development, adoption and application of standards (procedures, including ISO/IEC adaptation); IV - Financing and liability; V - International cooperation; VI - Final provisions. A brief overview shows the focus on the voluntariness of standards (except for cases related to regulations), accreditation and the register of standards. The characteristics are its reformability (update for EU integration) and practicality, which facilitates standardization in ICT, such as the adoption of DSTU ISO/IEC 27035-3:2024.

The Laws "On Technical Regulations and Conformity Assessment" dated January 15, 2015 No. 124-VIII (with updates, basis 3153-IX) and "On Accreditation of Conformity Assessment Bodies" dated May 17, 2001 No. 2407-III (with amendments dated March 26, 2025 No. 4328-IX) form the basis for assessment in ICT. The first law defines the principles for the development of regulations and assessment procedures, including modules (A-H) for certification, with an emphasis on a risk-based approach for ICT products. Its aspects: legal framework, authorities (Ministry of Economy, NAAU), procedures (declaration of conformity) and liability. The second law regulates the accreditation of bodies, setting requirements for independence, competence and monitoring, with updates in 2025 for EU harmonisation. Aspects: accreditation principles, register of bodies, appeals. Characteristics are their complementarity, focus on transparency and adaptation to ICT (e.g. accreditation for testing AI systems), which ensures trust in the certification.

5.3 Quality management and quality assurance based on ISO 9000 series standards

Quality management and quality assurance based on the ISO 9000 series of

standards are one of the cornerstones of modern management in the information technology (IT) sector, where rapid innovation and complex systems require a systematic approach to process control. In the context of 2025, when digital transformation is accelerated by artificial intelligence, cloud technologies and cybersecurity, the ISO 9000 series of standards provide a universal framework for organizations that develop software, provide IT services or manage data. These standards not only help minimize risks such as code errors or privacy breaches, but also contribute to increased efficiency, customer satisfaction and competitiveness in the global market. They are based on the principles of continuous improvement, customer focus and a process approach adapted to the dynamics of the IT sector, where projects are often iterative and require flexibility. As of October 2025, the series includes key documents such as ISO 9000:2015 (key terms), ISO 9001:2015 (requirements for quality management systems) and ISO 9004:2018 (guidance for sustainable success), taking into account the preparation for the updated ISO 9001:2026, the Draft International Standard of which was published in August 2025 to take into account modern challenges such as climate change resilience and digital transformation. The ISO 9000 series is a set of standards specifically designed to introduce the basic concepts of quality management, on the basis of which enterprises create and implement effective quality management systems (QMS). Initiated by the International Organization for Standardization (ISO) back in 1987 and constantly updated, this series covers not only the theoretical foundations, but also practical tools for integrating quality into all aspects of an organization's activities. For example, ISO 9000:2015 defines key terms such as "quality" (the degree of conformity to requirements), "quality management" (the coordination of activities to achieve quality objectives), and "continuous improvement" (according to the PDCA principle). Based on these, ISO 9001:2015 establishes requirements for QMS, and ISO 9004:2018 provides guidelines for achieving sustainable success through a focus on stakeholders and risks. In the IT sector, these standards are particularly relevant: they help create QMS for companies developing software, where quality is manifested in the reliability of code, system compatibility, and speed of releases. Based on these standards, an

enterprise can implement processes such as auditing customer requirements, monitoring suppliers (e.g., cloud providers), and analyzing data for improvement, which leads to a 20-30% reduction in defects according to ISO research for 2024-2025. The series is characterized by its universality (applicable to any organization, regardless of size or industry), its focus on processes (rather than products), and its integration with other standards, such as ISO/IEC 20000 for IT services or ISO/IEC 27001 for security. This makes ISO 9000 not just a set of rules, but a strategic tool for building a quality culture, where the implementation of a QMS becomes a competitive advantage, facilitating certification and access to international markets.

The recommendatory nature of the ISO series of standards emphasizes their voluntary nature, which distinguishes them from mandatory technical regulations, emphasizing the internal motivation of organizations to improve. Although ISO 9001:2015 is the basis for certification (confirmation of compliance by independent bodies such as Bureau Veritas or TÜV), the standards themselves are not mandatory: they offer best practices rather than rigid directives. This allows companies to adapt them to their needs - for example, in IT companies, they can be integrated with agile methodologies, where PDCA cycles are applied to sprints to respond quickly to feedback. The recommendatory status stimulates innovation: organizations can experiment with processes such as automated software testing without fear of violating the norm, but with a focus on achieving results, such as increasing customer satisfaction. According to the ISO Survey 2024, more than 1.1 million organizations worldwide are certified to ISO 9001, with a significant proportion in the IT sector, where the guidelines help businesses scale. Characteristics of this nature include flexibility (the possibility of partial implementation), a focus on results (focus on efficiency rather than bureaucracy), and global recognition, which facilitates partnerships. In 2025, with the preparation for ISO 9001:2026, the guidelines are expanded to include topics such as resilience and risk management, making the standards even more adaptable to challenges such as cyber threats in IT. The establishment of ISO 9000 standard requirements for a quality system occurs by defining it as a set of organizational structures, methods, processes and resources

necessary for overall quality management, providing a systematic approach to achieving objectives. ISO 9001:2015 details these requirements in eight principles, including leadership (the role of top management in promoting a quality culture), staff involvement (training and motivation, for example for IT developers), and a process approach (identifying key processes, such as software development or customer support). The quality system here is not an isolated function, but an integrated network: organizational structure (roles, responsibilities, such as quality assurance teams in IT), methodologies (standardized procedures, such as code review according to ISO/IEC 90003:2018), processes (from planning to monitoring, using KPIs such as bug response time) and resources (human, technological, financial, including tools such as Jira or GitHub). These requirements provide overall quality management, where the focus is on preventing defects rather than fixing them, with mechanisms for auditing and corrective action. In the IT sector, this is evident in the certification of companies such as Google or Microsoft, where QMS is integrated with DevOps for continuous improvement. The characteristics are comprehensiveness (covering all aspects of the business), measurability (through metrics such as customer satisfaction scores) and adaptability (to industry specifics, for example, combining with ISO/IEC 12207 for the software life cycle). In 2025, with a view to Draft ISO 9001:2026, the requirements are strengthened to the context of the organization and stakeholders, making the quality system even more strategic for sustainable development in IT.

5.4 Software standardization in the ICT sector

Software (software) standardization is a fundamental aspect of modern information and communication technology (ICT), ensuring not only technical compatibility and reliability, but also cost-effectiveness of development and implementation. In the context of 2025, when digitalization penetrates all areas of life - from artificial intelligence to cybersecurity - software standardization becomes a tool for harmonizing global practices, reducing risks and stimulating innovation. It is based on international standards, such as ISO/IEC 12207:2017 for life cycle processes and

ISO/IEC 25010:2023 for quality models, adapted in Ukraine as DSTU. This process is not limited to technical requirements, but covers economic, organizational and legal aspects, contributing to the creation of open systems and increasing competitiveness. Standardization transforms software from a chaotic product into a structured object, where each stage – from design to operation – is regulated by clear rules, ensuring quality and security in a dynamic digital environment.

Software as an object of development and standardization is characterized by its intangibility, complexity and rapid evolution, which makes them unique compared to traditional products. As an object of development, software includes code, algorithms, interfaces and databases that are created in an iterative process using programming languages, frameworks and tools such as Agile or DevOps. Standardization here is aimed at unifying these elements: for example, ensuring compatibility through APIs (Application Programming Interfaces) or compliance with security requirements according to ISO/IEC 27001:2022. The characteristics of software are its scalability (the ability to adapt to different platforms), modularity (division into independent components) and dependence on the human factor (developers, testers). As an object of standardization, software is subject to norms governing quality (functionality, performance, interoperability according to ISO/IEC 25010:2023), development processes (lifecycle according to ISO/IEC 12207:2017) and documentation. This ensures reproducibility, reduces errors and facilitates certification, making software not just code, but a system integrated into global ICT structures.

The economic features of software development are the high investment intensity in the early stages and the low costs of replication, which distinguishes them from tangible goods. Software development requires significant investments in human resources – developer salaries, training, tools – which can account for up to 70-80% of total costs, according to IEEE 2025 research. Economic efficiency is achieved through scalability: once created, code can be sold to millions of users with minimal additional costs, as in the case of SaaS (Software as a Service) models. However, risks include budget overruns due to changing requirements (scope creep) or errors leading to rework. Standardization here plays an optimization role: compliance with norms such

as ISO/IEC 90003:2018 for applying ISO 9001 to software reduces testing and support costs by 20-30%, contributing to return on investment (ROI) and competitiveness in the market. Economic features also include intellectual property: software is protected by patents and licenses, but open-source models, such as Linux, allow for collaborative development, reducing costs for small businesses.

Estimating the complexity of software development in the context of standardization requirements is critical for resource planning and quality assurance. The complexity is measured in person-months or function points (FP), where each functional element (input, output, queries) is rated for complexity. In a standardized context, according to ISO/IEC 20926:2009 (IFPUG method), documentation, testing, and integration requirements are taken into account, which increases the complexity by 15-25% for certified projects. For example, for medium-sized software (10-50 thousand lines of code), the complexity can be 100-500 person-months, with an emphasis on the analysis and verification stages. Estimation methods like COCOMO II (Constructive Cost Model) integrate standards: risk factors (security, compatibility) multiply the base estimate. The characteristics are subjectivity (dependence on team experience) and dynamism (changes in requirements), but standardization reduces variability, ensuring accurate forecasts and efficient resource allocation in ICT projects.

The challenges and tasks of software design are related to the balance between functionality, performance and usability in a limited resource environment. The main challenges are: the complexity of managing requirements (frequent changes from the customer), ensuring security (vulnerabilities, as in the CVE database 2025), compatibility with different platforms and scalability for big data. The tasks include modeling (using UML according to ISO/IEC 19505), optimization of algorithms and integration with cloud services. In the context of standardization, the problems are exacerbated by the requirements for tracing (tracking compliance with standards), and the task is to create a modular design for easy modification. The characteristics are iterativeness (prototyping to reduce risks) and multidisciplinary (involvement of architects, designers, testers), which makes design a key stage for achieving quality

according to ISO/IEC 25010:2023.

The stages of the software life cycle form a sequential structure from conception to decommissioning, providing a systems approach. According to ISO/IEC 12207:2017, the stages include: acquisition (requirements definition), delivery (development), operation (use), maintenance (upgrade) and disposal. In more detail: requirements analysis, design, coding, testing, implementation, operation and support. The characteristics are cyclicality (feedback at each stage) and adaptability (to agile or waterfall models), which allows you to manage risks and ensure quality in a dynamic ICT environment. The waterfall model of the software life cycle, known as waterfall, is a classic linear model, where the stages are performed sequentially without returns. It includes: requirements gathering, system design, detailed design, coding, testing, integration, implementation and support. Characteristics are rigidity (each stage ends with documentation), predictability (good for stable projects), and a focus on planning, but with drawbacks – low flexibility to change. In standardization, the model is supported by ISO/IEC 12207:2017 for critical systems, where documentation provides traceability, but in 2025 it is often combined with agile for hybrid approaches.

Documentation and its role in ensuring software quality are essential, as it records processes, requirements and solutions, facilitating audit, support and certification. The role of documentation is to reduce errors (through clear specifications), ensure traceability (from requirements to code) and facilitate knowledge transfer. According to ISO/IEC/IEEE 26515:2018, it is integrated into agile, increasing quality according to the principles of "documented development - reliable software". The definition of the types and content of documents involves a classification into system (requirements, architecture), user (manuals) and technical (code, tests). The content includes a description of functionality, interfaces, algorithms and acceptance criteria. The characteristics are structuredness (according to IEEE 829 templates for tests) and relevance, which ensures efficiency.

Development documentation covers the entire cycle: from SRS (Software Requirements Specification) to test plans and release notes. It includes diagrams, code reviews and logs, ensuring transparency and quality control. The requirements of the

standards for software documentation are set out in ISO/IEC/IEEE 15289:2019, where documents must be complete, unambiguous and verifiable. For example, for user documentation – accessibility according to ISO/IEC 26514:2022, for technical documentation – traceability. Characteristics are mandatory for certification and adaptability to methodologies. Special methods for evaluating and examining software and hardware include static analysis (code review), dynamic testing (unit tests) and expert assessments (peer review). Methods such as FMEA (Failure Mode and Effects Analysis) according to ISO/IEC 16085 assess risks, and expertise – compliance with standards through audits. Characteristics are objectivity and comprehensiveness. Standards in the field of software quality assurance, such as ISO/IEC 25010:2023, define models with characteristics (functionality, efficiency, compatibility). Others are ISO/IEC 90003:2018 for software quality, with a focus on metrics and processes. The characteristics are universality and measurability.

The organization of standardization work in the field of ICT and open systems is based on national bodies (UkrNDNC in Ukraine) and international (ISO, IEC), with committees for the development of standards. Open systems are interoperable platforms according to the OSI model (ISO/IEC 7498-1:1994), organized through consortia, such as W3C for web standards. Key areas for creating open information systems include interoperability (APIs, data standards like JSON), openness (open source per OSI), security (crypto standards), and scalability (cloud architectures per ISO/IEC 17788:2014). In 2025, the focus will be on AI integration and IoT, with standards like ISO/IEC 30141:2018, facilitating global collaboration.

5.5 Structure and content of state and international standards in the field of IT tools

In the field of information technology (IT) facilities, the structure and content of national and international standards play a key role in ensuring the interoperability, security and efficiency of systems. These standards form the basis for the development, implementation and certification of IT solutions, from software to network

infrastructure. In the context of 2025, when Ukraine continues to harmonize with European and international norms in accordance with the Association Agreement with the EU, these documents are evolving, integrating new technologies such as artificial intelligence, cloud computing and cybersecurity. They not only establish technical requirements, but also contribute to the standardization of processes, reducing risks and facilitating global integration. The structure of standards is usually unified, including the introduction, scope, regulatory references, terms and definitions, main provisions, test methods and annexes, which makes them convenient for practical use. The content focuses on the principles of quality, security and interoperability, ensuring adaptability to dynamic IT landscapes.

State standards of Ukraine in the field of information technology, known as DSTU (State Standards of Ukraine), are a set of documents that regulate various aspects of IT, from data processing to information protection. Key series include DSTU "Information Processing Systems", "Information Protection" and "Information Technologies", as well as other related standards. For example, DSTU 2229-93 "Information Processing Systems. Local Area Networks" establishes terms and requirements for local area networks, contributing to their standardization. The "Information Protection" series includes DSTU 7624:2014 "Information Technologies. Cryptographic Protection of Information. Cryptographic Algorithms Based on Elliptic Curves", which defines encryption methods to ensure data confidentiality. The "Information Technology" series covers DSTU ISO/IEC 2382-15:2005 "Information Technology. Vocabulary. Part 15: Programming", which provides terminology for software development, and DSTU EN 50600-1:2018 "Information Technology. Infrastructure and Equipment of Data Processing Centers. Part 1. General Requirements", which regulates the construction of data centers. Other standards, such as DSTU 2941-94 "Information Processing Systems. Systems Development. Terms and Definitions" and DSTU 2481-94 "Information Processing Systems. Intelligent Information Technologies. Terms and Definitions", complement this base, focusing on intelligent systems and development. The structure of these standards is standardized: it starts with an introduction and scope (e.g. for local networks or cryptographic

protection), followed by normative references to other DSTU or international standards, terms and definitions (often with English equivalents for harmonization), basic requirements (methods, algorithms, criteria), control and test methods, as well as annexes with examples or tables. The content is oriented towards practical implementation, with an emphasis on compatibility, security and efficiency, often harmonized with ISO/IEC. The general characteristic of these standards is their mandatory nature for state and commercial IT systems in Ukraine, adaptability to national needs (e.g. integration with European regulations), but with some lag behind global updates, which requires regular revisions. They contribute to national standardization, reducing barriers to the export of IT products and ensuring the protection of critical infrastructure.

International standards, adapted in Ukraine as DSTU ISO/IEC, are harmonized documents based on the developments of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Among them is DSTU ISO/IEC 90003:2006 "Software engineering. Guidelines for the application of ISO 9001:2000 to software (ISO/IEC 90003:2004, IDT)", which provides recommendations for integrating quality management systems into software development. The structure of this standard includes an introduction, scope (for organizations that develop or maintain software), normative references (to ISO 9001), terms and definitions (for example, "software product" or "customer requirements"), main sections with process guidelines (planning, development, testing), as well as annexes with examples. The content focuses on adapting quality principles to the software life cycle, with an emphasis on documentation and auditing. The current international version is ISO/IEC/IEEE 90003:2018, but Ukraine maintains 2006 with a reference to an older database that requires updating. Further, DSTU ISO/IEC 18014-2:2015 "Information technology. Security methods. Time stamping services. Part 2. Mechanisms that produce independent tokens (ISO/IEC 18014-2:2009, IDT)" regulates time-stamping mechanisms for digital documents. Its structure: introduction, scope (for security systems), terms (e.g., "stamping token"), requirements for mechanisms (algorithms, protocols), verification methods and applications with

models. The content details independent tokens for protection against forgery, with an emphasis on cryptography. The current ISO/IEC 18014-2:2021 includes an update to hash functions, which may be implemented in Ukraine soon. Finally, DSTU ISO/IEC 8823-1:2009 "Information technology. Open systems interconnection. Connection-oriented presentation layer protocol specification (ISO/IEC 8823-1:1994, IDT)" defines protocols for the OSI model. Structure: introduction, scope (for network systems), terms, abstract notation (ASN.1), protocol specifications, conformance and annexes. The content describes the data presentation layer in networks, ensuring interoperability. The common characteristic of these standards is their global orientation, IDT-harmonization (identical adaptation), focus on technical detail and integration with other ISO/IECs, but with a potential lag in national versions. They are voluntary but recommended for certification, facilitating international trade in IT equipment.

Network standardization and standards for IT architecture encompass a range of international and national documents that provide a framework for the design, implementation and management of complex systems. In the networking field, key standards are the IEEE 802 standards, such as IEEE 802.11 for Wi-Fi (current version 802.11-2020 with updates to 2025), which define the physical and MAC layers for wireless networks, including protocols, security and performance. ISO/IEC 7498-1:1994 (OSI model) and its derivatives, such as ISO/IEC 11801 for wired networks, establish layers of interaction, with an emphasis on interoperability. For IoT, ISO/IEC 30141:2018 "Internet of Things. Reference architecture", which integrates networks with devices. IT architecture is dominated by ISO/IEC/IEEE 42010:2022 "Software, systems and enterprises. Architecture description", which regulates the creation of descriptions of architectures, including views, models and stakeholders. The structure of these standards: introduction, scope (e.g. for networks or enterprises), terms, reference models, requirements and annexes with examples. The content focuses on flexibility, scalability and security, with assessment methods. Characteristics: they are universal, evolutionary (with regular updates), innovation-oriented (as in 5G or edge computing) and integrated (e.g. with ISO/IEC 27001 for security). In Ukraine, these

standards are harmonized as DSTU, contributing to digital transformation, but require adaptation to the national infrastructure to reduce dependence on imports.

5.6 Certification of IT sectors and services. Certification schemes

In the world of information technology (IT), service certification plays a role not just as a formal procedure, but as a real foundation for ensuring quality, reliability and compliance with global standards. It becomes a bridge between service providers and consumers, ensuring that cloud computing, user support or cybersecurity systems not only work effectively, but also meet requirements such as those set out in the ISO/IEC 20000 standard. This standard defines a comprehensive approach to IT service management, covering the stages of planning, implementation, monitoring and continuous improvement. IT service certification thus becomes a tool that not only confirms compliance, but also promotes innovation, reducing risks and increasing trust in the market. Certification as a concept encompasses a procedure during which an independent third party, such as an accredited body, verifies whether a product, process, service or management system meets established standards. In the IT context, this applies not only to technical aspects, but also to quality, security and interoperability. The key elements here are the object of certification – for example, the processes of delivering IT services; the compliance requirements based on standards such as ISO/IEC 27001 for information security; the actors, including the supplier, the certification body and the accreditation body; and the certificate, which becomes documentary evidence of success. This process not only increases competitiveness, but also integrates IT services into global supply chains, contributing to overall trust and stability.

Considering certification as a dynamic process, we see its structure as a sequence of stages, where each step depends on the previous one. Inputs include the supplier's application, complete documentation – from policies and procedures to contracts – as well as relevant standards and resources such as testing personnel and equipment. Outputs are not only a certificate, but also detailed assessment reports,

recommendations for improvement and data for further monitoring. The management mechanisms here are based on the principles of the PDCA (Plan-Do-Check-Act) cycle, adapted from ISO 9001, which allows for risk control, communication and response to change. The provision of resources is critical: from qualified auditors certified according to ISO/IEC 17021, to testing tools such as load simulation software, and even cloud platforms for remote analysis. In the IT sector, this process becomes iterative, allowing for adaptation to rapid technological changes, making certification not a static but a living system.

The certification system is presented as an autonomous structure with its own rules, procedures and governance mechanisms, intended solely for the purpose of confirming conformity. It is based on standards such as ISO/IEC 17000 and ISO/IEC 17021, which define accreditation criteria, appeal procedures and confidentiality. It is managed through accreditation bodies such as the International Accreditation Forum (IAF), which guarantee independence and impartiality. In the IT context, this system integrates with national standards – in Ukraine, for example, with DSTU and the activities of NAAU – and includes elements such as certification bodies (Bureau Veritas or TÜV), testing laboratories and certificate registries. Traceability from application to supervision makes it reliable, and adaptation to dynamic technologies, including cybersecurity and GDPR compliance, underlines its flexibility.

Regardless of the type or object, the certification process consists of universal stages that ensure consistency and consistency. First, the supplier submits an application with a detailed description of the object and documentation, after which the body assesses the feasibility. This is followed by a conformity assessment: from document verification in the first stage to process audits and testing, for example, load tests for IT services, in the second. The analysis of the results involves a detailed analysis of the reports, identifying non-conformities and proposing corrective actions. The certification decision - issuing a certificate or refusing with recommendations - is based on this analysis. Finally, inspection control includes periodic audits, monitoring changes and possible suspension of the certificate, ensuring cyclicality and continuous improvement.

Certification can be mandatory or voluntary, each of which has its own characteristics and motivations. Mandatory, regulated by law, applies to critical IT services related to security - for example, in Ukraine for information protection systems in the public sector under DSTU ISO/IEC 27001. It reduces public risks, as in medical systems, and ensures compliance with technical regulations. Voluntary is initiated by the supplier for marketing benefits, such as ISO/IEC 20000 certification, which increases customer trust and stimulates innovation. In the IT sector, voluntary prevails, as it is market-oriented, while mandatory is regulatory, creating a balance between coercion and freedom.

Certification schemes are sets of rules and procedures adapted to specific objects according to ISO/IEC 17067. In IT services, they vary: scheme 1 focuses on typical services, such as cloud services; scheme 2 on customized batches; scheme 3 on management systems with process audits; scheme 4 on services with continuous inspection; scheme 5 on full assessment with testing and supervision for critical systems, such as banking. These schemes adapt to agile methodologies, integrating automated testing, making certification more efficient in a dynamic environment.

Software certification has unique features due to its intangible nature and rapid evolution. It is based on the ISO/IEC 25010 standards for quality and ISO/IEC 12207 for the life cycle, including testing of functionality, security and compatibility using tools such as static code analysis. However, the problems are numerous: rapid software obsolescence makes the certificate short-lived; the complexity of testing does not allow to cover all scenarios, especially in AI; privacy risks during the audit; high cost for small businesses; and discrepancies in national requirements. The solutions are integration with DevOps and digital certificates that facilitate the process.

Organizing work on certification of information technology facilities - from hardware to networks - requires a systematic approach to ensure reliability. Planning begins with defining the object, for example, servers according to ISO/IEC 19770. Implementation includes auditing, EMC compatibility testing and cybersecurity. Resources include accredited laboratories according to ISO/IEC 17025 and experts, and control is integrated with the quality system. In IT, the emphasis is on

interoperability and scalability. In Ukraine, this is integrated with the national NAAU system and EU standards, contributing to digital transformation and minimizing the risks of failures.

5.7 Regulatory and legal framework for certification of products and services in the ICT sector

In the field of information and communication technologies (ICT), the regulatory framework for product and service certification acts as a fundamental element that ensures the harmonization of standards, consumer protection and Ukraine's integration into the international market. This framework is not a static set of rules, but a dynamic system that evolves in line with technological changes, such as the development of cybersecurity, cloud services and artificial intelligence. It covers the certification of hardware, software, telecommunications services and information security management systems, based on the principles of transparency, independence and compliance with European standards. In the context of 2025, when Ukraine continues to adapt to the EU acquis, this framework becomes a tool for increasing the competitiveness of the ICT sector, reducing risks and stimulating innovation.

The regulatory and legal framework for certification in ICT appears as an extensive hierarchical system of documents that are mandatory and form a single legal framework for confirming the compliance of products and services with established requirements. This system is structured according to the principle of subordination: at the top level - constitutional provisions and international agreements, then - national laws, by-laws, standards and methodological documents. Mandatoryness is ensured by sanctions for non-compliance, such as fines or a ban on product circulation. In the ICT sector, this hierarchy is adapted to the specifics of technologies: for example, it integrates requirements for certification of information security tools, telecommunications equipment and software products, taking into account rapid updates of standards, such as changes to DSTU ISO/IEC 27035-3:2024 on security incident management. The diversity is manifested in the division into general (for all

objects) and specialized (for ICT) documents, which provides flexibility and comprehensive coverage - from conformity assessment to supervision of certified objects.

Ukrainian legislation forms the basis of this system, establishing general principles and requirements for certification in ICT. The key one is the Law of Ukraine "On Standardization" of 2014 (as amended), which defines the procedures for harmonizing national standards with international ones, including ISO/IEC for ICT. Another important act is the Law "On Technical Regulations and Conformity Assessment" of 2015, which regulates mandatory and voluntary certification of products, such as computer equipment or software, with an emphasis on security and interoperability. In the context of cybersecurity, the Law "On Basic Principles for Ensuring Cybersecurity of Ukraine" of 2017 (with updates until 2025) introduces certification schemes for critical ICT infrastructure, including European schemes under EU Regulation 2019/881 (Cybersecurity Act). In addition, the Law "On Electronic Trust Services" of 2017 regulates the certification of electronic signatures and trust services, ensuring their recognition in the EU. These acts are characterized by mandatory nature, orientation towards European integration and control mechanisms, such as accreditation of certification bodies by the National Accreditation Agency of Ukraine (NAAU).

Subsidiary legislation, in particular resolutions of the Cabinet of Ministers of Ukraine, detail legislative norms, making them operational for the ICT sphere. For example, Resolution of the Cabinet of Ministers of Ukraine No. 205 of February 21, 2025 "Some issues of creating, administering and ensuring the functioning of an information technology facility" regulates the certification of information technology systems in the public sector, including data security requirements. Another key regulation is No. 179 of 3 March 2021 (as amended) on the National Economic Strategy until 2030, which integrates the certification of ICT products into the digital economy development plan. The regulations on the list of products subject to mandatory certification (e.g. No. 163 of 2011, as amended) include ICT equipment such as telecommunications devices or software packages for information protection. These

acts are characterized by a practical focus, establishing deadlines, procedures and responsible executors, such as the Ministry of Digital Transformation, and ensuring consistency with European technical regulations.

Fundamental organizational and methodological documents define the requirements for the organization of certification work, serving as a methodological foundation for ICT practitioners. This is, for example, DSTU ISO/IEC 17065:2019 "Requirements for bodies for the certification of products, processes and services", adapted in Ukraine, which establishes criteria for independence, competence and audit procedures. Another document is DSTU ISO/IEC 17021-1:2015 for the certification of management systems, applied to ICT services under ISO/IEC 20000. These documents are mandatory for accredited bodies, defining the stages of certification - from application to inspection control - and the resources required for testing, such as laboratories for testing electromagnetic compatibility. They are characterized by systematicity, a focus on the quality of processes and adaptation to ICT specifics, contributing to the standardization of work and the minimization of errors.

Organizational and methodological documents covering specific homogeneous groups of products and services, executed in the form of rules and procedures, specify procedures for ICT objects. For example, the Procedure for Certification of Information Protection Means, approved by the resolution of the Cabinet of Ministers of Ukraine, regulates the assessment of cybersecurity software. The Rules for Certification of Telecommunications Equipment according to DSTU EN 300, adapted in Ukraine, establish requirements for compatibility and security testing. These documents are mandatory for groups such as network equipment or cloud services, and include detailed audit procedures, sample documentation and compliance criteria. They are characterized by specialization, practicality and market orientation, allowing for the effective certification of homogeneous products such as mobile devices or IoT systems. Classifiers, lists and nomenclatures serve as tools for systematizing certification objects in ICT. The Ukrainian Classifier of Goods for Foreign Economic Activity (UKT FEA) and the State Classifier of Products and Services (DK 016:2010) define codes for ICT products, such as computers (code 8471) or software (code 58).

The lists of products for mandatory certification, updated by the Cabinet of Ministers of Ukraine (CMU) resolutions, include high-risk ICT equipment, such as cryptographic systems. The nomenclatures of standards, for example, from the DSTU catalog, cover the ISO/IEC series for ICT. These documents are characterized by their structure, mandatory registration, and trade facilitation, providing a single nomenclature for conformity assessment.

Recommended documents are optional, but valuable for developing and specifying issues of organizing certification in ICT, offering methods and forms for various procedures in order to increase the efficiency of specialists. For example, the UNBA methodological recommendations on auditing ICT systems according to ISO/IEC 27001 detail tools for risk assessment and process improvement. The recommendations of the Ministry of Digital Transformation on cloud services certification offer agile approaches to testing. These documents are characterized by flexibility, orientation to best practices and a focus on innovation, helping specialists optimize procedures, such as remote auditing or automated testing, without strict sanctions for non-use.

Reference information materials contain extended information on objects registered in the State Register, serving as a source for practitioners and consumers in ICT. These are, for example, the UNBA electronic databases with a register of certified bodies and products, which provide details about certificates for software or telecommunications equipment. Newsletters on updated standards, such as the report on DSTU ISO/IEC 27035-3:2024, provide analysis and examples. These materials are characterized by accessibility (often online), comprehensiveness and support for transparency, helping to find certified facilities, monitor changes and education, without being mandatory, but with high practical value for the sector.

5.8 Information support for standardization and certification in the field of ICT

In the field of standardization and certification of information technology (IT), information security acts as a key element that ensures the accessibility, relevance and

effective use of regulatory documents. It forms the basis for harmonizing processes, from the development of standards to their implementation in practice, contributing to the digital transformation of the Ukrainian economy. In the context of 2025, when Ukraine continues to integrate with European norms, information security becomes a tool to support innovation in the IT sector, including the standardization of software, cybersecurity systems and cloud technologies. This system not only preserves knowledge, but also ensures transparency, protecting intellectual property rights and facilitating the certification of products and services. It is based on the principles of accessibility, confidentiality and constant updating, adapting to rapid changes in technologies such as artificial intelligence and blockchain.

The Main Fund of Regulatory Documents, which is now known as the National Fund of Regulatory Documents, was established in accordance with the Order of the State Committee for Consumer Protection and Standardization of Ukraine dated March 25, 2003 No. 48 "On Approval of the Regulations on the Main Fund of Regulatory Documents". This Order, registered with the Ministry of Justice of Ukraine, establishes the legal basis for the formation and operation of the Fund as a centralized system for collecting and storing regulatory documents. In 2025, the Fund is administered by the State Enterprise "Ukrainian Scientific Research and Training Center for Standardization, Certification and Quality Problems" (SE "UkrNDNC"), which performs the functions of the national standardization body in accordance with the Government's resolutions. The Fund is a hierarchical structure that integrates paper and electronic resources, providing unified access to documents for state bodies, enterprises and specialists. Its creation was motivated by the need to systematize the regulatory framework after the reforms in the field of standardization, and today it covers more than a million documents, including adapted European EN and ISO/IEC standards adapted to Ukrainian realities. The characteristics of the fund are its state status, mandatory updating, and integration with international databases, such as those of the International Organization for Standardization (ISO), which makes it indispensable for IT specialists in certification processes.

The main tasks of the foundation are to ensure comprehensive management of

regulatory documents, which is critical for standardization and certification in IT. First of all, the foundation is engaged in the collection, systematization and storage of documents, including their updating in accordance with changes in legislation, such as the update of DSTU ISO/IEC 27001:2022 for information security management systems. The second task is to provide information services, which includes consultations, search queries and distribution of copies of standards for enterprises that conduct certification of IT services. The third is to monitor and analyze trends in standardization, for example, the integration of norms for artificial intelligence under ISO/IEC 42001:2023, in order to support scientific research and educational programs. In addition, the foundation ensures the protection of intellectual property, preventing unauthorized distribution, and promotes harmonization with the EU, as provided for by the Association Agreement. These tasks are characterized by systematicity, user orientation and integration with digital platforms, such as online catalogs of UkrNDNC, which allow remote access and automated updating, increasing efficiency in a dynamic IT environment.

The types of documents and databases of the fund form its basis, ensuring comprehensive coverage of the areas of standardization and certification. Among the types of documents, national standards (DSTU), harmonized with international ones (ISO, IEC, EN), technical regulations, codes of practice, catalogs and methodological recommendations stand out. In the IT sphere, this includes documents such as DSTU ISO/IEC 20000-1:2018 for service management, DSTU EN 301 549:2021 for the accessibility of ICT products and services, as well as technical specifications for software. The databases of the fund are electronic resources, such as the National Database of Standards on the UkrNDNC website, which contains search engines with filters by code, date and subject, as well as registers of certified bodies and products. Other databases include archives of canceled documents for historical analysis and integrated databases with European systems, such as PERINORM or ISO Online. Their characteristics are their structure, relevance (updated monthly, as in the newsletters for July 2025) and multimedia, with the ability to download PDF versions, which facilitates use in certification audits and the development of IT systems.

Subscription service and provision of services of the fund are aimed at ensuring convenient access for users, making information support a practical tool. Subscription service involves concluding contracts for regular receipt of updates, for example, monthly information packages with new standards and changes, as in the service "Information support on standardization issues" on the website of SE "Ukrmetrteststandart" for 2025. This includes electronic mailing, access to closed sections of databases and priority consultations. The provision of services covers one-time requests: copying of documents, search services, seminars on the interpretation of standards (for example, on ISO/IEC 25010 for software quality) and online access through portals. In 2025, services are digitized, using an electronic signature for authentication and integration with state registers. The features are fee-based (except for government agencies), data confidentiality and customer orientation, with the possibility of customization for IT companies conducting certification, contributing to the effective implementation of standards and reducing the cost of information search.

Information support and ownership of standards are regulated by the Law of Ukraine "On Standardization" dated June 5, 2014 No. 1315-VII (as amended), which establishes the legal framework for the dissemination and protection of regulatory documents. Information support, according to Article 24 of the Law, includes the publication of official texts of standards, the provision of information services through the national fund and ensuring access for all interested parties, with an emphasis on electronic formats for rapid distribution. This includes publication in official publications, online catalogs and bulletins, such as monthly updates for 2025, informing about new DSTU in the IT sphere. The ownership, under Article 25, belongs to the state for national standards, codes of practice and catalogues developed by the national authority, with a prohibition on unauthorized distribution. Enterprises own the rights to their own specifications, but state standards are protected, with the possibility of compensation for damages for infringement. The characteristics are a balance between accessibility (to encourage use) and protection (through licensing and sanctions), which ensures a state monopoly on key documents, contributing to a single policy in IT standardization and integration with the EU.