Information & Security

Published since 1998

M. Pleskach et al.
vol. 45 (2020): 57-76
https://doi.org/10.11610/isij.4504

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

# Standardization in the Field of Cybersecurity and Cyber Protection in Ukraine

***Mariia Pleskach*** [1] (✉), ***Valentyna Pleskach*** [1], ***Andrii Semenchenko*** [2], ***Danylo Myalkovsky*** [3], ***Taras Stanislavsky*** [3]

[1] *Taras Shevchenko National University of Kyiv, Kyiv, Ukraine*
*http://www.univ.kiev.ua/en*

[2] *The Institute of Senior Management of National Academy of Public Administration under the President of Ukraine, Kyiv, Ukraine, http://academy.gov.ua/?lang=eng*

[3] *State Service of Special Communication Administration, Ukraine*
*http://www.dsszzi.gov.ua/dsszzi/control/en/*

ABSTRACT:

This article demonstrates the similarity of approaches to standardization in the field of cybersecurity carried out by international standardization organizations (ISO, ITU, ETSI), leading regional organizations and selected countries. The authors consider necessary that Ukrainian committees of standardization report on the effectiveness of adopted cybersecurity standards. The harmonization of national with the international standards is essential for saving financial resources and time, and ensuring cross-border cooperation. The article considers a number of standardization organizations and approaches and a list of priority international standards of highest priority for improving the Ukrainian system of regulatory and technical documents on cybersecurity.

ARTICLE INFO:

RECEIVED: 17 NOV 2020
REVISED: 28 NOV 2020
ONLINE: 02 DEC 2020

KEYWORDS:

cybersecurity, cyber protection, standardization organizations, cybersecurity standards

✉ E-mail: pleskachmarija@gmail.com

## Introduction

The main issue of normative-technical and normative-legal support of cybersecurity and cyber protection consist in the imbalance of the development of the national standardization system in Ukraine in this area with the needs of national security, sustainable development of digital economy and society, international obligations and requirements. It is characterized by incompleteness, vagueness, inconsistency with relevant international standards, which highlights the need for separate research on these issues.

It has been shown that there is an urgent need to establish an entity on cybersecurity standardization in Ukraine.

## Methods

There are certain scientific methods used in this paper, such as analysis to find out the current situation of cybersecurity standardization in Ukraine. Also, authors used statistical method for adopting of ND TPI in dynamic. Comparison method was used for comparison the list of Ukrainian and international standards and standardization organizations in cybersecurity sphere.

### *Basic Material*

Incompleteness, vagueness of national standardization system in Ukraine, its inconsistency with international systems of standardization, and disregard of the best international experience is an urgent issue. This problem hinders national standardization system in Ukraine development. Solving of this problem could help to implement the relevant international experience in Ukraine.

European and North Atlantic vector of Ukraine's foreign policy, defined in a number of its national legislative acts of conceptual and strategic level, including the Law of Ukraine “On Basic Principles of Cybersecurity in Ukraine"[1], the Constitution of Ukraine,”[2] and international agreements.

On the other hand, these are significant shortcomings that are inherent in today's standardization in Ukraine in the cybersecurity sphere and cyber protection and hinder successful and secure activities in cyberspace, effective development of digital economy and society.

All this together necessitates the analysis and generalization of the best international experience on these issues in order to generalize it and further use in the formation and implementation of state policy of cybersecurity and cyber protection, improving the national standardization system in this area.

Despite the adopted laws “On National Security of Ukraine” and “On Basic Principles of Cybersecurity in Ukraine,” the problem of further development and adoption of such legislation as the laws “On Critical Infrastructure and its

[1] “On Basic Principles of Cybersecurity in Ukraine,” Law of Ukraine, 2017, https://zakon.rada.gov.ua/laws/show/2163-19.

[2] “The Constitution of Ukraine,” 1996, https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80=.

Protection," "On Security of Information and Information and Communication Systems" is actual, as well as a number of bylaws, including normative and normative-legal documents (standards, codes of established practice, technical regulations, etc.).

The Law of Ukraine "On Standardization" (hereinafter – the Law) defines a number of terms, including the term 'standardization' is an activity that consists in establishing provisions for general and repeated use of existing or potential tasks and is aimed at achieving an optimal degree of order in a certain sphere, the scope of the law, subjects and objects of standardization, its levels (international, regional and national) and the procedure for development and approval of national standards on the basis of (international and regional standards), etc.[3]

Article 17 of the Law states that national standards, codes of practice and amendments to them are developed on the basis of: international and regional standards; standards of the states which are members of the corresponding international or regional organizations of standardization and with which the corresponding international agreements of Ukraine on cooperation and carrying out of works in the sphere of standardization are concluded; scientific achievements, knowledge and practice.[4]

Each of the above approaches has its advantages and disadvantages. Thus, since Ukraine's independence in the field of cybersecurity and cyber protection, given its specifics, standards developed during the Soviet Union with their slight adaptation to new conditions have been used for a long time, as well as an approach based on the introduction of national cryptography school standards and domestic scientific achievements, knowledge and practice.

However, the cyber security standards of the 1990s and 2000s do not meet the needs of today, they must be superseded by modern models of the creation and maintaining cyber security, developed on the basis of modern international standards.

At the same time, approaches focused on the development of national standards based on international and regional standards; standards of states that are members of relevant international or regional standardization organizations, allow not only to save resources but also to ensure interoperability and are essential for the development of the national standardization system, given the real situation in which Ukraine is in this area.

Currently, if international standards are not taken as a basis for a national standard, code of practice and amendments to them, the national standardization body provides a written explanation at the request of the interested party,

[3] "On Standardization: The Law of Ukraine," 2014, https://zakon.rada.gov.ua/laws/show/1315-18#Text.

[4] Ibid.

and if the European standard is adopted, the identity of the national standard is ensured.[5]

In order for an international standard to receive the status of a national standard in Ukraine, special permission of the relevant standardization bodies that adopted this standard earlier is required. Among international standardization organizations, the leading role in the field of cybersecurity and cyber protection is played, first of all:

- International Organization for Standardization / International Electrotechnical Commission (ISO / IEC) is a non-governmental international organization;
- International Telecommunication Unit (ITU) - an international intergovernmental organization in the sphere of telecommunication standardization.[6]

At the regional level of standardization in the field of cyber security and cyber protection, based on the priorities of Ukraine's foreign policy, the experience of the European Institute of Standards and Technology (ETSI) is of the greatest interest with European Committee for Standardization.

It is also extremely important for Ukraine to analyze and summarize the experience of one of the world's leading organization in the field of cybersecurity and cyber protection – National Institute of Standards and Technology (NIST).[7]

### *International Organization for Standardization (ISO)*

ISO/IEC JTC 1 / SC 27 "Information security, cybersecurity and privacy protection" - Joint Technical Committee 1, subcommittee 27 *Information security, cybersecurity and privacy protection* deals with standardization issues.[8]

The purpose of the committee's activities, according to the information posted on its website (https://www.iso.org/committee/45306.html), is to develop standards for the protection of information and ICT. This includes general methods, techniques and guidelines for addressing both security and confidentiality aspects, such as:

- methodology assembly of security requirements; information security and ICT security management;
- in particular information security management systems, security processes, as well as security control and management; cryptographic and

[5] Ibid.

[6] "ITU-T Recommendations by series," 2020, https://www.itu.int/itu-t/recommendations/index.aspx?ser=X.

[7] National Institute of Standards and Technology, "National Bureau of Standards. NBS," NBSIR 79-1776R, 1979, www.nist.gov/pml/weights-and-measures/national-bureau-standards-publications-nbs.

[8] "ISO/IEC JTC 1/SC 27: Information security, cybersecurity and privacy protection," 2020, https://www.iso.org/committee/45306.html.

other protection mechanisms, including, but not limited to, mechanisms for protecting the accountability, availability, integrity and confidentiality of information;

- security management support documentation, including terminology, guidelines, and procedures for registering security components;
- security management aspects of identity management, biometrics and confidentiality; requirements for conformity assessment, accreditation and audit in the sphere of information security management systems; safety assessment criteria and methodology.

The main standards of this committee are:

- ISO / IEC 27000 series, which relate to information security management systems, their creation, evaluation, testing, modernization, etc.);
- ISO / IEC 15408 (Common Criteria's) and 18045 Evaluation criteria for IT security (Information Technology Security Assessment Methodology);
- ISO / IEC 20897 Security requirements and test methods for physically unclonable functions for generating non-stored security parameters (Security requirements and methods for testing physically non-cloned security parameters for continuous generation of security parameters);

and a set of standards for the applicability of requirements and parameters of cybersecurity in production and their interrelation.

### *International Telecommunication Union (ITU)*

In general, the ITU focuses on the following areas of standardization in the field of cybersecurity: national strategies; national CIRTs; Global Cyber Security Index; cyber training; global partnership; information on cyber security; fighting spam.

The ITU usually uses several types of documents, one of the main is recommendation. All recommendations are grouped by thematic areas[9]:

- X.800-X.849: Security (security of open networks, security when using the services of a third party); Supplement on security baseline for network operators;
- X.1000-X.1099: Information and network security (network security and security management);
- X.1100-X.1199: Secure programs and services (security of home and mobile networks, web, security protocols, security of Internet television);
- X.1200-X.1299: Cyberspace protection (cybersecurity review, anti-spam (13 standards) and identification management (13 standards);
- X.1300-X.1499: Secure programs and services;

[9] "ITU-T Recommendations by series".

- X.1500-X.1599: Exchange of information on cybersecurity;
- X.1600-X.1699: Security of cloud computing;
- X.1700-X.1729: Quantum communication.

The recommendations of the following series correspond to the direction of cyberspace and cybersecurity: X.1200-X.1299 Cyberspace security and X.1200-X.1229 Cybersecurity, as well as the series - X.1500-X.1599 Cybersecurity information exchange, which includes a review of cybersecurity, exchange of statements about vulnerability, exchange of information about events / incidents / heuristic analysis, exchange of policies, requests for information / heuristic analysis, identification, secure exchange.

It should also be noted the existence of the X.1600-X.1699 series on the security of cloud computing and X.1700-X.1729 quantum communications.

Having focused in more detail on the series on cybersecurity, it is advisable to cite the following accepted standards:[10]

- X.1205: Cybersecurity Review;
- X.1206: Vendor-neutral structure for automatic notification of security information and distribution of updates;
- X.1207: Guidance for telecommunications service providers on overcoming the risk of spyware and potentially unwanted software;
- X.1208: Cybersecurity indicator to increase the level of confidence and security in the use of telecommunications / information and communication technologies;
- X.1209: Opportunities and their contextual scenarios for information exchange and cybersecurity information exchange;
- X.1210: Overview of source fault protection mechanisms for Internet-based networks;
- X.1211: Methods of preventing web attacks;
- X.1212: Design considerations to improve user perception of reliability indicators;
- X.1213: Security requirements for counteracting botnets based on smartphones;
- X.1214: Security assessment methods in telecommunication / information and communication networks;
- X.1215: Cases of use for structured expression of threat information.

### *European Institute of Standards and Technology (ETSI)*

At ETSI, Technical Committee (TC) CYBER (Cybersecurity) is responsible for standardization issues. According to the information published on the website of this organization (https://www.etsi.org/cyber-security/tc-cyber-roadmap),

[10] For details see https://www.itu.int/itu-t/recommendations/index.aspx?ser=X.

the activity of this committee is directed to the following main areas: understanding the cybersecurity ecosystem, security and privacy on the Internet of Things (IoT), cybersecurity of critical national infrastructures, protection of personal data and communications, corporate and individual cybersecurity, cybersecurity tools, support for EU legislation, forensics and quantum secure cryptography, etc. (Figure 1).

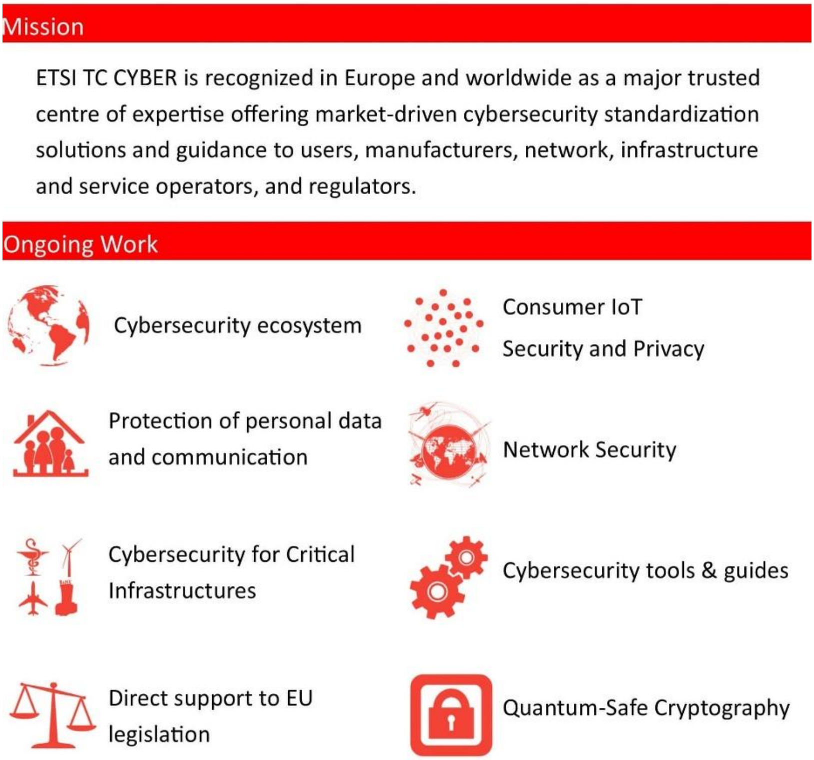
The main results of committee's activity in areas directly related to cybersecurity are:

- development of a technical report on the global cybersecurity ecosystem (TR 103 306) to identify and compile lists of global cybersecurity components;
- TS 103 532 focuses on attribute-based encryption to control access to data, the purpose of which is to protect the identity of the user, preventing the disclosure of data to an outsider;
- TS 103 486 describes how devices can be detected pseudonymically and forms a trust mechanism;
- TR 103 370 focuses on technical standards that can be used to protect data under the GDPR,[11] which focuses on personal information;
- TS 103 645 – the first international standard for IoT consumers was adopted by TC CYBER in 2019. "Cybersecurity in the Internet of Things" is a technical specification that describes the introduction of security of IoT products;
- TS 103 645 maintains a basic level of security for consumer goods connected to the Internet, providing a set of 13 recommendations, including the storage of security-sensitive data, including cryptographic keys, and encryption when transmitting such sensitive data at a level consistent with technology and its use (items 4.4 and 4.5);
- TS 103 458 describes the high level of attribute-based encryption (ABE). It defines the protection of personal data on IoT, WLAN, cloud and mobile services, where secure access to data must be provided by several parties, depending on who that party is;
- TR 103 303 defines 'critical infrastructure' – any infrastructure, the loss or disruption of which, in whole or in part, will have a significant negative impact on one or more economic actions of the parties concerned, the safety, security or health of the population. Examples include power plants, drinking water, hospitals and railways etc.;
- TR 103 303 considers the roles and follow-up of critical infrastructure protection, where critical infrastructure consists in whole or in part of technologies that use cybersecurity mechanisms. As a result, measures

[11] "General Data Protection Regulation," 2016, https://gdpr-info.eu/.

and processes for critical infrastructure protection (CI) are identified and appropriate mechanisms to be implemented are identified;

- TS 103 457 solves the problem when organizations want to protect customer data using a cloud that is not under their direct control. TS 103 457 standardizes the interface between a trusted "secure repository" and a cloud, which can be anywhere where such sensitive data is stored in the repository. In this case, the use of cryptographic mechanisms is given attention due to the requirements for the generation, use and secure storage of cryptographic keys for encryption and signing (paragraph 5.4);
- TR 103 456 – guidance on the implementation of the NIS Directive, paying due attention to the use of cryptographic methods in establishing secure connections, considering them as a new technology related to the provision of relevant services and the operation of related services (paragraph 7.2, 7.3 and 8.1).



Mission

ETSI TC CYBER is recognized in Europe and worldwide as a major trusted centre of expertise offering market-driven cybersecurity standardization solutions and guidance to users, manufacturers, network, infrastructure and service operators, and regulators.

Ongoing Work

Cybersecurity ecosystem

Consumer IoT Security and Privacy

Protection of personal data and communication

Network Security

Cybersecurity for Critical Infrastructures

Cybersecurity tools & guides

Direct support to EU legislation

Quantum-Safe Cryptography

**Figure 1: Roadmap of the ETSI Cyber Security Technical Committee [**https://www.etsi.org/technologies/cyber-security**].**

### *European Committee for Standardization*

The European Committee for Standardization unites the National Standardization Bodies (NSBs) of the 27 European Union countries, United Kingdom, the Republic of North Macedonia, Serbia and Turkey plus three countries of the European Free Trade Association – Iceland, Norway and Switzerland.[12] A National Standardization Body is the one-stop-shop for all stakeholders and is the main focal point of access to the concerted system, which comprises regional (European) and international (ISO) standardization. It is the responsibility of the CEN National Members to implement European Standards as national standards. The National Standardization Bodies distribute and sell the implemented European Standard and have to withdraw any conflicting national standards.

However, CEN's cybersecurity activity result is:

- CEN/TC 301 EN ISO 15118-1:2019 (WI=00301047) Road vehicles – Vehi¬cle to grid communication interface – Part 1: General information and use-case definition (ISO 15118-1:2019) and CEN/TC 151 EN ISO 19014-4:2020 (WI=00151458) Earth-moving machinery – Functional safety – Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system (ISO 19014-4:2020). Both of these standards were published.
- CEN/CLC/JTC 13 prEN ISO/IEC 27007 (WI=JT013034) Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing (ISO/IEC 27007:2020) and CEN/CLC/JTC 13 prEN XXXXX (WI=JT013029) Cybersecurity evaluation methodology for ICT products are under drafting.

### *National Institute of Standards and Technology (NIST)*

The National Institute of Standards and Technology (NIST) is a non-governmental non-profit organization that coordinates voluntary standardization work in the private sector of the economy, manages the activities of standards development organizations and decides to grant the standard national status (if different firms are interested).

NIST (according to Wikipedia), as a rule, does not develop standards, but is the only organization in the United States that adopts (approves) national (federal) standards. This corresponds to the main task of NIST – to help solve problems of national importance (energy savings, environmental protection, safety of human life and working conditions).

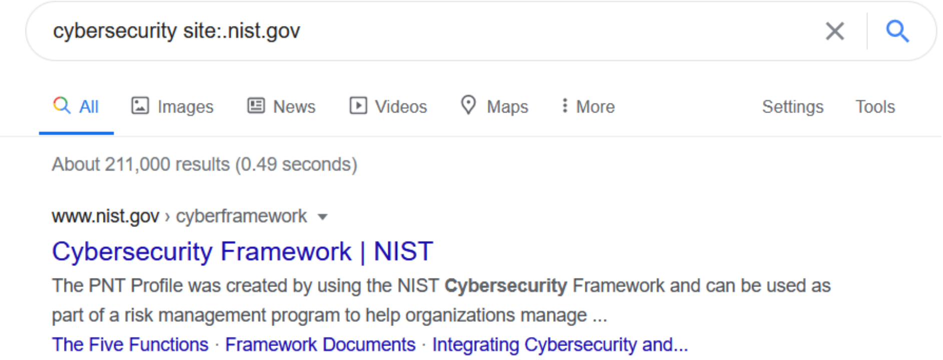
Standards are developed by organizations that have been accredited by the American National Standards Institute (more than 400 firms and organizations). The most famous of them: the American Society for Testing and Materials (ASTM International); American Society for Quality Control (ASQC); American Society of Mechanical Engineers (ASME); Society of Automotive Engineers (SAE International), Institute of Electrical and Electronics Engineers (IEEE), etc.

[12] See https://standards.cen.eu/dyn/www/f?p=CENWEB:5.

NIST can develop a Federal Information Processing Standard (FIPS) in the cases provided by statute and / or there are compelling federal government requirements for cybersecurity. FIPS publications are issued by NIST after approval by the Minister of Trade in accordance with Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987. In addition, take into account the provisions of the Federal Law "Cyber Security Research and Development Act" (2002, as amended in 2020).[13]

Cybersecurity activities include: Computer Security Resource Center, Purely Cybersecurity, Privacy, Risk Management, Cybersecurity Data Blog, National Cybersecurity Centre, National Cybersecurity Education Initiative (NICE).

Thousands of NIST publications refer to cybersecurity (Figure 2), which confirms the considerable attention paid to the standardization of cybersecurity issues.


cybersecurity site:.nist.gov

About 211,000 results (0.49 seconds)

www.nist.gov › cyberframework

Cybersecurity Framework | NIST

The PNT Profile was created by using the NIST **Cybersecurity** Framework and can be used as part of a risk management program to help organizations manage ...

The Five Functions · Framework Documents · Integrating Cybersecurity and...

**Figure 2. Screenshot with search results for cybersecurity publications**

The main series of publications on information security and information systems (including distributed) are special FIPS 800 publications.

Publications in the NIST (SP) 800 series [14] represent information of interest to the computer community. The series contains NIST guidelines, recommendations, specifications, and annual cybersecurity activity reports.

SP 800 publications are designed to meet the security and confidentiality needs of the information and information systems of the US Federal Government. NIST develops SP 800 publications in accordance with its statutory responsibilities under the Federal Information Security Modernization Act

[13] "Cyber security research and development act," 2002, https://www.congress.gov/107/plaws/publ305/PLAW-107publ305.pdf.

[14] Available at https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information.

(FISMA) of 2014.[15]

Created in 1990, the series reports on the research, guidelines of the Information Technology Laboratory and advocacy efforts in the field of computer security and its joint activities with industry, government and academic organizations.

It should be noted that according to information about publications,[16] their number is more than 180 items.

It is also important to highlight the practices of using such publications, which allows us to assess both the effectiveness and methods of application of these publications. One of the latest publications is the March 2020 report, Approaches to Using the Cyber Security Framework for Federal Authorities.

This research highlights different ways of organizing cybersecurity, but all of them are based on the basic approach of risk management and reporting on its effectiveness at the cross-organizational level (Figure 3).

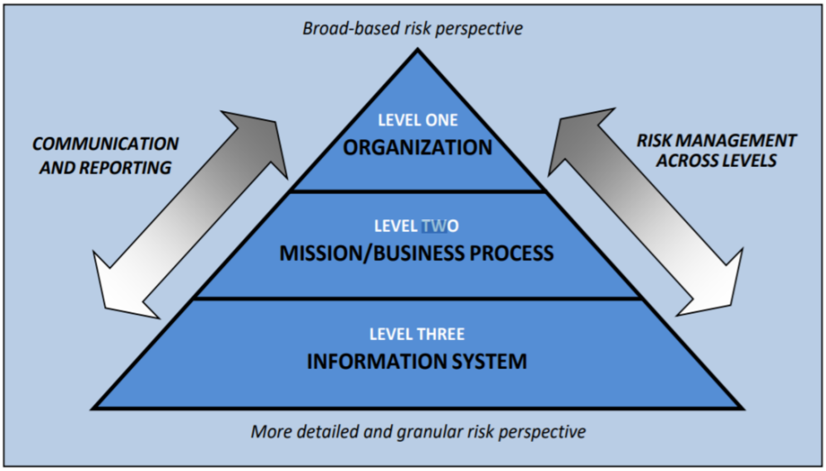

Broad-based risk perspective
COMMUNICATION AND REPORTING
RISK MANAGEMENT ACROSS LEVELS
LEVEL ONE
ORGANIZATION
LEVEL TWO
MISSION/BUSINESS PROCESS
LEVEL THREE
INFORMATION SYSTEM
More detailed and granular risk perspective

**Figure 3. Cross-organizational approach to risk management [NIST IR 8170 [17]]**

The main publications cited in this information report are NIST SP 800-37 Rev. 2 “Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy,”[18] NIST SP 800-53 “Security

[15] “Federal Information Security Modernization Act,” 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2521/text.

[16] See https://csrc.nist.gov/publications/sp800.

[17] Matt Barrett, Jeff Marron, Victoria Yan Pillitteri, Jon Boyens, Stephen Quinn, Greg Witte, and Larry Feldman, “Approaches for Federal Agencies to Use the Cybersecurity Framework,” NIST, NISTIR 8170, March 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf.

[18] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

and Privacy Control for Federal Information Systems and Organizations,"[19] Publications 199 and 200.

Another major activity of NIST is the publication of FIPS information processing standards (https://www.nist.gov/itl/current-fips). The following FIPS standards are currently in force: 140-2 - Security requirements for cryptographic modules); 180-4 – secure hash standard (SHS); 186-4 – Digital Signature Standard (DSS); 197 – Advanced Encryption Standard (AES); 198-1 – Hash key authentication code (HMAC); 199 – Standards for categorization of security of Federal information and information systems (2004); 200 – Minimum Security Requirements for Federal Information Systems (2006); 201-2 – Confirmation of Personal Identity (PIV) of Federal Employees and Contractors (2013); 202 – SHA-3 standard: hash function based on permutation and extension-output (2015).

## *Cybersecurity Standardization in Ukraine*

In general, technical regulation in Ukraine is realized in accordance with the Law of Ukraine "On Standardization."[20] The new version of this Law will come into force in December 2020/ This version is more adapted to European and international legislation in this area. This Law defines the infrastructure and procedure for the development, revision and adoption of national standards, as well as the powers of standardization entities, in particular the national standardization body. The national standardization body adopts, repeals or restores national standards, as well as coordinates the activities of technical standardization committees.

According to the website of the National Standardization Body (SE UkrNDNC, http://uas.org.ua/ua),[21] the condition of standardization in the cybersecurity sphere in Ukraine is characterized by a number of such major problems as:

- miss of technical committee for standardization in the cybersecurity area, but since 1992 TC-20 "Information Technologies" has been functioning and since 1995 TC-107 "Technical protection of information" has been functioning;
- annual programs of work on national standardization for 2020 [22] and previous years of development or adoption national standards in the field of cybersecurity are not provided;
- TC-20 and TC-107 in cybersecurity sphere don't carry out standardization activity in cybersecurity sphere.

[19] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[20] "On standardization: The law of Ukraine."

[21] Ukrainian Research and Training Center of Standardization, Certification and Quality, 2020, http://uas.org.ua/ua/.

[22] http://uas.org.ua/wp-content/uploads/2020/02/nakaz-38-21.02.2020-Programa-2020.pdf.

Thus, the following main conclusions can be made about the condition of standardization cybersecurity sphere in Ukraine and the prospects for its development based on the study and generalization of best international experience:

- there are no standardization entities in Ukraine today that have coordinated activity of interested legal entities and private persons (stakeholders) for the purpose of organizing and performing work on international, regional, and national standardization in the field of cybersecurity;
- there is no systematic funding for standardization activity in the cybersecurity sphere and cyber protection in Ukraine;
- there are no normative documents (standards) that would set comprehensive requirements for products, rules, procedures and processes, as well as formally defined requirements for entities in the field of cybersecurity in Ukraine;
- this direction of state policy can be ensured through the implementation of effective public-private partnership in Ukraine, development and implementation of the concept and strategy of standardization in the cybersecurity sphere.

Other TCs, such as TC-20 Information Technology, which is a member of Subcommittee 27 of the Joint Standards Committee of the International Organization for Standardization (SC 27 JTC 1 ISO) and which ensures the adoption of a number of national standards in the spheres of cryptographic information protection, harmonizes national standards with international standards in the field of electronic signature, international cryptographic algorithms, information security management, etc.

However, it is necessary to establish a TC on the standardization of cybersecurity. The results of international standardization are characterized by a large number of standards and recommendations in cybersecurity sphere and information security, the availability of reports on the effectiveness of their application, which are not prepared in accordance with domestic law.

In addition, the lack of a strategy, concept and program for cybersecurity standardization in Ukraine will lead to unsystematic research on these issues, chaos in decision-making on cybersecurity standards.

The State Service of Special Communications and Information Protection of Ukraine (SSSCIP) is a state body that is designed to provide, cyber protection, telecommunications, use of radio frequency resources of Ukraine, etc. SSSCIP focuses on ensuring the national security of Ukraine from external and internal threats and is part of the security and protection sector of Ukraine. One of the main tasks of SSSCIP is the formation and implementation of state policy in the areas of cryptographic and technical protection of information,[23] cybersecurity, etc., countering technical intelligence, operation, security and development of the state system of government communication, electronic identification (using electronic trust services), electronic trust services [24] (in terms of establishing requirements for security and protection of information during the provision and use of electronic trust services, monitoring compliance with legislation in the field of electronic trust services); ensuring in the prescribed manner and within the competence of the activities of entities that directly carry out the fight against terrorism, etc. An important step towards the modernization of security standards should be considered the introduction in 2015-2016 of normative document of technical protection of information (## 2.6-002-2015, 2.6-003-2015, 2.7-013-2016), which defines the procedure for comparing the functional components of security, components of trust to security, as well as the results of evaluation of means of protection of information against unauthorized access, defined by ISO / IEC 15408, with the requirements of normative document of technical protection of information (RD TPI) 2.5-004-99 "Criteria for assessing the security of information in computer systems from unauthorized access."[25]

Standardization of the procedure for elaboration, adoption, revision and cancellation of interdepartmental normative documents of the technical information protection system was first carried out by the Resolution of the Cabinet of Ministers of Ukraine of June 26, 1996 # 677, for the implementation of which the provision was developed by SSSCIP RD TPI 1.6-002-03 "Rules for the construction, presentation, design and designation of regulations of the system of technical protection of information and which was mandatory for any entities whose activities are related to technical protection of information." Then, in 1996-1997, the SSSCIP developed and adopted three parts of the national standard DSTU 3396: Information protection. Technical protection of information (Basic provisions. Procedure. Terms and definitions.).

Then the dynamics of development of normative and technical documents of the Technical protection of information [TPI] system of non-secret content can be presented as follows: 1999 - 12; 2000 - 3; 2001 - 7; 2002 - 1; 2003 - 2; 2004 - 1; 2005 - 1; 2007 - 4; 2008 - 2; 2009 - 2; 2011 - 1; 2012 - 2; 2013 - 1; 2015 - 2; 2016 - 1; from 2017 - now - 0.

[23] "On Protection of Information in Information and Telecommunication Systems," The law of Ukraine, 1994, https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

[24] "On electronic trust services," The law of Ukraine, 2017, https://zakon.rada.gov.ua/laws/show/2155-19#Text.

[25] "RD TPI 2.5-004-99: Kryterii otsinky zakhyshchenosti informatsii v komp'iuternykh systemakh vid nesanktsionovanoho dostupu" [2.5-004-99 "Criteria for assessing the security of information in computer systems from unauthorized access"], Ukrainian Government, 2018, http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342.

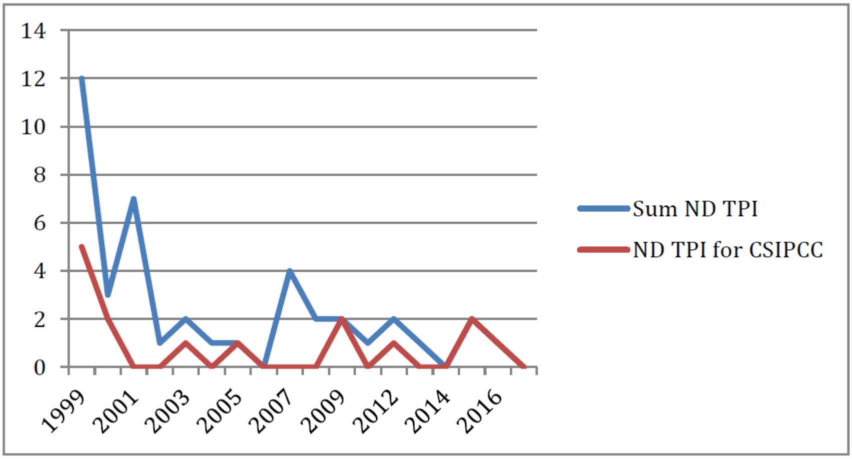


**Figure 4. Adopting of ND TPI in dynamic (1999-2019).**

Regarding the most applicable organizational and technical mechanism - a comprehensive system of information protection with confirmed compliance (CSIPCC), which is defined by the Law of Ukraine “On Information Protection in Information and Telecommunication Systems,”[26] the dynamics of 15 ND TPI by year can be represented as: 1999 - 5; 2000 - 2; 2003 - 1; 2005 -1; 2009 - 2; 2011 - 1; 2015 - 2; 2016 - 1.

In 1999-2005, attention in the development of regulatory and technical documents was mainly focused on the definition of security services, ways to describe them in the terms of reference when creating a protection system. Subsequently, the emphasis shifted to determining the methods and procedures for assessing security services in the newly created security systems.

In 2015-2016, normative documents were adopted (ND TPI 2.6-002-2015, ND TPI 2.6-003-2015, ND TPI 2.7-013-2016), which emphasize the compliance of the approach introduced in our country in 1999 with the provisions of the international standard on information technology (IT) security requirements ISO / IEC 15408.

The increase the number of adopted national standards, harmonized with international ones, is mainly due to the periodic need for regulatory and technical support of certain legislative initiatives. This is confirmed by the adoption of a number of cryptographic international standards at the stage of Ukraine's accession to the World Trade Organization (2005-2007) and the adoption and implementation of the Laws of Ukraine “On Electronic Digital Signature” (2004-2009). Further implementation of the European regulation on electronic identification and electronic trust services eIDAS through the adoption of the Law of

[26] “On Protection of Information in Information and Telecommunication Systems.”

Ukraine "On electronic trust services"[27] led to the establishment of requirements for their use through the approval of the Cabinet of Ministers of Ukraine "Requirements in electronic trust services." It is worth noting that they include information security standards: in particular, ISO / IEC 15408, and Information Security Management System (ISMS): ISO / IEC 27 001 (requirements), 27002 (Code of Practice for Measures) and 27005 (information security risk management).

The adoption of the Law of Ukraine "On Basic Principles of Cybersecurity in Ukraine" did not lead to the intensification of the systematic development of national standards in the cybersecurity sphere. After this, some ISMS standards were adopted or revised in Ukraine. These are eight standards that base on: ISO/IEC 27000:2018, ISO/IEC 27001:2013/Cor 2:2015, ISO/IEC 27002:2013/Cor 2:2015, ISO/IEC 27005:2018, ISO/IEC TS 27008:2019, ISO/IEC 27011:2016/Cor 1:2018, ISO/IEC 27018:2019, ISO/IEC TS 27034-5-1:2018.

In connection with the development of standardization in the sphere of information security, information security management systems [28] and risk management, the task of further revision of current regulations in order to modernize (transform) mechanisms for building information security systems and their operation in accordance with information security management standard series ISO/IEC 27000, 31000, conformity assessment taking into account the best practices of international law.

It is also important that the implementation of international standards in the cybersecurity sphere will take into account not only national state or public interests, but also individual. After all, in practice, the interests of different structural elements (levels) of cyber security (person, society and state) may not be consistent with each other.

Given this, it is necessary to define clear criteria and principles for distinguishing public (state, society) and private (person) interests in cyberspace, in order to eliminate the problem of complete or partial mismatch of interests at different levels (person, society, state).

For example, state law enforcement and intelligence agencies may be interested in monitoring, covert surveillance, and monitoring of its citizens and society to ensure public order, so the state is somewhat favorable to the insecurity of Internet protocols for collecting data on individuals.

But a person is interested in ensuring that his rights, including during the use of cyberspace, are not violated by the state, because according to Part 2 of Art.

[27] "On Electronic Trust Services."

[28] Valentyna Pleskach, Mariia Pleskachand Olena Zelikovska, "Information Security Management System in Distributed Information Systems," *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine*, 2019, pp. 300-303, https://doi.org/10.1109/ATIT49449.2019.9030484.

3 of the Constitution of Ukraine,[29] the state is responsible to person for his activities, and the main duty of the state is to establish and ensure human rights and freedoms. By not providing an effective mechanism for the cyber security of persons, the state puts society as a whole at risk. So, the purpose of the state is to create appropriate conditions for the realization of human rights and freedoms.

Therefore, it is important to develop standards for cyber security not only for public administration entities (those that defend primarily the public interest), but also for those entities that defend the private interest, for business entities, citizens of Ukraine and their associations, other persons carrying out activities and / or providing services related to national information resources, electronic information services, electronic transactions, electronic communications, information security and cyber security.

Another area for improving the national standardization system in the cybersecurity sphere could be the introduction of a national rating of enterprises, institutions, organizations that implement international cybersecurity standards and are ready and able to maintain them throughout their activities.

This area of activity of authorized entities could also help to achieve the appropriate level of culture of relations in Ukraine, including information, to establish an institution of reputation in Ukraine, which is very valuable in European countries, but, unfortunately, is not very developed in Ukraine. And to speed up the implementation of this mechanism, it would also be appropriate to apply certain benefits to such entities, or to determine the procedure for full or partial compensation for training services provided by employees of such enterprises, institutions, organizations to improve knowledge in cybersecurity and more.

## Conclusions

This article demonstrates the similarity of the standardization directions in the cybersecurity sphere carried out by international organizations (ISO, ITU) and regional organizations (ETSI, CEN) for standardization, NIST USA, including the periodic publication of practices for the application of these standards. In Ukraine, we see an almost complete absence of cybersecurity standardization processes, so it is necessary to establish a new technical committee for standardization in this area, which would ensure systematic development, including through harmonization of national cybersecurity standards with international ones, their adoption, and regular review and updating. It is also proposed to introduce practices of preparation and publication by technical standardization committees reports on the effectiveness of adopted standards in the cybersecurity sphere.

The main issues of normative-technical and normative-legal provision of cybersecurity subjects are determined: inconsistency of the state and development in Ukraine of the national system of standardization in the cybersecurity

[29] "The Constitution of Ukraine."

sphere and cyber protection with the needs of national security, sustainable development of digital economy and society, international obligations and requirements national legislation, its incompleteness, vagueness, inconsistency with international standardization systems and disregard for best international experience in this area;

In this article substantiated the necessity of formation the national standards based on international standards and harmonization the standards of states-members of international or regional standardization organizations, which is important for saving financial and time resources, and for ensure cross-border cooperation.

It is defined the list of international standards and standardization organizations, the activity results of which should be taken into account in the process of improving the system of regulatory and technical and regulatory documents on cyber security and cyber protection in Ukraine.

The dynamics of development of the system of normative and technical documents of SSSCIP is analyzed. The main stages are defined and the characteristic of each of them is given.

It is substantiated the necessity of establishment the national rating of the enterprises, establishments, the organizations which are implementing the international standards of cybersecurity and during all time of the activity are ready to confirm a condition of their maintenance is proved.

Taking into account the new legal norms and conditions defined in the Law of Ukraine "On Amendments to the Law of Ukraine On Information Protection in Information and Telecommunication Systems" "to confirm compliance of information systems with information protection requirements," it is advisable to more flexibly and reasonably implement of information resources and information in ITS on the basis of European approaches (standards) to information security, without obligatory application of the procedure of confirmation of conformity of the complex system of information protection.

## References

[1] "On Basic Principles of Cybersecurity in Ukraine," Law of Ukraine, 2017, https://zakon.rada.gov.ua/laws/show/2163-19.

[2] "The Constitution of Ukraine," 1996, https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80=.

[3] "On standardization: The law of Ukraine," 2014, https://zakon.rada.gov.ua/laws/show/1315-18#Text.

[4] "ITU-T Recommendations by series," 2020, https://www.itu.int/itu-t/recommendations/index.aspx?ser=X.

[5] National Institute of Standards and Technology, "National Bureau of Standards. NBS," NBSIR 79-1776R, 1979, https://www.nist.gov/pml/weights-and-measures/national-bureau-standards-publications-nbs.

[6] "ISO/IEC JTC 1/SC 27: Information security, cybersecurity and privacy protection," 2020, https://www.iso.org/committee/45306.html.

[7] "General Data Protection Regulation," 2016, https://gdpr-info.eu/.

[8] "Cyber security research and development act," 2002, https://www.congress.gov/107/plaws/publ305/PLAW-107publ305.pdf.

[9] "Federal Information Security Modernization Act," 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2521/text.

[10] Matt Barrett, Jeff Marron, Victoria Yan Pillitteri, Jon Boyens, Stephen Quinn, Greg Witte, and Larry Feldman, "Approaches for Federal Agencies to Use the Cybersecurity Framework," NIST, NISTIR 8170, March 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf.

[11] Ukrainian Research and Training Center of Standardization, Certification and Quality, 2020, http://uas.org.ua/ua/.

[12] "On Protection of Information in Information and Telecommunication Systems," The law of Ukraine, 1994, https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

[13] "On electronic trust services," The law of Ukraine, 2017, https://zakon.rada.gov.ua/laws/show/2155-19#Text.

[14] "RD TPI 2.5-004-99: Kryterii otsinky zakhyshchenosti informatsii v komp'iuternykh systemakh vid nesanktsionovanoho dostupu" [2.5-004-99 "Criteria for assessing the security of information in computer systems from unauthorized access"], Ukrainians Government, 2018, http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342.

[15] Valentyna Pleskach, Mariia Pleskachand Olena Zelikovska, "Information Security Management System in Distributed Information Systems," 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 300-303, https://doi.org/10.1109/ATIT494 49.2019.9030484.

## About the Authors

Maria **Pleskach** is a PhD student of the Institute of Law of Taras Shevchenko National University of Kyiv. https://orcid.org/0000-0003-3296-5475

Valentyna **Pleskach** is a Dr. Habil. (Economics), Professor, Candidate of Technical Sciences, Head of the Department of Applied Information Systems, Faculty of Information Technologies, Taras Shevchenko national University of Kyiv. https://orcid.org/0000-0003-0552-0972
*E-mail*: v.pleskach64@gmail.com.

Andrii **Semenchenko** is a Dr. PA (Public Administration), Professor, a Candidate of Science (Engineering), a director of The Institute of Senior Management of National Academy of Public Administration under the President of Ukraine, Kyiv. https://orcid.org/0000-0001-6482-3872.
E-mail: andrii.semenchenko@gmail.com.

Danylo **Mialkovskyi** is a PhD (Candidate) PA (Public Administration), Deputy Director of the Information Protection Department of the Administration of the State Service of Special Telecommunication and Information Protection of Ukraine, Kyiv. https://orcid.org/0000-0002-8246-8437
E-mail: daniilvm71@gmail.com.

Taras **Stanislavskyi** is a PhD. (Candidate) PA (Public Administration), Deputy Director of the Department of Logistic of the Administration of the State Service of Special Telecommunication and Information Protection of Ukraine, Kyiv.
http://orcid.org/0000-0002-8606-2557. E-mail: stv1@i.ua.