SATBAYEV UNIVERSITY

Computing & Engineering

Volume 1 (2023), Issue 3, 1-7

https://doi.org/10.51301/ce.2023.i3.01

International standards in the field of cryptography

Y. Aitkhozhayeva*, D. Akhmetsharipov

Satbayev University, Almaty, Kazakhstan

**Corresponding author: y.aitkhozhayeva@satbayev.university*

Abstract. Using mathematical algorithms and transformations to protect data by encrypting it, cryptographic mechanisms are reliable and indispensable methods of protecting information today. However, without certain rules, requirements and recommendations for the use of cryptographic mechanisms, the implementation of encryption does not provide adequate protection against information security threats. To solve this problem, it is necessary to focus on international standards in the field of cryptography, which contain the best techniques, practices and recommendations for ensuring data security. This paper reviews four ISO technical committees (ISO/IEC JTC 1/SC 27, ISO/IEC JTC 1/SC 29, ISO/IEC JTC 1/SC 29, ISO/IEC JTC 1/SC 6b ISO/TC 68/SC 2) involved in the development and regulation of international cryptographic standards. The cryptographic standards developed by these committees are analyzed. International standards are categorized by the type of cryptographic security mechanisms considered. Six main categories were identified, such as encryption mechanisms, authentication mechanisms, hash function mechanisms, key management mechanisms, prime number and bit generators, and requirements for cryptographic modules. Forty-eight international standards are analyzed by category, of which forty are active and eight are under development. The content of the most relevant international standards from each category is disclosed, their goals and objectives are indicated. The question of adaptation and harmonization of the considered international standards in the Republic of Kazakhstan is touched upon, as they play a key role in guaranteeing data security during their transmission and storage.

Keywords: *cryptography, information security, international standards.*

1. Introduction

The availability of information and communication technologies is the basis for building a modern information society and, at the same time, the reason for the need to ensure the security of this information society. The choice of the research theme is justified by the importance of cybersecurity issues in the modern digital society, where in-demand digital technologies are accompanied by potential threats and risks. Huge amounts of information stored in databases, transmitted through networks and processed in information systems require reliable protection mechanisms. In this context, cryptography plays an important role and cryptographic standards serve as a reliable guide to ensure the correct application of cryptographic mechanisms.

In today's world, standards play an important role by establishing generally accepted norms and rules to maintain uniformity and efficiency in various fields. In the digital age, when information technology is becoming an integral part of our daily lives, standards become even more important, especially in ensuring information security and interoperability.

International cryptographic standards are specifications and guidelines designed to guarantee the protection of confidentiality, integrity and authentication of data in the digital space. They cover broad aspects of cryptography, ranging from encryption methods to key management processes. International organizations such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are actively involved in the development and negotiation of these standards, thereby ensuring worldwide consistency in approaches to cryptographic security and creating universal frameworks for data exchange and interoperability on a global scale.

Cryptographic standards not only provide best techniques, practices, and technical guidance, but also foster common concepts and terminologies. This promotes mutual understanding between countries and organizations, fosters a common language in cybersecurity, and enhances overall preparedness to address threats in the digital space.

The purpose of this study is to analyze the scope of activities of organizations involved in the development and regulation of ISO/IEC international standards in the field of cryptography, categorize international standards by cryptographic security mechanisms based on their analysis, and reveal the content of the most relevant international standards from each category.

2. Materials and methods

2.1. Technical committees

The study examined and analyzed existing and currently relevant international cryptographic standards available on the ISO.org web resource. This source provided an extensive set of standards covering various aspects of cryptography, ranging from encryption methods to authentication and key management.

The research and analysis revealed that international cryptography standards are developed and regulated by four bodies, also known as technical committees.

Technical committees are specialized bodies that develop and maintain standards related to various aspects including cryptographic methods, protocols and technologies. These

committees play a key role in developing regulations that define the application of various encryption methods, authentication, key management and other cryptographic mechanisms. These committees bring together experts and stakeholders from around the world to harmonize and develop standards that promote interoperability and provide a high level of security in various fields including information technology, multimedia, finance, and telecommunications [1].

Figure 1 shows the four main technical committees involved in the development and regulation of international cryptographic standards.

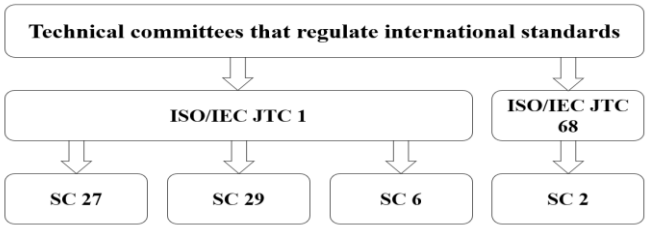

Figure 1. Technical committees governing international cryptographic standards

ISO/IEC JTC 1 (Joint Technical Committee 1) is a technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that specializes in standardization in the field of information security. Within this committee, it develops and updates cryptographic standards that cover a wide range of topics such as encryption algorithms, security protocols, key management, authentication methods, etc. The history of this committee, is related to the development of information security and cryptography. It begins at the end of the 20th century, when information security became one of the key aspects in the field of information technology. Joint Technical Committee 1 (JTC 1) was founded in 1990 by ISO and IEC. Within JTC 1, several subcommittees (Subcommittee, hereafter SC) were established: SC 27, SC 29 and SC 6 [2].

SC 27 (Subcommittee), focuses on various aspects of information security, including cryptography. The tasks of this committee include the development of standards, guidelines and recommendations on cryptography, as well as on other aspects of information security. Today, ISO/IEC JTC 1/SC 27 remains a key forum for the discussion and development of cryptography standards, playing an important role in securing information technology and systems worldwide [3].

SC 29 (Subcommittee), like SC 27, is a subcommittee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), except that it specializes in standardization in the areas of image, audio, and multimedia coding. The history of this committee also dates back to the period of intensive development of digital technologies at the end of the 20th century, when multimedia technologies became increasingly common in various fields such as telecommunications, entertainment, education and medicine. The SC 29 subcommittee focuses on standardizing the encoding, compression and transmission of multimedia data to ensure compatibility, playback quality and security. SC 29 develops and regulates standards for various file formats, codecs, and transmission protocols, and also develops standards and recommendations for protecting multimedia content, including cryptographic methods and protocols to ensure data confidentiality and integrity [4]. To date, Subcommittee SC 29 continues to actively work on developing and updating multimedia standards, including improving cryptographic techniques for securing multimedia data in various applications and industries.

SC 6 (Subcommittee 6) is also part of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), is concerned with information technology standardization in the areas of data management and organization. It focuses on various aspects of information management, including standards and recommendations for data models, data description languages, data processing methods, database management systems, and many other aspects related to organizing and storing information. The history of the SC 6 subcommittee dates back to the period of rapid development of information technology in the second half of the 20th century, when there was a need to standardize the management and organization of data. Since then, there has been an active development of standards focused on the efficient and secure organization and management of information. Cryptography is not the main focus of SC 6, but aspects of cryptography are also covered in standards related to data security and information systems protection [5].

ISO/TC 68 (International Organization for Standardization/Technical Committee 68) is a technical committee of the International Organization for Standardization (ISO) that deals with standardization in the areas of financial services, banking and monetary system. The committee's activities are aimed at developing and approving international standards that help to ensure the efficiency, reliability and safety of financial transactions and banking services. These standards address both data exchange, message formats, authentication processes, information security, including cryptographic mechanisms, and other technical and organizational aspects related to financial transactions.

ISO/TC 68 covers a wide range of topics including banking, payment systems, insurance, asset management, and other aspects of financial services. The work of the committee includes discussion and development of new standards, updating existing standards to meet changing market needs [6].

SC 2 (Subcommittee 6), is a subcommittee of ISO/TC 68 Technical Committee, focuses on the development of international standards in banking, securities and other financial services. The history of SC 2 is rooted in the development of the banking and financial industry, especially in the context of electronic payment systems and cards. Cryptography also plays an important role in the work of SC 2. In the context of financial services and banking, cryptography is used to ensure information security, data protection and transaction confidentiality. Thus, cryptography is an integral part of SC 2 work and plays a key role in ensuring the safety and soundness of financial transactions and banking services [7].

2.2. Categorization of International Standards

After analyzing international cryptographic standards, six major categories of international standards were identified, each covering specific aspects of cryptographic applications. Forty-eight standards were examined, of which forty are active and eight are under development. Standards were analyzed and categorized by identifying major thematic clusters, identifying key terms and technical solutions, and determining their impact on information security.

The categorization of international standards was done in the following aspects: encryption mechanisms were identified in the first category, authentication mechanisms were identified in the second category, hash function mechanisms were identified in the third category, key management mechanisms were identified in the fourth category, prime number and bit generators were identified in the fifth category, and requirements for cryptographic modules were identified in the sixth category.

Figure 2 shows the scheme of the performed categorization.

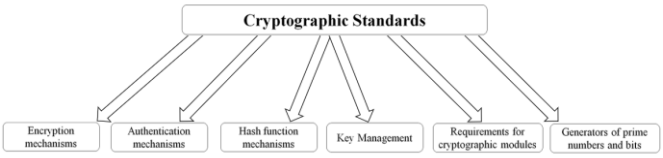

Figure 2. Categorization of International Cryptographic Standards (change title, should be: Requirements for Cryptographic Modules)

The stages of analysis and categorization of standards allowed us to identify their importance in ensuring strong data protection in today's digital world. This approach to research allows to present a complete picture of standards and their role in cryptographic security.

3. Results and discussion

Fourteen standards covering encryption mechanisms, five standards dealing with authentication mechanisms, three standards dealing with hash function mechanisms, eight standards dealing with key management, three standards dealing with prime number and bit generators, and five standards dealing with requirements for cryptographic modules were identified and analyzed. Below is an analysis of several major international cryptographic standards in each of the six categories.

3.1. Encryption mechanisms

ISO/IEC Standard 18033. Information security. Encryption algorithms. The ISO/IEC 18033 series consists of seven parts, of which six are valid, dealing with cryptographic encryption algorithms and key management techniques. The first part of the standard, ISO/IEC 18033-1, is dedicated to presenting the general definitions and concepts used in subsequent parts of the standard. The standard introduces the basic concepts of encryption and describes the general aspects of its application and characteristics. The second part of the standard, ISO/IEC 18033-2, defines encryption systems for data confidentiality, which use encryption algorithms to protect plaintext information in transmission or storage. The third part of the standard, ISO/IEC 18033-3, specifies block ciphers in symmetric encryption systems, describing algorithms for processing plaintext blocks and defining crypto algorithms for 64-bit (TDEA, MISTY1, CAST-128, HIGHT) and 128-bit (AES, Camellia, SEED) block ciphers. The fifth part of the standard, ISO/IEC 18033-5, addresses identity-based encryption mechanisms. The sixth part of the standard, ISO/IEC 18033-6, describes two homomorphic encryption mechanisms such as El-Gamal exponential encryption and Paye encryption. The seventh part of the standard, ISO/IEC 18033-7, deals with mechanisms for customized block ciphers [8]. The current standards of ISO/IEC 18033 series have no adapted and harmonized analogues in the Republic of Kazakhstan.

ISO/IEC Standard 29150. Information technology. Security techniques. Signcryption. ISO/IEC 29150 defines four mechanisms for encrypting signatures, based on public key encryption methods that require their own public and private key pairs for both sender and receiver [9]. The current standard was published in December 2011 and amended in March 2013. In the Republic of Kazakhstan there is no adapted and harmonized analogue of this standard.

ISO/IEC 10116. Information technology. Security techniques. Modes of operation for an n-bit block cipher. ISO/IEC 10116 specifies modes of operation for an n-bit block cipher to ensure data confidentiality in transmission or storage. However, these modes do not include data integrity protection and do not guarantee confidentiality of message length information [10]. The current version of the standard was published in July 2017. The adapted and harmonized analogue of the standard is used in the Republic of Kazakhstan.

ISO/IEC Standard 14888. Information technology. Security tecniques. Digital signatures with appendix. The ISO/IEC 14888 series of standards consists of three parts, each defining encryption and digital signature mechanisms. The first part of the standard, ISO/IEC 14888-1, describes the general principles and requirements for digital signatures with an annex. The second part of the standard, ISO/IEC 14888-2 addresses digital signature mechanisms based on integer factoring. The third part of ISO/IEC 14888-3 addresses digital signatures based on discrete logarithm [11]. The current versions of the standards were published in April 2008, validated in October 2015 and in November 2018. The Republic of Kazakhstan has and uses an adapted and harmonized analogue of these standards.

ISO/IEC Standard 13888. Information security. Non-repudiation. The ISO/IEC 13888 series of standards consists of three parts, each focusing on fault tolerance techniques using cryptographic encryption mechanisms. The first part of the standard, ISO/IEC 13888-1, is a generic model with descriptions and requirements for the subsequent sections. The second part of the standard, ISO/IEC 13888-2, defines common structures for services that provide authorship preservation, as well as communication-related mechanisms for provenance preservation and secure delivery. The third part of the standard, ISO/IEC 13888-3 defines mechanisms for providing specific, communication-related fault tolerance services using asymmetric cryptographic techniques [12]. The current versions of the standards were published in December 2012 and validated in September 2020. There are no adapted and harmonized analogues of this standard in the Republic of Kazakhstan.

3.2. Authentication mechanisms

ISO/IEC Standard 19772. Information security. Authenticated encryption. ISO/IEC 19772 specifies five authenticated encryption mechanisms based on block cipher algorithms that require a shared secret key between sender and receiver to ensure confidentiality, integrity and authentication of the data source. Of the five mechanisms described, four allow authentication of unencrypted data by separating the data into an encrypted portion and additional authenticated

data [13]. The current version of the standard is published in November 2020. The Republic of Kazakhstan has an adapted and harmonized analogue of this standard.

ISO/IEC 9798 Information technology. Security techniques. Entity authentication. The ISO/IEC 9798 series of standards consists of six parts describing different authentication mechanisms. The first part of ISO/IEC 9798-1 describes general requirements and constraints for object authentication mechanisms. The second part of the standard, ISO/IEC 9798-2 describes object authentication mechanisms that use authenticated encryption algorithms. Of the mechanisms described in the standard, four mechanisms provide authentication between two objects without the involvement of a trusted third party, two mechanisms are mechanisms for one-way authentication of one object to another, and two mechanisms for mutual authentication of two objects. The remaining mechanisms involve a trusted third party online to create a shared secret key. All of these mechanisms implement mutual or unilateral authentication of objects. The third part of ISO/IEC 9798-3 describes object authentication mechanisms based on digital signatures and asymmetric methods. A digital signature is used to verify the identity of an object. The standard describes ten mechanisms, the first, five of which do not require a trusted online third party, while the last five utilize trusted online third parties. Both categories include two mechanisms for one-way authentication and three mechanisms for mutual authentication. The fourth part of ISO/IEC 9798-4 specifies mechanisms for authenticating objects using the cryptographic verification function. Of these, two are for authentication of a single object (one-way authentication), while the others are mechanisms for mutual authentication of two objects. The fifth part of ISO/IEC 9798-5 specifies mechanisms for authenticating objects using zero-disclosure methods. The sixth part of ISO/IEC 9798-6 defines eight object authentication mechanisms that use manual data transfer between authenticating devices. Of these, four are enhanced versions of the mechanisms described in the previous version of ISO/IEC 9798-6:2005, with reduced user involvement and enhanced security [14].

The current versions of the standards have been published: part one in July 2010, part two in June 2019, part three in January 2019, part four July 2012, part five in December 2009 and part six in December 2012.

ISO/IEC Standard 25185. Identification cards. Integrated circuit card authentication protocols. ISO/IEC 25185 describes an authentication protocol for use in physical and logical access control systems based on ICC (International Chamber of Commerce) and related standards including AES-128, RSA-2048 and SHA-256 for encryption and hashing, defines PLAID? and its implementation to ensure interoperability between different implementations [15]. The current standard was published in January 2016 and is current at this time. In the Republic of Kazakhstan there is no adapted and harmonized analogue of this standard.

3.3. Hash-functions

ISO/IEC Standard 10118. Information technology. Security techniques. Hash-functions. The ISO/IEC 10118 series of standards consists of four parts describing hash function mechanisms. The first part of the standard, ISO/IEC 10118-1 defines hash functions for providing authentication, integrity and fault tolerance services, where the second part of the standard, ISO/IEC 10118-2 defines hash functions using the n-bit block cipher algorithm. The third part of ISO/IEC 10118-3 describes hash functions using iterative round-robin functions. The fourth part of ISO/IEC 10118 defines two hash functions, MASH-1 and MASH-2, based on modular arithmetic [16]. The current versions of the standards were published in October 2016, October 2010, October 2018, and July 2014. The first and fourth parts of the standard have adapted and harmonized analogues in the Republic of Kazakhstan.

ISO/IEC Standard 9797. Information technology. Security techniques. Message Authentication Codes (MAC). The series of standards consists of three parts dealing with the hash function mechanism. The first part of the standard, ISO/IEC 9797-1 specifies six MAC algorithms that use a secret key and an n-bit block cipher to compute an m-bit MAC. The second part of the standard, ISO/IEC 9797-2 specifies MAC algorithms that use a secret key and a hash function (or its rounding function or sponge function) to compute an m-bit MAC. The third part of the standard, ISO/IEC 9797-3 defines Message Authentication Code (MAC) algorithms that use a secret key and a universal hash function with an n-bit result to compute an m-bit MAC based on the block ciphers specified in ISO. /IEC 18033-3 and stream ciphers specified in ISO/IEC 18033-4[17]. The current versions of the standards were published in March 2011, June 2021 and November 2011. In the Republic of Kazakhstan, the above standards do not have adapted and harmonized counterparts.

3.4. Key management

ISO/IEC 11770 Standard. Information technology. Security techniques. Key management. The ISO/IEC 11770 series of standards consists of seven parts. The first part of the standard, ISO/IEC 11770-1, defines a universal key management model independent of a particular cryptographic algorithm. The standard covers both automated and manual aspects of key management, including data elements and operations for obtaining key management services. The second part of ISO/IEC 11770-2 specifies mechanisms for key establishment using symmetric cryptographic methods in three environments: point-to-point, key distribution center (KDC) and key translation center (KTC). The third part of ISO/IEC 11770-3 defines key management mechanisms based on asymmetric cryptographic methods. Schemes for their use in key agreement are considered, as well as schemes that can be used when delivering keys to establish a shared secret key in a symmetric cryptographic system. The fourth part of ISO/IEC 11770-4 defines key generation mechanisms based on weak secrets that can be easily memorized by humans. The fifth part of ISO/IEC 11770-5 defines mechanisms for establishing common symmetric keys between groups of objects. The sixth part of ISO/IEC 11770-6:2016 defines key derivation functions, i.e., functions that take secret information and other (public) parameters as input and output one or more "derived" parameters. The seventh part of ISO/IEC 11770-7 defines mechanisms for inter-domain key exchange with password-based authentication, all of which are four-party key exchange protocols with password-based authentication [18].

Up-to-date versions of the standards were published in the following years: part one in December 2010, part two in October 2018, part three in October 2021, part four in February 2021, part five in November 2020, part six in October 2016, and part seven in July 2021.

The first, second and fourth parts of the standard have adapted and harmonized counterparts in the Republic of Kazakhstan.

ISO/IEC 27099. Information technology. Public key infrastructure. Practices and policy framework. ISO/IEC 27099 establishes requirements for information security management of public key infrastructure (PKI) services. It includes policies and practices for certification through an information security management system (ISMS). The standard focuses on information security risk assessment and covers the public key lifecycle. It uses concepts from ISO/IEC 27000 standards and rules from ISO/IEC 27002 for information security management [19].

The standard was published in June 2022 and is current at the moment.

The Standard has no adapted and harmonized analogues in the Republic of Kazakhstan.

ISO/IEC 29192 Information technology. Security techniques. Lightweight cryptography. The ISO/IEC 29192 family of standards comprises eight parts, of which the third part deals with block key management techniques. The standard defines key stream generators for lightweight stream ciphers adapted for implementation in constrained environments.

Within this standard, two dedicated key stream generators are presented for lightweight stream ciphers such as:

- Enocoro: a lightweight key stream generator with a key size of 80 or 128 bits;
- Trivium: a lightweight key stream generator with a key size of 80 bits [20].

The standard was published in October 2012 and is relevant today.

There are no adapted harmonized versions of this standard available in the Republic of Kazakhstan.

ISO/IEC 18033. Information security. Encryption algorithms. Of the seven parts of the standard, the fourth part describes key management techniques. ISO/IEC 18033-4 defines output functions for combining a key stream with plaintext, key stream generators for creating a key stream, and object identifiers assigned to dedicated key stream generators in accordance with ISO/IEC 9834 [21]. The current version of the standard is published in August 2020. There is no adapted and harmonized analogue of this standard in the Republic of Kazakhstan.

3.5. Prime number generation

ISO/IEC Standard 18032. Information security - Prime number generation. ISO/IEC Standard 18032 describes and specifies methods for generating and verifying prime numbers required for cryptographic protocols and algorithms. The standard describes methods to verify the simplicity of a number, methods of their generation, including probabilistic and deterministic approaches [22]. The current version of the standard was published in December 2020. In the Republic of Kazakhstan there is no adapted and harmonized analogue of this standard.

ISO/IEC Standard 20543. Information technology. Security techniques. Test and analysis methods for random bit generators in accordance with ISO/IEC 19790 and ISO/IEC 15408. ISO/IEC 20543 is a description and methodology for evaluating random bit generators intended for cryptographic applications, regardless of their determinism. The standard was published in October 2019 and is currently valid [23]. There is no adapted and harmonized analogue of this standard in the Republic of Kazakhstan.

3.6. Requirements for cryptographic modules

ISO/IEC Standard 19790. Information technology. Security techniques. Security requirements for cryptographic modules. ISO/IEC 19790 specifies security requirements for cryptographic modules used in security systems designed to protect confidential information in computer and telecommunication environments. The standard specifies four levels of security for cryptographic modules, where each security level represents a stepwise increase in protection over the previous level [24]. The current version of the standard was published in September 2012 and corrected with an addendum in October 2015. In the Republic of Kazakhstan there is no adapted and harmonized analogue of this standard.

Standard ISO/IEC 24759 Information technology. Security techniques. Test requirements for cryptographic modules. ISO/IEC 24759 establishes and defines the methods used by test laboratories to verify that a cryptographic module meets the requirements specified in ISO/IEC 19790:2012. The methods are designed to ensure a high degree of objectivity in the testing process and to ensure uniformity of results across test laboratories. The standard also specifies requirements for the information that vendors provide to test laboratories as evidence to demonstrate that their cryptographic modules meet the requirements specified in ISO/IEC 19790:2012 [25]. The current version of the standard was published in March 2017. The adapted and harmonized analogue of this standard is used in the territory of the Republic of Kazakhstan.

ISO/IEC TC 20540. Information technology. Methods of security assurance. Testing cryptographic modules in their operational environment. ISO/IEC TC 20540 provides guidelines and checklists to support the specification and operational testing of cryptographic modules in an organization's security environment. Cryptographic modules have four levels of security defined in ISO/IEC 19790 to ensure the confidentiality of data of different levels of importance and for use in different environments (e.g., secure facility, office, removable media, completely unsecured location) [26]. The current version of the standard was published in May 2018. There is no adapted and harmonized analogue of this standard in the Republic of Kazakhstan.

Standard ISO/IEC 17825. Information technology. Security techniques. Testing methods for the mitigation of non-invasive attack classes against cryptographic modules. ISO/IEC 17825 specifies metrics for a non-invasive attack mitigation test to determine compliance with the requirements specified in ISO/IEC 19790 for security levels 3 and 4. These metrics are closely related to the security functions listed in ISO/IEC 19790. Testing is performed on specific cryptographic module boundaries and I/O available at specific boundaries [27]. The standard was published in January 2016 and has an adapted and harmonized counterpart in the Republic of Kazakhstan.

4. Conclusions

Cryptography, as a fundamental science of information security, is an integral part of today's digital world. Its role is growing rapidly in the context of the expanding Internet, the rapid development of information technology, blockchain technologies and the spread of the Internet of Things (IoT). Cryptography is complex mathematical algorithms that not only provide privacy and authentication, but also protect data from ever-evolving cyber threats. Cryptography not only represents an area of active research, but also plays a critical

role in shaping a digital trust environment where information remains secure and the integration of new technologies is based on sound security principles.

Cryptography standards are the foundation for securing information and data exchange. They define critical important mechanisms such as encryption algorithms, authentication methods, hash function mechanisms, key management mechanisms, prime and bit generators, and requirements for cryptographic modules.

The presented analysis of standards, their categorization gives an opportunity to simplify and accelerate the search and selection of necessary standards when developing and/or applying security mechanisms in the field of cryptography. Developed by experts and recognized by international organizations such as ISO and IEC, these standards guarantee the compatibility and reliability of cryptographic solutions. Thanks to standards, any industry can build secure systems that meet the highest information security requirements and ensure data protection in the digital world.

References

[1] Technical Committees ISO (en). ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/technical-committees.html

[2] Technical Committees ISO/IEC JTC 1 (en). Online Browsing Platform. *Retrieved from*: https://jtc1info.org/about/

[3] ISO/IEC JTC 1/SC 27 (en). ISO Online Browsing Platform. *Retrieved from:* https://www.iso.org/committee/45306.html

[4] ISO/IEC JTC 1/SC 29 (en). ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/committee/45316.html

[5] ISO/IEC JTC 1/SC 6 (en). ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/committee/45072.html

[6] Technical Committees ISO/TC 68 (en). ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/committee/49670.html

[7] Technical Committees ISO/TC 68/SC 2 (en). ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/committee/49670.html

[8] ISO/IEC 18033 (en). Information security - Encryption algorithms. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=18033

[9] ISO/IEC 29150 (en). Information technology - Security techniques-Signcryption. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=29150

[10] ISO/IEC 10116:2017 (en). Information technology - Security techniques — Modes of operation for an n-bit block cipher. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=10116

[11] ISO/IEC 14888-3:2018 (en). IT Security techniques - Digital signatures with appendix. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=14888

[12] ISO/IEC 13888 (en). Information technology — Security techniques — Non-repudiation. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=13888

[13] ISO/IEC 19772:2020 (en). Information security - Authenticated encryption. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/standard/81550.html

[14] ISO/IEC 9798 (en). Information technology - Security techniques- Entity authentication. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=9798

[15] ISO/IEC 25185 (en). Identification cards- Integrated circuit card authentication protocols. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=25185

[16] ISO/IEC 10118 (en). IT Security techniques - Hash-functions. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=10118

[17] ISO/IEC 9797 (en). Information technology - Security Techniques-Message Authentication Codes (MACs). ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=9797

[18] ISO/IEC 11770 (en). Information technology - Security techniques - Key management. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=11770

[19] ISO/IEC 27099 (en). Information technology - Public key infrastructure- Practices and policy framework. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=27099

[20] ISO/IEC 29192 (en). Information technology - Security techniques- Lightweight cryptography. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=29192

[21] ISO/IEC 18033 (en). Information security - Encryption algorithms. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=18033

[22] ISO/IEC 18032 (en). Information security - Prime number generation. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=18032

[23] ISO/IEC 20543 (en). Information technology- Security techniques - Test and analysis methods for random bit generators. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=20543

[24] ISO/IEC 19790 (en). Information technology — Security techniques — Security requirements for cryptographic modules. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=19790

[25] ISO/IEC 24759 (en). Information technology - Security Techniques-Test requirements for cryptographic modules. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=24759

[26] ISO/IEC TC 20540 (en). Information technology — Security techniques — Testing cryptographic modules in their operational environment. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=20540

[27] ISO/IEC 17825 (en). Information technology. Security techniques. Testing methods for the mitigation of non-invasive attack classes against cryptographic modules. ISO Online Browsing Platform. *Retrieved from*: https://www.iso.org/search.html?q=17825

Криптография саласындағы халықаралық стандарттар

Е. Айтхожаева*, Д. Ахметшәріпов

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: y.aitkhozhayeva@satbayev.university*

Аңдатпа. Деректерді шифрлау арқылы қорғау үшін математикалық алгоритмдер мен түрлендірулерді қолдана отырып, криптографиялық механизмдер бүгінгі күнге дейін ақпаратты қорғаудың сенімді және таптырмас әдістері

болып табылады. Алайда, криптографиялық механизмдерді қолдану бойынша белгілі бір ережелер, талаптар мен ұсыныстар болмаса, шифрлауды жүзеге асыру ақпараттық қауіпсіздік қатерлерінен тиісті қорғауды қамтамасыз етпейді. Бұл мәселені шешу үшін криптография саласындағы халықаралық стандарттарға назар аудару қажет, онда ең жақсы техникалар, тәжірибелер және деректер қауіпсіздігін қамтамасыз ету бойынша ұсыныстар жинақталған. Жұмыста криптография саласындағы халықаралық стандарттарды әзірлеумен және реттеумен айналысатын төрт ISO (ISO/IEC JTC 1/SC 27, ISO/IEC JTC 1/SC 29, ISO/IEC JTC 1/SC 6B ISO/TC 68/SC 2) техникалық комитеттеріне шолу жасалды. Осы комитеттер әзірлеген криптография саласындағы стандарттарға талдау жүргізілді. Криптография саласындағы қауіпсіздікті қамтамасыз ету тетіктерінің түрі бойынша халықаралық стандарттарды санаттау жүргізілді. Шифрлау механизмдері, аутентификация механизмдері, хэш функциялары, кілттерді басқару механизмдері, жай сандар мен бит генераторлары, криптографиялық модульдерге қойылатын талаптар сияқты алты негізгі санат анықталды. Санаттар бойынша қырық сегіз халықаралық стандарт талданды, оның ішінде қырық белсенді, ал сегізі әзірленуде. Әр санаттағы ең өзекті халықаралық стандарттардың мазмұны ашылды, олардың мақсаттары мен міндеттері көрсетілген. Қазақстан Республикасында қаралған халықаралық стандарттарды бейімдеу және үйлестіру мәселесі қозғалады, өйткені олар деректерді беру және сақтау кезінде олардың қауіпсіздігіне кепілдік беруде шешуші рөл атқарады.

Негізгі сөздер: *криптография, ақпаратты қорғау, халықаралық стандарттар*.

Международные стандарты в области криптографии

Е. Айтхожаева[*], Д. Ахметшәріпов

[1] *Satbayev University, Алматы, Казахстан*

**Автор для корреспонденции: y.aitkhozhayeva@satbayev.university*

Аннотация. Используя математические алгоритмы и преобразования для защиты данных путем их шифрования, криптографические механизмы являются надежными и незаменимыми методами защиты информации на сегодняшний день. Однако без определенных правил, требований и рекомендаций по использованию криптографических механизмов, реализация шифрования не обеспечивает должной защиты от угроз информационной безопасности. Для решения данной проблемы необходимо ориентироваться на международные стандарты в области криптографии, в которых собраны лучшие техники, практики и рекомендации по обеспечению безопасности данных. В работе выполнен обзор четырех технических комитетов ISO (ISO/IEC JTC 1/SC 27, ISO/IEC JTC 1/SC 29, ISO/IEC JTC 1/SC 6б ISO/TC 68/SC 2), занимающихся разработкой и регулированием международных стандартов в области криптографии. Проведен анализ разработанных этими комитетами стандартов в области криптографии. Проведена категоризация международных стандартов по типу рассматриваемых механизмов обеспечения безопасности в области криптографии. Определены шесть основных категорий, такие как механизмы шифрования, механизмы аутентификации, механизмы хэш-функций, механизмы управления ключами, генераторы простых чисел и битов, требования к криптографическим модулям. По категориям проанализировано сорок восемь международных стандартов, из которых сорок являются активными, а восемь находятся в стадии разработки. Раскрыто содержание наиболее актуальных международных стандартов из каждой категории, указаны их цели и задачи. Затронут вопрос адаптации и гармонизации рассмотренных международных стандартов в Республике Казахстан, поскольку они играют ключевую роль в гарантировании безопасности данных при их передаче и хранении.

Ключевые слова: *криптография, информационная безопасность, международные стандарты*.

Received: 20 April 2023
Accepted: 15 September 2023
Available online: 30 September 2023