Scientific and Practical Cyber Security Journal (SPCSJ) 5(3): 30-36 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

SYNTHESIS OF QUANTUM KEY DISTRIBUTION AND LIGHTWEIGHT ENCRYPTION FOR DATA PRIVACY IN MODERN INFORMATION AND COMMUNICATION SYSTEMS

Sergiy Gnatyuk, NAU Cybersecurity R&D Lab http://cyberlab.fccpi.nau.edu.ua/
National Aviation University, Kyiv, Ukraine
Rat Berdibayev, Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
Yuliia Burmak, NAU Cybersecurity R&D Lab http://cyberlab.fccpi.nau.edu.ua/
National Aviation University, Kyiv, Ukraine
Dinara Ospanova, Kazakh Humanitarian Juridical Innovative University, Semey, Kazakhstan
Yuliia Polishchuk1 , NAU Cybersecurity R&D Lab http://cyberlab.fccpi.nau.edu.ua/
National Aviation University, Kyiv, Ukraine

ABSTRACT: Key distribution is one of the most important problems of cryptography. This problem can be solved by different approaches – QKD is one of these methods. Today there are many QKD methods and systems, most of them is used in complex with traditional cryptography. In this paper the analysis of quantum technologies was carried out. It was declared that QKD is most implemented quantum technology in both laboratory (experimental) and commercial sector. Modern QKD protocols were analyzed as well as advantages / disadvantages were defined. Also it was declared, that QKD protocols can be used in complex with lightweight encryption for data privacy in modern information and communication systems (for example, IoT). To provide high security level lightweight algorithms can be changed on secure post-quantum algorithms.

KEYWORDS*: ICT,cybersecurity, QKD, data privacy, encryption, IoT, lightweight cryptography.*

1. Introduction

The main features of information security are confidentiality, integrity and availability (CIA-Triad, Fig. 1). Only providing these all gives availability for development secure ICT[1]:

- *Confidentiality* is the basic feature of information security, which ensures that information is accessible only to authorized users who have an access.
- *Integrity* is the basic feature of information security indicating its property to resist unauthorized modification.
- *Availability* is the basic feature of information security that indicates accessible and usable upon demand by an authorized entity.

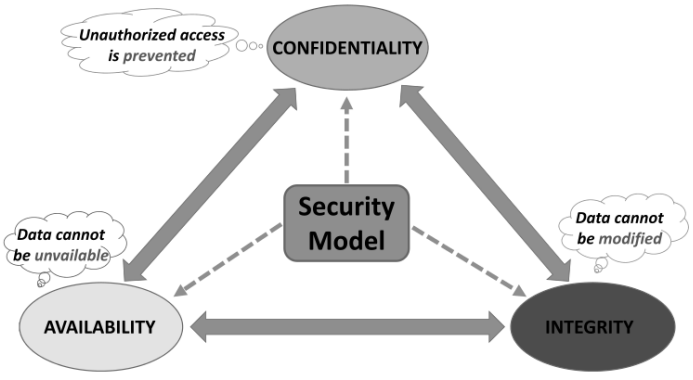

Figure 1. CIA-Triad

One of the most effective ways to ensureconfidentiality and data integrity during transmission is cryptographic systems. The purpose of such systems is to provide key distribution, authentication, legitimate users authorisation, and encryption. *Key distribution is one of the most important problems of cryptography.* This problem can be solved with the help of the following approaches [2]:

- *Classical information-theoretic schemes* (requires channel with noise; efficiency is very low, 1-5%).

- *Classical public-key cryptography schemes* (Diffie-Hellman scheme, digital envelope scheme; it has computational security).
- *Classical computationally secure symmetric-key cryptographic schemes* (requires a pre-installed key on both sides and can be used only as scheme for increase in key size but not as key distribution scheme).
- *Quantum key distribution* (provides information-theoretic security; it can also be used as a scheme for increase in key length).
- *Trusted Couriers Key Distribution* (it has a high price and is dependent on the human factor).

In recent years, quantum cryptography (QC) has attracted considerable interest. Quantum key distribution (QKD) plays a dominant role in QC. The overwhelming majority of theoretic and practical research projects in QC are related to the development of QKD protocols. The number of different quantum technologies is increasing.

The first of all *quantum technologies of information security* consist of [2]:

- Quantum key distribution.
- Quantum secure direct communication.
- Quantum steganography.
- Quantum secret sharing.
- Quantum stream cipher.
- Quantum digital signature etc.

QUANTUM DIGITAL SIGNATURE		*QUANTUM KEY DISTRIBUTION*		*QUANTUM STREAM CIPHER*	*QUANTUM SECRET SHARING*		*QUANTUM SECURE DIRECT COMMUNICATION*		
QDS using single qubits	**QDS** using entangled states	**QKD** using single qubits and qudits	**QKD** using entangled states	Yuen 2000 protocol (Y-00, αη-scheme)	**QSS** using single qubits	**QSS** using entangled states	**Ping-pong** protocol	**QSDC** using single qubits	**QSDC** with block transfer

Figure 2. Quantum technologies of information security

The main task of this study is…

2. QKD protocols

2.1. Review of the modern QKD protocols

QKD includes the following protocols:

- protocols using single (non-entangled) qubits (two-level quantum systems) and qudits (*d*-level quantum systems, *d*>2);
- protocols using phase coding;
- protocols using entangled states;
- decoy states protocols and some other protocols.

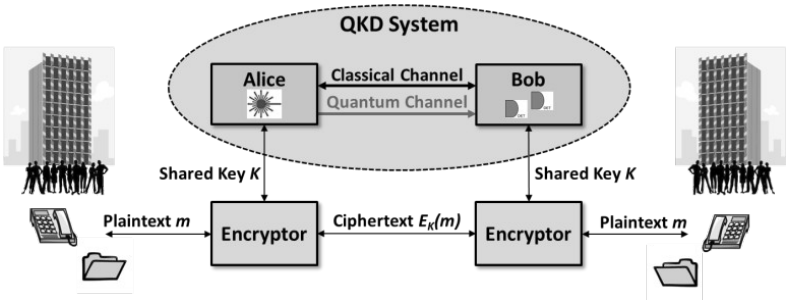

Figure 3. Scheme of QKD system implementation

The main task of QKD protocols is encryption key generation and distribution between two users connecting via quantum and classical channels (Fig. 3). In 1984 Ch. Bennett from IBM and G. Brassard from Montreal University introduced the first QKD protocol, which has become an

alternative solution for the problem of key distribution. This protocol is called *BB84* and it refers to QKD protocols using single qubits. The states of these qubits are the polarisation states of single photons. The BB84 protocol (Fig. 4) uses four polarisation states of photons (0°, 45°, 90°, 135°). These states refer to two mutually unbiased bases. Error searching and correcting is performed using classical public channel, which need not be confidential but only authenticated. For the detection of intruder actions in the BB84 protocol, an error control procedure is used, and for providing unconditionally security a privacy amplification procedure is used. The efficiency of the BB84 protocol equals 50%. Efficiency means the ratio of the photons number which are used for key generation to the general number of transmitted photons.

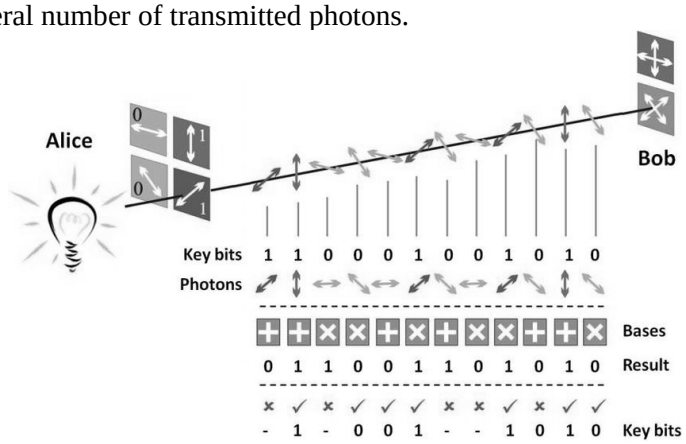

Figure 4. Scheme of BB84 protocol realization

Six-state protocol requires the usage of four states, which are the same as in the BB84 protocol, and two additional directions of polarization: right circular and left circular. Such changes decrease the amount of information, which can be intercepted. But on the other hand, the efficiency of the protocol decreases to 33%.

Next, the *4+2 protocol* is intermediate between the BB84 and B92 protocol. There are four different states used in this protocol for encryption: “0” and “1” in two bases. States in each base are selected non-orthogonal. Moreover, states in different bases must also be pairwise non-orthogonal. This protocol has a higher information security level than the BB84 protocol, when weak coherent pulses, but not a single photon source, are used by sender. But the efficiency of the 4+2 protocol is lower than efficiency of BB84 protocol.

In the *Goldenberg-Vaidman protocol*, encryption of “0” and “1” is performed using two orthogonal states. Each of these two states is the superposition of two localised normalised wave packets. For protection against intercept-resend attack, packets are sent at random times.

A modified type of Goldenberg-Vaidman protocol is called the *Koashi-Imoto protocol*. This protocol does not use a random time for sending packets, but it uses an interferometer’s non-symmetrisation (the light is broken in equal proportions between both long and short interferometer arms).

Another type of QKD protocol is a protocol using phase coding: for example, the B92 protocol using strong reference pulses. An eavesdropper can obtain more information about the encryption key in the B92 protocol than in the BB84 protocol for the given error level, however. Thus, the security of the B92 protocol is lower than the security of the BB84 protocol. The efficiency of the B92 protocol is 25%.

The *Ekert protocol (E91)* (Ekert, 1991) refers to QKD protocols using entangled states. Entangled pairs of qubits that are in a singlet state $|\psi^-\rangle = 1/\sqrt{2}(|0\rangle|1\rangle - |1\rangle|0\rangle)$ are used in this protocol. Qubit interception between Alice to Bob does not give Eve any information because no coded information is there. Information appears only after legitimate users make measurements and communicate via classical public authenticated channel. But attacks with additional quantum systems (ancillas) are nevertheless possible on this protocol.

The *SARG04 protocol* does not differ much from the original BB84 protocol (Fig. 5). The main difference does not refer to the ‘quantum’ part of the protocol; it refers to the “classical” procedure of key sifting, which goes after quantum transfer. Such improvement allows increasing security against photon number splitting attack. The SARG04 protocol in practice has a higher key rate than the BB84 protocol.

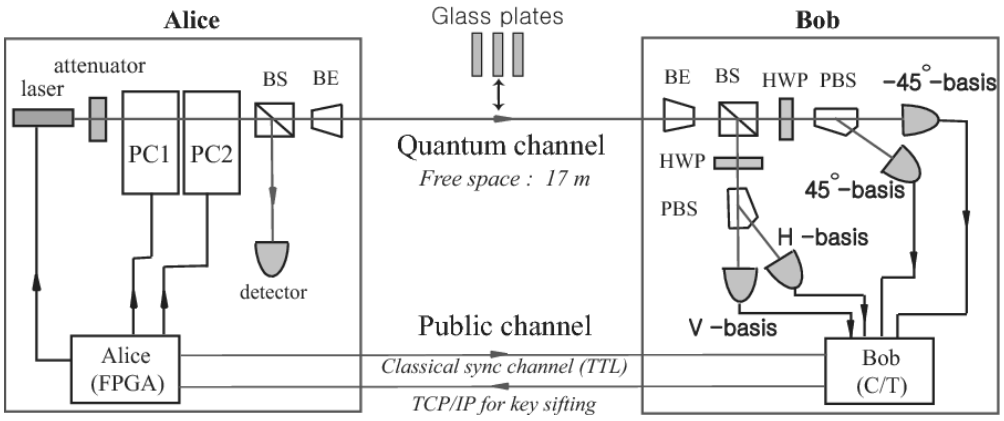

Figure 5. Scheme of SARG04 protocol implementation

Another way of protecting against photon number splitting attack is the use of *decoy states QKD protocols* (Fig. 6), which are also advanced types of BB84 protocol. In such protocols, besides information signals Alice's source also emits additional pulses (decoys) in which the average photon number differs from the average photon number in the information signal. Eve's attack will modify the statistical characteristics of the decoy states and/or signal state and will be detected. As practical experiments have shown for these protocols (as for the SARG04 protocol), the key rate and practical length of the channel is bigger than for BB84 protocols. Nevertheless, it is necessary to notice that using these protocols, as well as the others considered above, it is also impossible without users pre-authentication to construct the complete high-grade solution of the problem of key distribution.

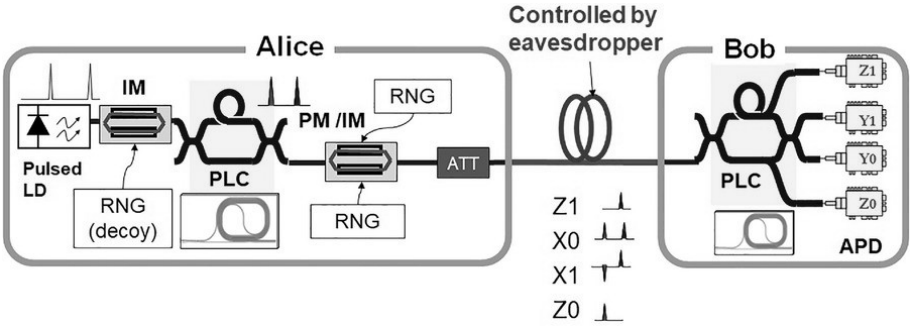

Figure 6. Scheme of decoy states QKD protocols

2.2. Advantages and disadvantages of QKD protocols

As a conclusion, after the analysis of the first and scale quantum method, we must sum up and highlight the following *advantages of QKD protocols*[2-4]*:*

1) These protocols always allow eavesdropping to be detected because Eve's connection brings much more error level (compared with natural error level) to the quantum channel. The laws of quantum mechanics allow eavesdropping to be detected and the dependence between error level and intercepted information to be set. This allows applying privacy amplification procedure, which decreases the quantity of information about the key, which can be intercepted by Eve. Thus, QKD protocols have unconditional (information-theoretic) security.

2) The information-theoretic security of QKD allows using an absolutely secret key for further encryption using well-known classical symmetrical algorithms. Thus, the entire information security level increases. It is also possible to synthesize QKD protocols with Vernam cipher (one-time pad) which in complex with unconditionally secured authenticated schemes gives a totally secured system for transferring information.

The disadvantages of quantum key distribution protocols are following [2-4]:

1) A system based only on QKD protocols cannot serve as a complete solution for key distribution in open networks (additional tools for authentication are needed).

2) The limitation of quantum channel length which is caused by the fact that there is no possibility of amplification without quantum properties being lost. However, the technology of quantum repeaters could overcome this limitation in the near future.

3) Need for using weak coherent pulses instead of single photon pulses. This decreases the efficiency of protocol in practice. But this technology limitation might be defeated in the nearest future.

4) The data transfer rate decreases rapidly with the increase in the channel length.

5) Photon registration problem which leads to key rate decreasing in practice.

6) Photon depolarization in the quantum channel. This leads to errors during data transfer. Now the typical error level equals a few percent, which is much greater than the error level in classical ICT and systems.

7) Difficulty of the practical realisation of QKD protocols for *d*-level quantum systems.

8) The high price of commercial QKD systems (€ 120K +).

3. IoT Cybersecurity and Lightweight Cryptography

It was defined a lot of QKD challenges as well as many advantages for modern ICT. Most of all advantages relate to the only key distribution part and the security of encryption process is open question that depends on encryption algorithm [5]. Up to date secret key ciphers have key length of 256 bit (min) and cannot be implemented effective for example in IoT systems to ensure its security and privacy (Fig. 7).

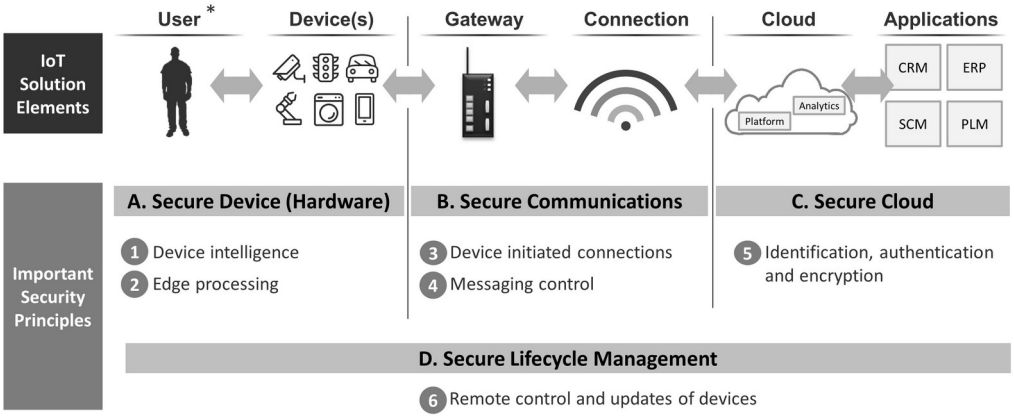

Figure 7. Principles of IoT cybersecurity

Encryption is an effective countermeasure, and the IoT is now required to apply encryption to sensor devices in environments with various restrictions that have not previously been subject to encryption (Fig. 8). Lightweight cryptography is a technology researched and developed to respond to this issue. The biggest security-related threat of IoT systems from the traditional IT systems is that even using devices for data collection from the real world can become a target of cyberattacks. For example, the purpose of applying IoT to a plant is to significantly improve the productivity and maintainability by collecting data from a large number of sensors installed in production equipment, by analyzing it and performing autonomous control in real time. If sensor data should be falsified during this process, incorrect analysis results would be induced and erroneous control would result due to such an occurrence having the potential of leading to major damage. Moreover, since measurement data and control commands are trade secrets associated with the know-how of production and management, preventing leakages is also important from the viewpoint of competitiveness. Even if there is no problem at present, it is necessary to consider the effect of threats that might become evident in the future. Applying encryption to sensor devices means the implementation of data protection for confidentiality and integrity, which can be an effective countermeasure against the threats. Lightweight cryptography has the function of enabling the application of secure encryption, even for devices with limited resources [6].

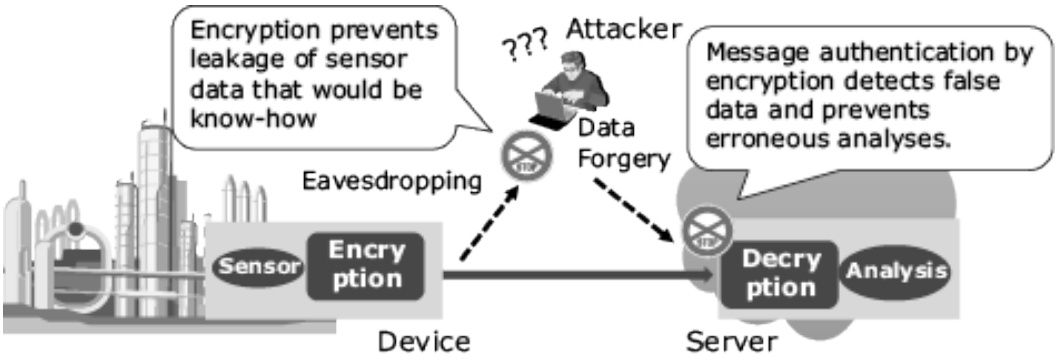

Figure 8. Encryption in IoT

Encryption is already applied as standard on the data link layer of communication systems such as the cellphone. Even in such a case, encryption in the application layer is effective in providing end-to-end data protection from the device to the server and to ensure security independently from the communication system. Then encryption must be applied at the processor processing the application and on unused resources and hence should desirably be as lightweight as possible (Fig. 9).

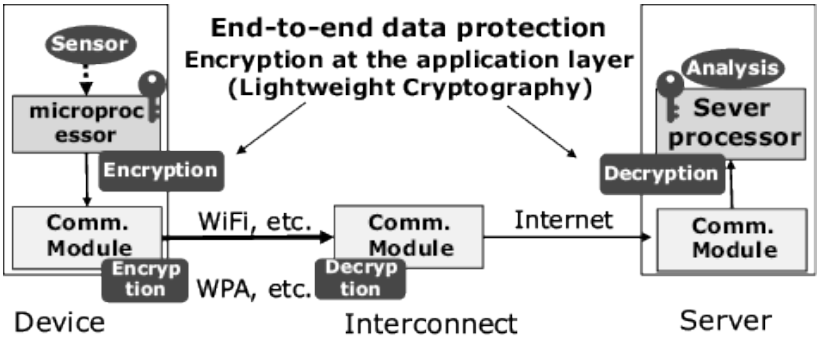

Figure 9. Lightweight encryption in IoT

The symmetric key cryptography uses the same secret key for encryption and decryption. With the processing that is relatively lightweight, it is used in data encryption and authentication. On the other hand, public key cryptography uses a secret key in decryption and a public key different from the secret key in encryption, and it is quite difficult to guess the secret key from the public key. The computational complexity of the public key cryptography is typically as high as more than 1,000 times that of the symmetric key cryptography, but this technology is used in sharing the secret key used in symmetric key cryptography and the digital signature, thanks to the asymmetrical property. With a system such as a plant or car- control system, it may be possible to embed the secret keys shared by the devices in advance. In such a case, secure and efficient data protection can be implemented using symmetric key cryptography alone. On the other hand, with a system that performs encrypted communications dynamically with unspecified parties such as an inter-vehicle communication system, the use of public key cryptography is effective. Symmetric key cryptography can be widely applied to devices that are subject to severe resource restrictions. The symmetric key cryptography consists of core functions such as block or stream ciphers (cryptographic primitives) and methods to apply the core function to a packet called the block cipher mode of operation for encryption and/or authentication.

Today there are many standardized algorithms of lightweight cryptography:

- ISO/IEC 29192-1:2012 Information technology — Security techniques — Lightweight cryptography — Part 1: General
- ISO/IEC 29192-2:2019 Information security — Lightweight cryptography — Part 2: Block ciphers
- ISO/IEC 29192-3:2012 Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers
- ISO/IEC 29192-4:2013 Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques

- ISO/IEC 29192-5:2016 Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions
- ISO/IEC 29192-6:2019 Information technology — Lightweight cryptography — Part 6: Message authentication codes (MACs)
- ISO/IEC 29192-7:2019 Information security — Lightweight cryptography — Part 7: Broadcast authentication protocols

4. Conclusions

In this paper the analysis of quantum technologies was carried out. It was declared that QKD is most implemented quantum technology in both laboratory (experimental) and commercial sector. Modern QKD protocols were analyzed as well as advantages / disadvantages were defined.

Also it was declared, that QKD protocols can be used in complex with lightweight encryption for data privacy in modern information and communication systems (for example, IoT). To provide high security level lightweight algorithms can be changed on secure post-quantum algorithms [7,8].

REFERENCES

1. Gnatyuk S. Advanced Technologies of Quantum Key Distribution, Monograph, London, Great Britain : InTech, 2018, 227 p. DOI: 10.5772/65232
2. Korchenko O., Vorobiyenko P., Vasiliu Ye., Gnatyuk S. elecommunications Networks: Current Status and Future Trends, Monograph [edited by Jesus Hamilton Ortiz], Rijeka, Croatia : InTech, 2012, 446 p.
3. Z. Hu, S. Gnatyuk, T. Okhrimenko, V. Kinzeryavyy, M. Iavich, Kh. Yubuzova, High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits, CEUR Workshop Proceedings, Vol. 2393, pp. 810-821, 2019.
4. Gnatyuk S., Okhrimenko T., Azarenko O., Fesenko A., Berdibayev R. Experimental Study of Secure PRNG for Q-trits Quantum Cryptography Protocols, Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT 2020), Kyiv, Ukraine, May 14, 2020, pp. 183-188.
5. Labadze G., Iavich M., Iashvili G., Gagnidze A., Gnatyuk S. Post-quantum digital signature scheme with BB84 protocol, CEUR Workshop Proceedings, Vol. 2915, pp. 35-44, 2021.
6. Iavich M., Kuchukhidze T., Gnatyuk S., Fesenko A. Novel certification method for quantum random number generators, International Journal of Computer Network and Information Security, Volume 13, Issue 3, pp. 28-38, 2021.
7. Iavich M., Gnatyuk S., Arakelian A., Iashvili G., Polishchuk Y., Prysiazhnyy D., Improved Post-quantum Merkle Algorithm Based on Threads, Advances in Intelligent Systems and Computing, Vol. 1247 AISC, pp. 454-464, 2021.
8. M. Iavich, S. Gnatyuk, G. Iashvili, A. Fesenko. Cyber security European standards in business. Scientific and Practical Cyber Security Journal (SPCSJ), 3(2):36-39, 2019