DOI: 10.18372/2410-7840.25.17593
УДК 681.3.06

JUSTIFICATION OF DIRECTIONS FOR IMPROVING AUTHENTICATION PROTOCOLS IN INFORMATION AND COMMUNICATION SYSTEMS

Alla Havrylova, Yuliia Khokhlachova, Andrii Tkachov, Natalia Voropay, Vladyslav Khvostenko

The analysis of information about the conducted cyber-threats makes it possible to identify modern information security problems when transmitted through unprotected communication channels. When conducting such an analysis, various components of the methods of implementing cyber threats are considered, but in this paper, it is proposed to pay attention to the motivational component of the emergence of threats and the existing effective tools for countering them. Such a comprehensive approach will make it possible to predict various modes of cyberattacks that cybercriminals can use against certain systems and to prepare the necessary digital security systems for the implementation of future threats. The influence of the exponential growth of the capacities of computing devices on the growth of the possibilities of implementing attacks by cybercriminals on cryptographic algorithms was also revealed. In this regard, the work considered the possibilities of increasing the level of resistance to such interventions, which are ensured by the NIST requirements for stability and security in the conditions of the post-quantum period. To determine the level of security of data transmission over an insecure network with privacy, integrity and authentication, a comparative analysis of the capabilities of information transmission protocols was conducted. The results of the analysis are presented in the form of a scheme of security and stability of protocols and algorithms that made it to the finals of the NIST competition. To ensure the integrity and authenticity of users when establishing communication sessions with websites, it is recommended to use TLS protocols. A scheme of the process of authenticated encryption and verification of the authenticity of an encrypted message transmitted using a TLS connection has been developed. The process diagram of authentication encryption and decryption of information when establishing a communication session in TLS protocols has been developed. A comparative analysis of different versions of TLS protocols was carried out.

Keywords: *authentication, TLS protocols, cyber threats, NIST, methods of implementing cyber threats.*

INTRODUCTION

Digital computing has increased productivity, efficiency and communications in business. However, this has led to the emergence and constant growth of cyber-attacks, which are the main threats to information security. All users of information and communication networks and systems must protect data and online assets from hackers and cyber attackers.

A cyber threat or threat to cyber security is a malicious act by cyber criminals. The goal of such attackers is to damage data, steal business data or disrupt the operation of digital business systems. Cyber threats are aimed at organizing data leaks, spreading computer viruses, conducting denial-of-service (DoS) attacks, and phishing. But business is not the only field for cyber threats. Not only legal entities of the state and non-state levels, but also private individuals are under the crosshairs.

The largest share of crimes committed with the help of Internet networks falls on the public and financial sectors. Today's advanced information technologies show interest not only out of scientific interest or in search of solutions to the most important problems of humanity, but also through the search for ways to get rich quickly at the expense of individuals, various levels of business structures, for conducting remote espionage and for causing damages due to unauthorized access to critical infrastructure, data, as well as distortion and theft of information.

METHODS AND MATERIALS

Formulation of the problem. The main task is to analyze the requirements for maintaining a certain level of information security in modern information and communication systems and networks in accordance with the existing threats of the post-quantum period and the use of TLS/SSL protocols to ensure the reliability and security of transmitted data.

RESULTS

Problems of information security in modern information and communication systems and networks. When analyzing threats to information security in relation to systems and networks, it is necessary to consider not only the methods of implementing cyber threats, but also the motivational component of their occurrence and the existing effective tools for countering them (Fig. 1).

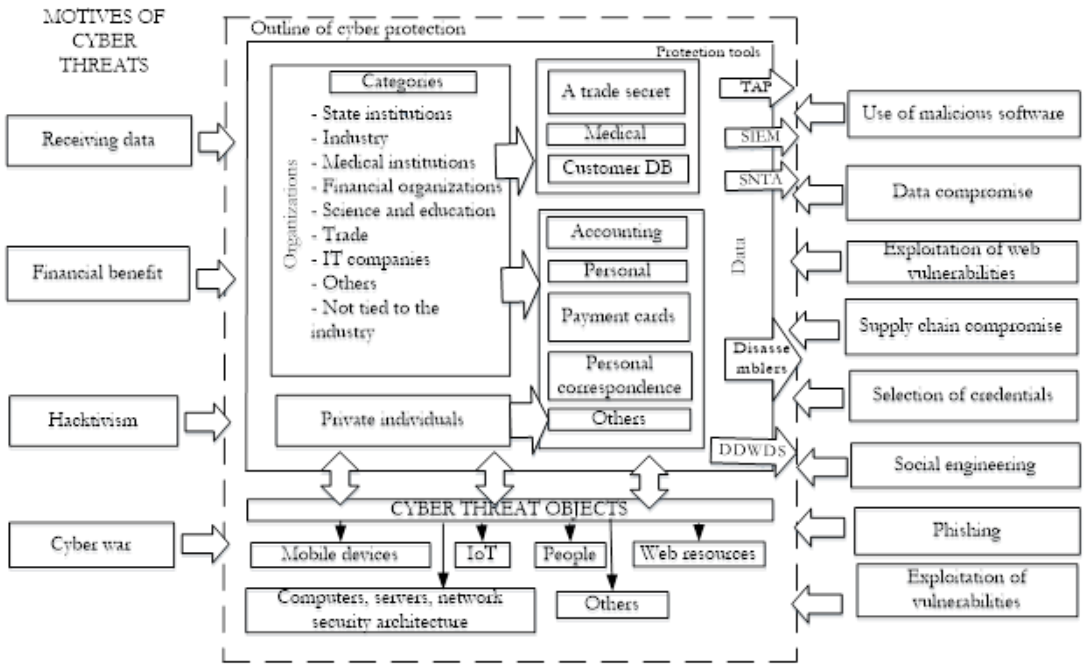

Fig. 1. Structural diagram of the cyber environment of information security threats in information and communication systems according to the motivational component

Such a comprehensive approach will make it possible to predict various modes of cyberattacks that cybercriminals can use against certain systems and to prepare the necessary digital security systems for the implementation of future threats.

It can be seen from the scheme that, depending on the motivational component of cyber threats, attackers use a number of methods of carrying out cyber-attacks. Thus, the motive for obtaining data is implemented mainly through the use of malicious software, phishing, exploiting web and other types of vulnerabilities and social engineering methods, obtaining financial benefits - using social engineering methods and data compromise and the supply chain, hacktivism – the use of web vulnerabilities, the selection of credentials and phishing, the purpose of the motive of "cyber war" is realized with the help of - malicious software.

In fig. 1 also provides effective tools for maintaining the cyber security contour, with the help of which you can identify and warn against cyber threats even before they occur. This list is currently represented by the tools of intellectual analysis of cyber threats:

• SIEM tools, which provide management of security information and events, which allows you to silently monitor the network of cloud computing, intranet, Internet and servers; in case of detection of anomalies, immediate detection of the hacker is ensured;

• Malware Disassemblers are used to reverse engineer malware, which helps to figure out how the malware works and creates defenses against all malware that works in a similar way;

• threat analysis platforms (TAP), which are intelligent open-source projects designed to collect data worldwide and post it on a web portal to gather information about the latest hacks and how to overcome such hacks;

• software for network traffic analysis (SNTA), which helps collect network usage data to be able to clean such massive data using big data and machine learning and find patterns while monitoring the network;

• Deep and Dark Web Data Scrubbers (DDWDS) are used to collect data on what regularly happens in the digital underworld commonly known as the dark web.

Considering the current circumstances, the safety of critical infrastructure facilities comes first. Therefore, it is necessary not only to protect them from a physical point of view, but also to consider the

possibilities of increasing the security of information transmission through unprotected channels with the help of cryptographic protection.

According to the conducted studies [1, 2] regarding the spheres of activity targeted by cyber threats and the frequency of use of methods of implementing these threats for the period from the beginning of 2022, the following was found.

1. The largest number of methods of implementing threats to information security was aimed at such sectors as medicine, science and education, as well as trade; the smallest number was characteristic of state bodies, private individuals, industry and financial institutions (Fig. 2).

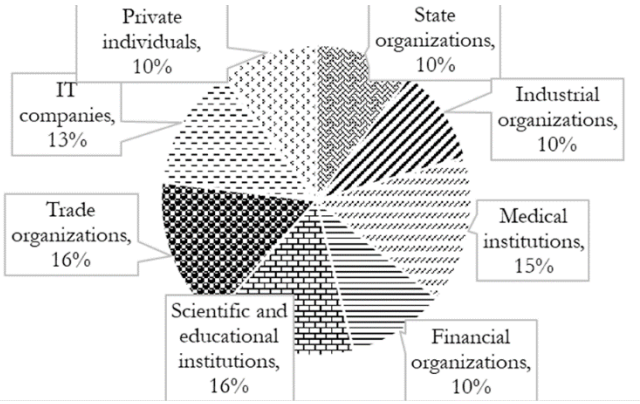

Fig. 2. Distribution of categories of users by the number of methods of implementing threats to their cyber protection systems in 2022

This is explained primarily by the fact that cybercriminals are increasingly interested in realizing their motives through cyber defense systems with less protected perimeters, and therefore cheap implementation.

2. Malicious software and social engineering methods occupy the first place in terms of the frequency of use of methods of implementing cyberthreats (Fig. 3). The supply chain compromise method was used the least.

Considering the current circumstances, the safety of critical infrastructure facilities comes first. Therefore, it is necessary not only to protect them from a physical point of view, but also to consider the possibilities of increasing the security of information transmission through unprotected channels with the help of cryptographic protection.

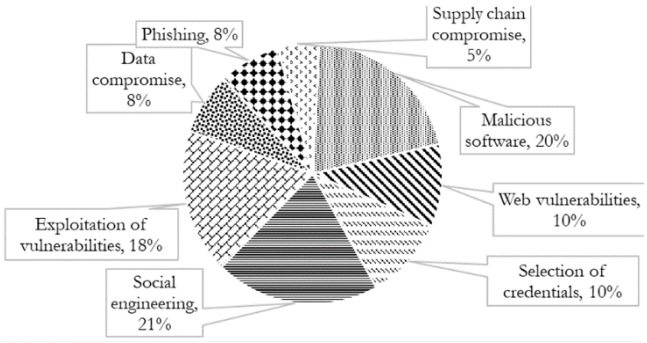

Fig. 3. Frequency of use of cyber threat implementation methods in 2022

Requirements for the prevention and impossibility of cyberattacks

According to the trends of exponential growth of the capacities of computing devices, cybercriminals have an increasing opportunity to implement attacks on cryptographic algorithms that ensure the stability of security services. This is also confirmed by research in the field of post-quantum cryptography by specialists of NIST (National Institute of Standards and Technology) of the USA (Report on Post-Quantum Cryptography) [3-5].

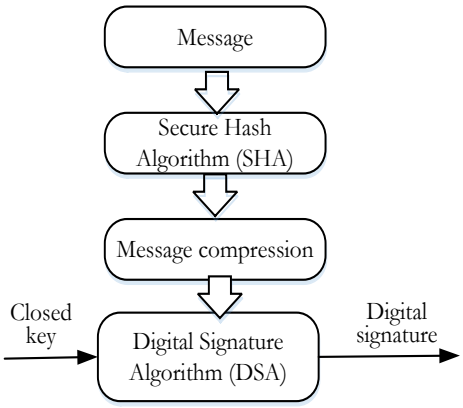

Fig. 4. Algorithm for creating a digital signature according to the DSS standard

They note that the emergence of full-scale quantum computers calls into question the crypto-resistance of asymmetric cryptography algorithms, and in February 2019, NIST experts, during the opening of a post-quantum cryptography competition, said that elliptical algorithms are also being questioned curves [6-9].

The main requirements of NIST relate to stability and security in the conditions of the post-quantum period [10]. Thus, according to safety requirements, it is recommended to use the following standards [6, 7].

I. As an electronic signature standard, use DSS (Digital Signature Standard) [6], which was adopted in America and is based on the FIPS-186 document and the DSA (Digital Signature Algorithm) algorithm (Fig. 4, 5).

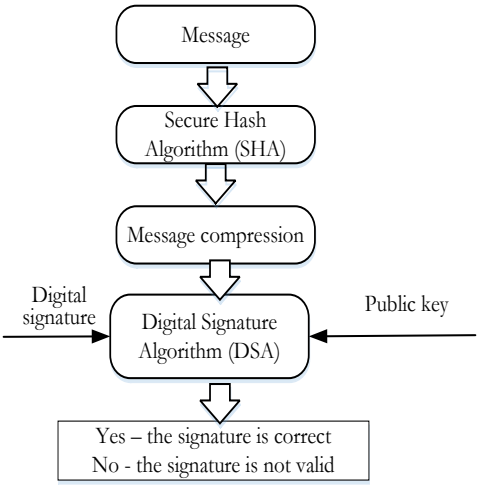

Fig. 5. Algorithm for verification of digital signature according to the DSS standard

DSA (Digital Signature Algorithm) refers to algorithms using a public key to create an electronic signature. The signature is created secretly, but can be publicly verified. This means that only one subject can create a message signature, but anyone can verify its correctness. The algorithm is based on the computational complexity of taking logarithms in finite fields.

The algorithm was proposed by NIST in August 1991 and is patented by the U.S. Patent 5231668, but NIST has made this patent available for use without license deductions. Algorithm together with the cryptographic hash function SHA-1 is part of the DSS (Digital Signature Standard), first published in 1994 (FIPS-186 (Federal Information Processing Standards) document). Later, 2 updated versions of the standard were published: FIPS 186-2 (January 27, 2000) and FIPS 186-3 (June 2009) [11].

II. As key distribution standards, use the instructions for pair-wise establishment of keys SP 800-56A (Fig. 6) and two-way confirmation of keys SP 800-56B (Fig. 7) (Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography) [9].

According to fig. 6 the SP 800-56A standard defines keying schemes based on the problem of discrete logarithms over finite fields and elliptic curves, including several variations of Diffie-Hellman and Menezes-Kuvanston (MQV) keying schemes.

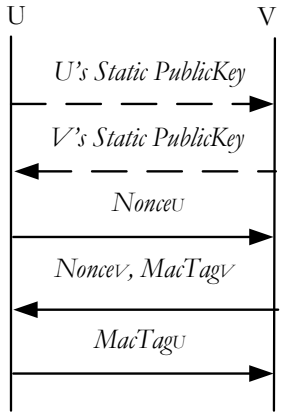

Fig. 6. Paired key installation scheme by SP

U/V – sender/receiver of the message; PublicKey – public key; NonceU, NonceU – temporary U/V label; MacTagU/MacTagV – U/V integrity and authentication code.

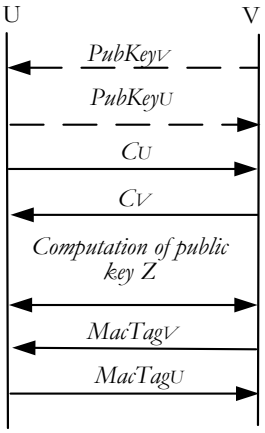

Fig. 7. Scheme of two-way confirmation of keys according to SP 800-56B

U/V – sender/receiver of the message; PubKeyU, PubKeyV – U/V public key; CU/CV – encrypted text U/V; Z is a common key for U and V; MacTagU, MacTagV – integrity confirmation code and U/V authentication.

III. Use of the new standard in protocols: TLS, SSH, IPSec [8]:

1) TLS (protocol for secure data transfer over a secure network with privacy, integrity and authentication) (Fig. 8) – the new TLS 1.3 standard.

2) SSH using keys (Fig. 9).

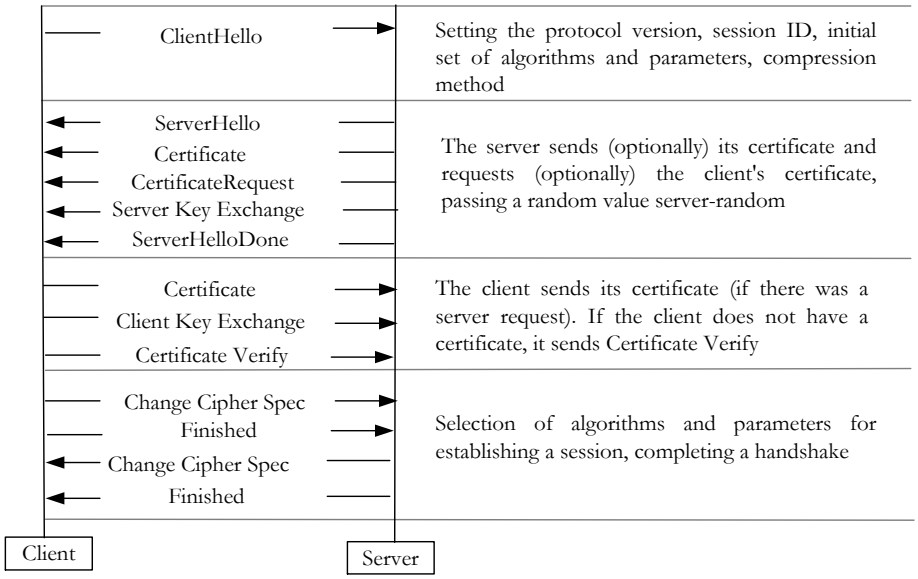

Fig. 8. Scheme of the implementation of the exchange of notifications in the information and communication network using the TLS protocol

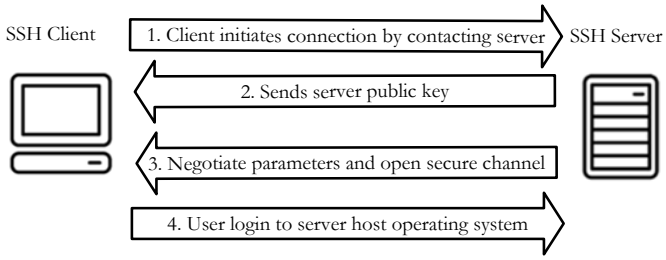

Fig. 9. Implementation scheme of information exchange using the SSH secure access protocol for remote systems

SSH is a protocol for secure access to remote systems. Basically, SSH is used to access servers, for remote access to a console, a terminal, to a command interpreter of a remote machine (mainly a Linux operating system, but it can also be another network equipment or even a device with a Windows operating system). The use of keys has a number of security-related advantages: they are difficult to break (the sufficient length of the key ensures stable cryptoresistance to brute-force or dictionary matching attacks); when using keys, no private information is stored on the server.

1) IPSec – network traffic protection protocol (Fig. 10), which, despite its excessive complexity and redundancy, has a number of important properties that allow ensuring the required level of security:

hardware independence; no need to change code for applications.

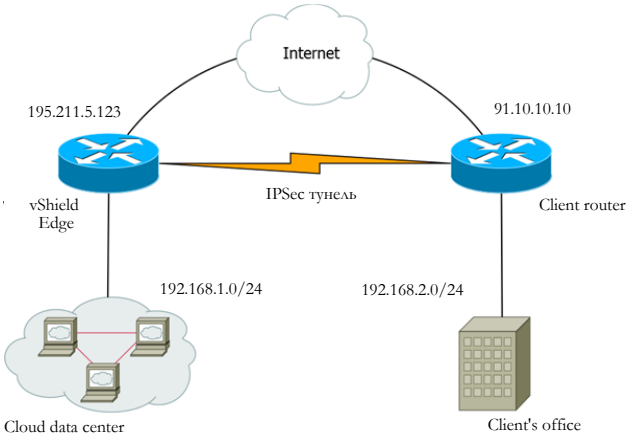

Fig. 10. Scheme of implementation of communication according to the IPSec network traffic protection protocol

The IP package provides full protection, including protection for higher-level protocols; packet filtering based on authenticated headers, sender and receiver addresses, which provides simplicity and low cost, is suitable for routers; transparent to users and applications.

The IP package provides full protection, including protection for higher-level protocols; packet filtering based on authenticated headers, sender and receiver addresses, which provides simplicity and low

cost, is suitable for routers; transparent to users and applications.

IV. Security model of post-quantum asymmetric encryption algorithms IND-CCA2 [8] (Fig. 11).

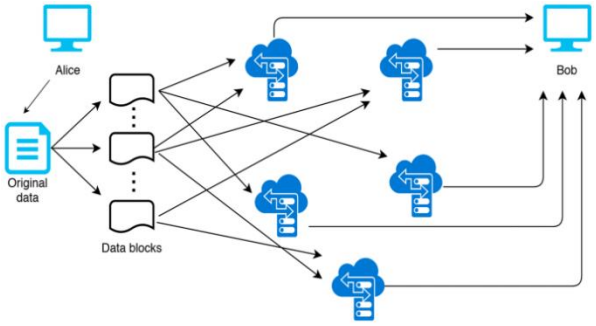

Fig. 11. Security model of post-quantum asymmetric encryption algorithms IND-CCA2 for message exchange between communication participants

IND-CCA2 is a security model of indistinguishability during an attack based on an adaptively selected ciphertext.

The indistinguishability (uncertainty) of the encrypted text is an important security property of many encryption schemes.

If the cryptosystem has the property of indistinguishability, then the thief will not be able to distinguish pairs of encrypted texts based on the message that they encrypt [12, 13, 14].

V. Security model of post-quantum digital signatures.

As a NIST standard today, it is proposed to use the EUF-CMA model as a security model for post-quantum signatures (Fig. 12, 13).

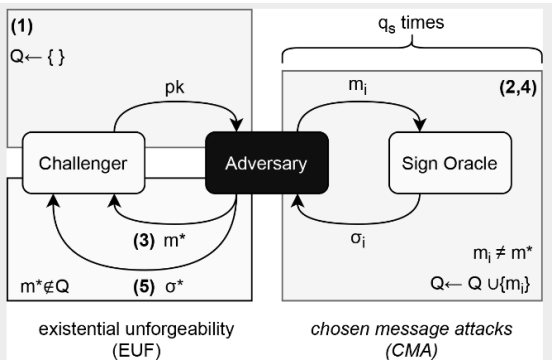

Fig. 12. Formalized EUF-CMA security model

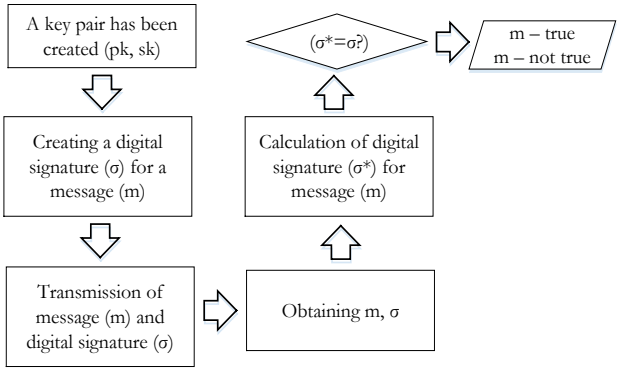

Fig. 13. Functional presentation of the EUF-CMA security model

EUF-CMA determines existential non-forgery from attacks based on adaptively selected messages. In particular, security under EUF-CMA does not allow a cryptanalyst to produce a signature for key-dependent messages, for example, a signature when using a full private sk key. If there is at least one key-dependent message request, the security of the signature mechanism is broken [14-18].

There are two general formal definitions for the security of a digital signature scheme. Each of these definitions is presented as a "game" or experiment that is performed between an attacker and some honest challenger. EUF-CMA is based on the theory of mathematical models of making optimal decisions in conflict conditions. Since the parties involved in most conflicts are interested in hiding their own intentions from the enemy, decision-making in conflict occurs in conditions of uncertainty. The main property of this model is that the attacker will not be able to pick up the signature [16, 19].

VI. Security model of post-quantum key encapsulation protocols. The CK model includes three main components: the unauthenticated intruder model (UM), the authenticated intruder model (AM) and the authentication mechanism (authenticator) (MT). The CK security model is used for authentication of key exchange (AKE) [15, 20]. The CK model concerns the security of the session key used in a communication session. It is evaluated using a formal model for key exchange protocols and the capabilities of cryptanalysts. The concept of session key security (or SK-security) aimed at ensuring the security of individual session keys. Its violation is a compromise of the session key. In the case of key security, an attacker "knows nothing about the value of the key" when he

intercepts the data of the key exchange protocol and performs attacks on other sessions and interacting parties.

VII. The distributed scheme of "semantic secure encryption" SEM-CPA [5].

Semantic security is a concept that describes the security of an encryption scheme and captures the idea that a secure encryption scheme must hide all information about unknown plaintext. The attacker is allowed to choose between two plaintexts m0 and m1, and he receives the encryption of any of the plaintexts. An encryption scheme is semantically secure if the thief cannot guess with a probability better than 0.5 whether this ciphertext is an encryption of the message m0 or m1. Semantic security requires that what can be efficiently computed for some plaintexts from their ciphertexts can be computed just as easily in the absence of those ciphertexts.

This scheme is intended to consider the use of such encryption algorithms that support a cryptographic system in which only insignificant information about the plaintext can be extracted from the encrypted text. Semantically safe encryption algorithms are the Goldwasser-Mikali algorithm (Fig. 14), the El Gamal algorithm (Fig. 15) and the Peyer algorithm (Fig. 16).

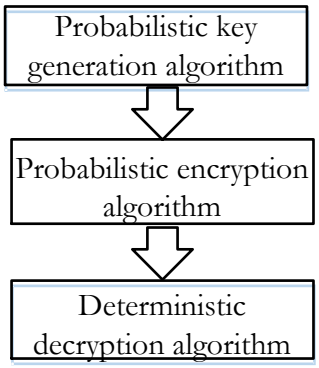

Fig. 14. Goldwasser-Mikali encryption algorithm

These schemes are considered provably secure, since their semantic security can be reduced to the solution of some complex mathematical problem (for example, Deterministic Diffie-Hellman or Quadratic finality problem).

At the same time, the security criterion is the attacker's access to less than 264 selected cipher-text-key pairs.

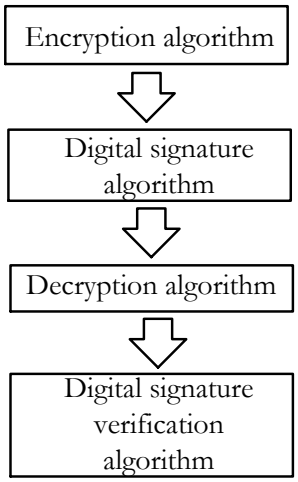

Fig. 15. El Gamal encryption algorithm

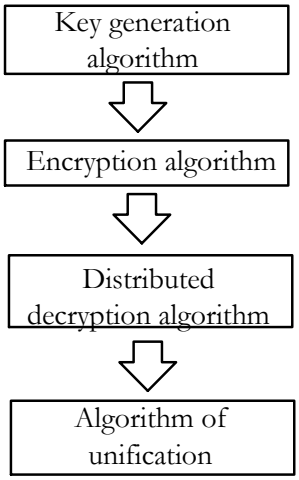

Fig. 16. Peyer encryption algorithm

Regarding the requirements regarding stability, the following is recommended [6].

I. 128 bits of classical security / 64 bits of quantum security, providing AES-128 margin of resistance.

II. 128 bits of classical security / 80 bits of quantum security, providing SHA-256 / SHA3-256 / SHA-384 / SHA3-384 robustness margin.

III. 256 bits of classical security / 128 bits of quantum security, providing AES-256 stability margin.

At the same time, the stability criterion is the MAXDEPTH parameter, in which quantum attacks are limited by a set of fixed operating times, or the depth of the circuit:

- 240 logical gates, i.e. the approximate number of gates, which will be performed consistently per year;

- 264 logic gates, which modern classical computing architectures can perform consecutively in ten years;

- no more than 296 logic gates, that is, the approximate number of gates that atomic-scale qubits with the speed of light can perform in a millennium.

Thus, NIST suggests considering the following models:

- for symmetric cryptography algorithms – under the conditions of the IND-CCA2 (Indistinguishability Adaptive Ciphertext Attack) security model, which determines resistance to an adaptive attack based on the selected text cipher;

- for an electronic digital signature – under the conditions of the EUF-CMA security model (existentially unforgeable under adaptive chosen message attacks);

- for the key encapsulation protocol – under the conditions of the Canetti-Krawczyk security model (SK-security).

To provide a secure key encapsulation mechanism in the III round of NIST, the CRYSTALS-Kyber algorithm (Fig. 17) was chosen, which is based on asymmetric encryption and the Fujisaki-Okamoto transformation [25].

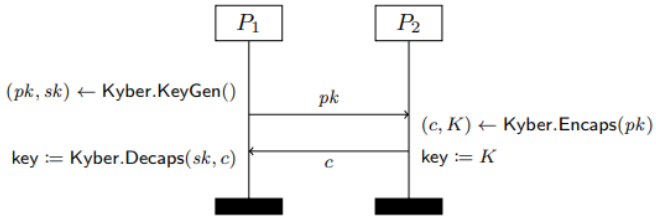

Fig. 17. Scheme of the key exchange protocol when using the CRYSTALS-Kyber algorithm

This algorithm describes a direct application of the key encapsulation mechanism. At the same time, the public key pk is hashed into the "preliminary key" K, and the encrypted text is hashed into the final key K. Then, the common key obtained during the exchange of keys already includes the full "presentation" of each participant.

In addition to CRYSTALS-Kyber, four more general-purpose key encapsulation algorithms have been identified - BIKE [21], Classic McEliece [22], HQC [23] (built on error-correcting codes) and SIKE (built on isogenies), which, provided elimination of identified shortcomings, may be included in the finalists.

Universal algorithms left for further development are based on other principles: BIKE and HQC used elements of algebraic coding theory and linear codes, which are also used in error correction schemes. NIST intends to further standardize one of these algorithms for the lattice theory alternative CRYSTALS-Kyber. The SIKE algorithm [24] is based on the use of supersingular isogeny (rotation in a supersingular isogenic graph) and is also considered as a candidate for standardization, as it has the smallest key size. But as of August 3, 2022, the SIKE post-quantum encryption algorithm was cracked using an ordinary computer in just one hour [26].

In the table 1 shows the characteristics of key encapsulation algorithms selected for comparison, which are based on algebraic lattices and mathematical codes [27].

Table 1

Characteristics of key encapsulation algorithms on algebraic lattices and mathematical codes

Algorithm	The length of the public key, bytes	The length of the private key, bytes	The length of the crypto-conversion result, bytes	Speed of direct crypto-conversion, operations/ms	Speed of reverse crypto-conversion, operations/ms
CRYSTALS-KYBER	5 422	5 422	5 422	2 112 734	15 843 611
BIKE	9 034	9 034	9 034	1 967 128	43 842 551
Classic McEliece	8 188	8 188	8 188	1 786 760	37 247 437
HQC	1 440	3 168	1 504	3 529 138	2 703 872

From the given data in the table, it can be concluded that among the advantages of the CRYSTALS-KYBER algorithm, relatively small encryption keys that are easy to exchange, as well as high speed of operation, can be singled out. The proof of resistance to attacks is built considering the assumptions of the complexity of the tasks, which are proven to be difficult. From a mathematical point of view, it is assumed that with an increase in the size of the lattice, which is necessary for solving these problems, the time will increase exponentially. Therefore, lattice tasks are considered resistant to attacks using a classical computer. However, the question of resistance to quantum attacks remains open.

From 69 algorithms aimed at working with digital signatures, CRYSTALS-Dilithium [28], FALCON [29] and SPHINCS+ [30] were singled out, the existing versions of which are listed in the table. 2.

Table 2

Characteristics of versions of digital signature algorithms on algebraic lattices and mathematical codes

Algorithm	The length of the public key, bytes	The length of the private key, bytes	The length of the crypto-conversion result, bytes	Speed of direct crypto-conversion, operations/ms	Speed of reverse crypto-conversion, operations/ms
CRYSTALS-Dilithium 2	1 184	2 800	2 044	1 355 434	327 362
CRYSTALS-Dilithium 3	1 472	3 504	2 701	2 348 703	522 267
CRYSTALS-Dilithium 5	1 760	3 856	3 366	2 856 803	871 609
Falcon 512	1 793	8 193	1 330	5 948.1	27 933.0
Falcon 768	897	4 097	690	-	-
Falcon 1024	1 441	6 145	1 077	2 913.0	13 650.0
SPHINCS+ (SHA-256)	64	128	33 408	527 413 100	5 463 884

Rigorous stability justification is given only in the CRYSTALS-Dilithium and SPHINCS+ schemes. But they assume of the complexity of a number of tasks, the complexity of which has not been proven. Of all the finalists, the SPHINCS+ algorithm is the most difficult to implement, the speed of operation is low. However, this algorithm was left as a backup option, since it is the only one built on a different mathematical basis - on the basis of hash functions, and not lattices. The CRYSTALS-Dilithium and FALCON algorithms are highly efficient. CRYSTALS-Dilithium was recommended as the primary algorithm for electronic digital signatures, FALCON is focused on solutions that require a minimum signature size. SPHINCS+ lags behind the first two algorithms in terms of signature size and speed, but was retained among the finalists as a fallback.

The CRYSTALS-Kyber, CRYSTALS-Dilithium, and FALCON algorithms used cryptography methods based on the solution of lattice theory problems, the solution time of which does not differ on conventional and quantum computers. The SPHINCS+ algorithm uses cryptography techniques based on hash functions.

Analysis of the use of TLS/SSL protocols to ensure the reliability and security of data in modern information and communication systems and networks

When using the protocols of the TLS/SSL family to ensure secure data transmission over an insecure network with privacy, integrity, and authentication, their architecture consists of 2 protocols [12].

I – handshake protocol (purpose – authentication and key exchange), on which the Client and the Server perform the following procedures:

- agree on the version of the protocol;
- select a cryptographic algorithm or cipher suite;
- authenticate each other using asymmetric cryptography;

• define the shared secret that will be used for symmetric encryption at the next level.

II – recording protocol. At this level, the following procedures are performed:

• all outgoing messages are encrypted using the secret key set during the handshake;

• encrypted messages are transmitted from the Client to the Server;

• the server checks received encrypted messages for changes;

• if there are no changes, the encrypted messages are decrypted using the secret key.

To ensure that the encrypted message has not been modified during transmission, TLS protocols use authenticated encryption (Fig. 18).

From the above diagram, it can be seen that the authenticated encryption of a user's message consists of three processes.

The first process is encryption. The sender's text message (M) goes through a symmetric encryption algorithm (AES-256-GCM or CHACHA20). This encryption algorithm also takes as input a shared secret key (K) and a randomly chosen nonce (nonce) or initialization vector (IV). It will return an encrypted message.

The second process is authentication. The unencrypted message (M), secret key (K), and nonce/IV become input to the MAC algorithm, (GCM for AES-256, or POLY1305 for CHACHA20). This MAC algorithm behaves like a cryptographic hash function and produces a MAC (Message Authentication Code) as the output.

Moreover, according to the AES-256-GCM algorithm, the security level of the hash function corresponds to the security level of the keys; however, unlike other modes, SHA-384 is used. More "heavyweight" keys make this cipher somewhat slower, but it is keys of this size that have the advantage of being secure, even if a sufficiently powerful quantum computer is used. ChaCha20-POLY1305, on the other hand, is an algorithm that takes 512 bits as input and outputs 512 bits in a way that makes it extremely difficult to determine what the input was, and which ensures that each of the output bits is affected by each bit applied to the input. The technique is to create a block with a 256-bit key, a 128-bit constant, and a 128-bit mix of counter value with a value that is used only once.

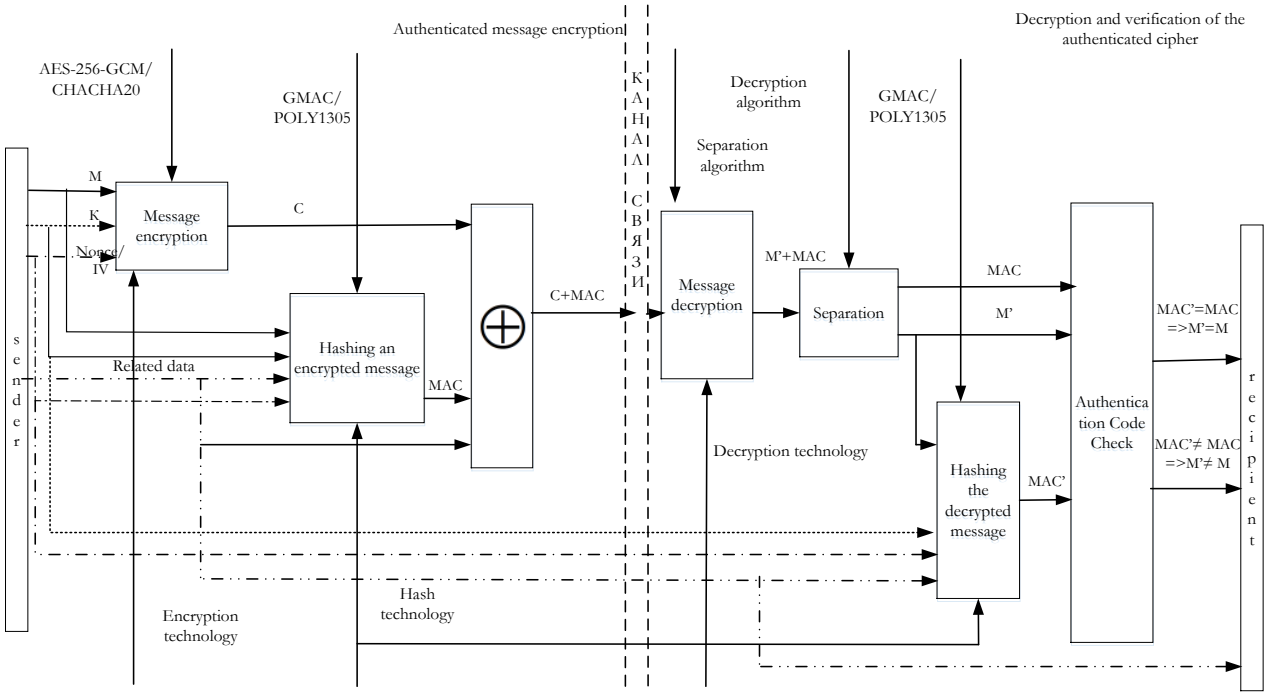

Fig. 18. Scheme of the process of authenticated encryption and authentication of an encrypted message transmitted over a TLS connection

The third process is MAC concatenation and encrypted message (C). The result is sent to the transmission channel and delivered to the recipient (authentication tag).

In TLS 1.3, in addition to the encrypted message, related data is authenticated: addresses, ports, protocol version, or sequence number. This information is not encrypted and is known to both parties.

As such, the associated data is also an input to the MAC algorithm, and because of this, the whole process is called Authenticated Encryption with Associated Data, or AEAD for short.

Deciphering an authenticated message and verifying that it has not been altered during transmission consists of four processes.

The first process is the decryption of the encrypted message (C).

The second process is separation. The decrypted message (M') is separated from the authentication code (MAC).

The third process is hashing the decrypted message. The unencrypted message is sent to the MAC algorithm along with the shared secret (K) and nonce/IV.

The fourth process is checking the received hash code. The calculated authentication code (MAC') is compared with the received (MAC) and, if they match (MAC'=MAC), then the received and sent messages match (M'=M).

Thus, the TLS protocol provides both confidentiality and integrity in the transmission of encrypted data.

At this point in time, the current version of the Internet security protocol remains TLS 1.2. But, since work often takes place over a cellular connection, where high latency is possible, over time, a significant slowdown in the spread of the TLS 1.2 protocol began to occur. To replace it, a new version, TLS 1.3, is being put into operation.

The sequence of actions related to the authentication encryption of information (on the sender's side) and its decryption and verification (on the recipient's side) when establishing a communication session in the TLS 1.2 and TLS 1.3 protocols are shown in Fig. 19 and Fig. 20.

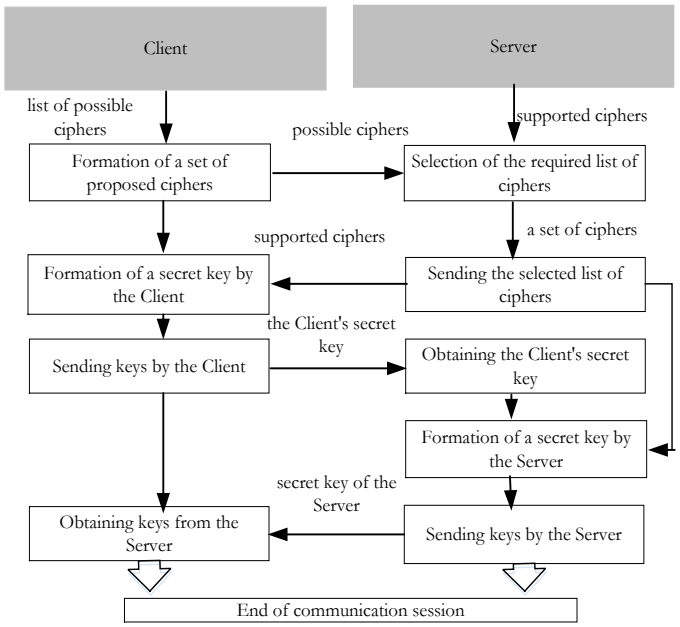

Fig. 19. Process flow diagram for authentication encryption and decryption using the TLS 1.2 protocol

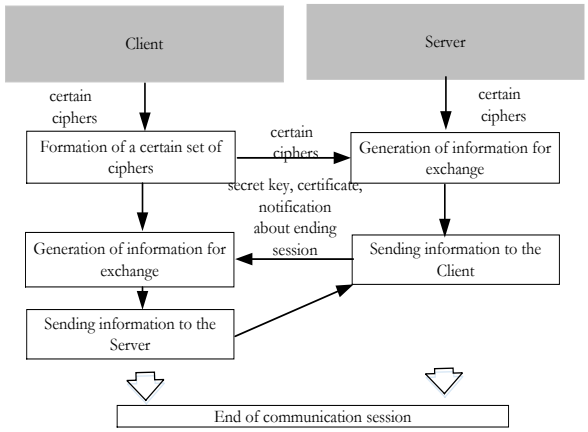

Fig. 20. Process flow diagram for authentication encryption and decryption using the TLS 1.3 protocol

According to the data presented in Fig. 19 and Fig. 20, the following can be distinguished:

1. TLS 1.3 contains more secure key exchange mechanisms, in which only the ephemeral Diffie-Hellman algorithm or the Elliptic Curve Diffie-Hellman algorithm remained. Thus, perfect forward secrecy is achieved, in contrast to the TLS 1.2 protocol.

2. The number of operations for conducting the handshake protocol in TLS 1.3 is at least one round-trip faster than in TLS 1.2.

3. Symmetric encryption in TLS 1.3 is more secure because the set of ciphers used is mandatory, and

it also removes some algorithms from the list that are easy to crack, such as Block Cipher Mode, RC4 or Triple DES.

4. The cipher suite in TLS 1.3 is also simpler as it only contains the AEAD and hashing algorithm.

5. Key exchange algorithms in TLS 1.3 and signatures are placed in separate fields, while in TLS 1.2 they are combined into a cipher suite.

6. The number of recommended cipher suites in TLS 1.2 is 37, while in TLS 1.3 there are 5.

7. In TLS 1.3, the signature is cryptographically more secure, since the entire handshake is signed, and not part of it, as in TLS 1.2.

8. TLS 1.3 pays significant attention to elliptic curve cryptography, adding several improved curve algorithms that are as fast as TLS 1.2 without compromising security.

CONCLUSION

Considering the current circumstances, the safety of critical infrastructure facilities comes first. Therefore, it is necessary not only to protect them from a physical point of view, but also to consider the possibilities of increasing the security of information transmission through unprotected channels with the help of cryptographic protection.

The conducted analysis showed that the use of an electronic digital signature based on asymmetric crypto-algorithms in the post-quantum period cannot provide a guaranteed level of crypto-resistance, and accordingly may be prone to a special type of attack based on a full-scale quantum computer.

The security schemes that exist today, despite their lengthy analysis and research, do not guarantee the same levels of security and stability in the post-quantum period as they do today. This may justify further research in the field of elliptic cryptography using and combining encryption systems with provable security.

REFERENCES

[1] Havrylova Alla, Khokhlachova Yulia, Pohorelov Volodymyr. Analiz zastosuvanna hibrydnyh krypto-kodovyh konstruktsiy dlia pidvyshenna rivna stiykosti hesh-kodiv do zlamu // Bezpeka informacii, 2022. T. 28, № 2. pp. 87-101. DOI: 10.18372/2225-5036.28.16953.

[2] Viyna v Ukraine. Puls Kiberzahystu // Derjavna slujba spetczviazku ta zahystu informacii, serpen 2022. URL: https: // www. ppl. org. ua / wp-content/uploads/2022/09/1662392024242416.pdf.

[3] Guide for Cybersecurity Event Recovery, 2022. URL: https: // nvlpubs. nist. gov / nistpubs /.../ NIST.SP.800-184.pdf.

[4] Security requirements for cryptographic modules, 2020. URL: https://csrc.nist. gov/publications/ fips/fips140-2/fips1402. pdf.

[5] Guide to LTE Security, 2020. URL: https: // csrc.nist.gov /publications/ drafts / 800-187/ sp-800_187_draft.pdf.

[6] Yevseiev S., Ponomarenko V., Laptiev O., Milov O. and others. Synergy of building cybersecurity systems: monograph. // PC TECHNOLOGY CENTER, Kharkiv, 2021. 188 p.

[7] Tsyhanenko O. Development of digital signature algorithm based on the Niederreiter crypto-code system. // Information Processing Systems, 2020. Issue 3 (162), pp. 86-94.

[8] Havrylova A. A. Analiz kryptografichnyh algorytmiv podanyh do tretiogo turu konkursy NIST // Artualni pytannia zabezpechennia slujbovo-boyovoi diyalnosti syl sectoru bezpeky i oborony: materialy vseukr. krug. stolu (m. Kharkiv, 23 kvit. 2021 r.), FOP Brovin O.V., 2021. Vyp. 5, pp. 361 - 365.

[9] Report on Post-Quantum Cryptography, 2022. URL: https://csrc.nist.gov /publications/detail/ nistir/8105/final.

[10] Post-Quantum Cryptography, 2018. URL: https:/ /csrc. nist. gov/ Projects / postquantum-cryptography/round-3-submissions.

[11] FIPS PUB 180-4, Secure Hash Standard (SHS), 2019. URL: https: // nvlpubs. nist. gov / nistpubs /FIPS/NIST.FIPS.180-4.pdf.

[12] Yesina M.V. Model bezpeky postkvantovyh protokoliv inkapsuliacii kluchiv // Prykladna radioelektronika, 2018. T. 17, № 3, 4. pp. 160-167.

[13] Ciphertext indistinguishability. URL: http://cse. iitkgp.ac.in/~debdeep/courses_iitkgp/FCrypto/scribes/scribe8.pdf.

[14] Yesina M. V. Modeli bezpeky postkvantovyh kryptografichnyh prymityviv // Matematychne ta komputerne modeluvannia. Seriya: Tehnichni naury, 2019. Vyp. 19. pp. 49-55. DOI: 10.32626/ 2308-5916.2019-19.49-55

[15] Horbenko Yu. I., Potiy O. V., Onoprienko V. V., Yesina M. V., Maleyeva H. A. Osnovni polojennia shodo modeli bezpeky dlia asymetrychnyh peretvoren typu z urahuvanniam vymoh ta zagroz postkvantovogo periodu // Radiotehnika. 2020.

Vyp. 202. pp. 28-36 DOI:10.30837 / rt.2020.3. 202.02 EUF-CMA and SUF-CMA.

[16] Haitner I., Holensteiny T. On the (im) possibility of key dependent encryption, in: TCC'09 // Theory of Cryptography, 6th Theory of Cryptography Conference, San Francisco, CA, USA, 2009, Lecture Notes in Comput. Sci. Vol. 5444, Springer, Berlin, 2009, pp. 202-219.

[17] Hofheinz D., Unruh D. Towards key-dependent message security in the standard model. EUROCRYPT'08//Advances in Cryptology, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, 2008, Lecture Notes in Comput. Sci. Vol. 4965, Springer, Berlin, 2008, pp. 108-126.

[18] Applebaum B., Cash D., Peikert C., Sahai A. Fast cryptographic primitives and circular-secure encryption based on hard learning problems// Advances in Cryptology – CRYPTO'09, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2009. Lecture Notes in Comput. Sci. Vol. 5677, Springer, Berlin, 2009. pp. 59-618.

[19] Bellare M. Symmetric encryption. URL: https:// cseweb.ucsd.edu/~mihir/-cse207/w-se.pdf.

[20] Ran Canetti, Hugo Krawczyk Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. URL: http://iacr.org/archive/ eurocrypt2001/20450451.pdf.

[21] BIKE: Bit Flipping Key Encapsulation, 2022. URL: https: // bikesuite. org / files /v4.1/ BIKE_ Spec.2020.10.22.1.pdf.

[22] Classic McEliece: conservative code-based cryptography, 2020. URL: https:// classic. mceliece. org /nist/mceliece-20201010.pdf.

[23] Hamming Quasi-Cyclic (HQC), 2020. URL: http://pqc-hqc.org/doc/hqcspecification_2020-10-01.pdf.

[24] David Jao. Supersingular Isogeny Key Encapsulation. URL: https: // csrc. nist. gov / csrc / media/ Projects / post - quantum - cryptography / documents/round-4/submissions/SIKE-spec.pdf.

[25] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, Damien Stehlé. CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM // 2018 IEEE European Symposium on Security and Privacy, 2018, pp. 353-367 URL: https: //research.ibm.com /publications/crystals-kyber-a-cca-secure-module-lattice-based-kem DOI 10. 1109/EuroSP. 2018.00032.

[26] Yesina M. V., Vdovenko S. H., Horbenko I. D. Modeli bezpeky postkvantovyh asymetrychnyh shyfriv na osnovi nerozriznuvasti // Zbirnyk naukovyh prac *JVI*, Kharkiv, 2019. Vyp. 16. C. 15-26. DOI: 10.46972/2076-1546.2019.16.02.

[27] Horbenko I. D., Kachko O. H., Ponomar V. A., Yesina M. V., Askolzina O. S., Kulibaba V. A. Analiz sutnosti ta modeli protokolu inkapsuliacii kluchiv u kilci polinomiv nad skinchenym polem // Prykladna radioelektronika, 2018. T. 17, № 3, 4. pp. 127-137.

[28] Sara Ricci, Lukas Malina, Petr Jedlicka, David Smékal, Jan Hajny, Peter Cibik, Petr Dzurenda, Patrik Dobias Implementing CRYSTALS-Dilithium Signature Scheme on FPGAs // ARES 21: Proceedings of the 16th International Conference on Availability, Reliability and SecurityAugust 2021 Article No.: 1, pp. 1-11 URL: https://dl.acm.org/ doi/fullHtml/10.1145/3465481.3465756.

[29] Fouque P. A. et al. Falcon: Fast-fourier lattice-based compact signatures over NTRU URL: https: //eprint.iacr.org/2021/772.pdf.

[30] Bernstein D., Dobraunig Christoph, Eichlseder Maria, Fluhrer Scott R., Gazdag S., Hülsing Andreas, Kampanakis Panos, Kölbl Stefan, Lange T., Lauridsen Martin M., Mendel Florian, Niederhagen R., Rechberger Christian, Rijneveld J., Schwabe P. SPHINCS + Submission to the NIST post-quantum project URL: https://www. semanticscholar.org/paper/SPHINCS-%2B-Submission -to-the-NIST-post-quantum-Bernstein-Dobraunig /d87c9542622bf5345da856959a0ae959d55ed6b6.

ОБГРУНТУВАННЯ НАПРЯМКІВ ВДОСКОНАЛЕННЯ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Аналіз інформації про проведені кіберзагрози дозволяє виявити сучасні проблеми безпеки інформації при передачі незахищеними каналами зв'язку. При проведенні такого аналізу враховують різні складові методів реалізації кіберзагроз, але в даній роботі за-пропоновано звернути увагу на мотиваційну складову виникнення загроз й існуючи дієві інструменти протидії їм. Такий комплексній підхід дозволить спрогнозувати різні режими кібератак, які кіберзлочинці можуть застосувати проти певних систем та підготувати необхідні цифрові системи безпеки при реалізації майбутніх загроз. Також було виявлено вплив експоненційного зростання потужностей обчислювальних пристроїв на зростання можливостей реалізації атак кіберзлочинцями на криптографічні алгоритми. У зв'язку з цим в

роботі були розглянуті можливості підвищення рівня протидії таким втручанням, які забезпечуються за допомогою вимог NIST до стійкості та безпековості в умовах постквантового періоду. Для визначення рівня безпековості передачі даних за не-безпечною мережею із забезпеченням приватності, цілісності та автентифікації, було проведено порівняльний аналіз можливостей протоколів передачі інформації. Результати аналізу представлені у вигляді схеми безпеки та стійкості протоколів та алгоритмів, які вийшли у фінал конкурсу NIST. Для забезпечення цілісності та справжності користувачів під час встановлення сеансів зв'язку з вебсайтами рекомендовано використовувати TLS-протоколи. Розроблено схему процесу автентифікованого шифрування та перевірки справжності зашифрованого повідомлення, що пере-дається за допомогою TLS-з'єднання. Розроблено процесну схему автентифікаційного шифрування та розшифрування інформації при встановленні сеансу зв'язку в протоколах TLS. Проведено порівняльний аналіз різних версій протоколів TLS.

Ключові слова: аутентифікація, TLS-протоколи, кіберзагрози, NIST, методи реалізації кіберзагроз.

Alla Havrylova, Senior Lecturer of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".
Гаврилова Алла Андріївна, старший викладач кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут".
E-mail: alla.havrylova@khpi.edu.ua.
Orcid ID: 0000-0002-2015-8927.

Yulia Khokhlachova, candidate of technical sciences, associate professor of the department of information technology security of the National Aviation University.
Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Andrii Tkachov, candidate of technical sciences, associate professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".
Ткачов Андрій Михайлович, кандидат технічних наук, доцент кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут".
E-mail: andrii.tkachov@khpi.edu.ua.
Orcid ID: 0000-0003-1428-0173.

Natalia Voropay, PhD in Engineering, associate professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".
Воропай Наталія Ігорівна, кандидат технічних наук, доцент кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут".
E-mail: voropay.n@gmail.com.
Orcid ID: 0000-0003-1321-7324.

Vladyslav Khvostenko, PhD in Economics, Associate Professor, patent attorney of Ukraine of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".
Хвостенко Владислав Сергійович, кандидат економічних наук, патентний повірений України, доцент кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут".
E-mail: vladyslav.khvostenko@khpi.edu.ua.
Orcid ID: 0000-0002-6436-4159.

DOI: 10.18372/2410-7840.25.17594
УДК 004.43

DESIGN AND EVALUATION OF AN IOTA-BASED MEDICAL INFORMATION SYSTEM

Oleksandr Shmatko, Yaroslav Kliuchka, Roman Korolov, Vladyslav Khvostenko, Sergii Dunaiev

The traditional medical information systems are plagued by issues such as data breaches, lack of privacy, and data integrity concerns. This paper presents the design and evaluation of an IOTA-based medical information system aimed at addressing these challenges. In recent years, blockchain technology has emerged as a powerful tool for securing and managing data in a decentralized manner. One area where this technology has the potential to revolutionize the way we do things is in e-medicine. E-medicine, or electronic medicine, refers to the use of technology to deliver healthcare services remotely. This includes telemedicine, online consultations, and remote monitoring of patients' health status. IOTA blockchain technology, in particular, has a lot of potential in e-medicine. IOTA is a distributed ledger technology that uses a directed acyclic graph (DAG) instead of a traditional blockchain. The main ad-vantage of this approach is that it eliminates the need for miners and makes the system more scalable, fast, and energy-efficient. IOTA is also designed