International Journal of Safety and Security Engineering
Vol. 12, No. 5, October, 2022, pp. 563-568
Journal homepage: http://iieta.org/journals/ijsse

Securing an Information System via the SSL Protocol

Olga Purchina[1*], Anna Poluyan[2], Dmitry Fugarov[1]

[1] Department of Automation and Mathematical Modeling in the Oil and Gas Industry, Faculty of Energy and Oil and Gas Industry, Don State Technical University, 1 Gagarin Square, Rostov-on-Don 344003, Russia
[2] Department of Computing Systems and Information Security, Faculty of Informatics and Computer Engineering, Don State Technical University, 1 Gagarin Square, Rostov-on-Don 344003, Russia

Corresponding Author Email: olga.purchina@mail.ru

https://doi.org/10.18280/ijsse.120503

Received: 19 August 2022
Accepted: 12 October 2022

Keywords:
cryptography, encryption methods, information system, protocols

ABSTRACT

The aim of the study is to improve the quality and level of security of an information system for monitoring cargo vehicles at production sites via modern encryption methods, which will provide for accurate management decisions in the event of a system breach. In accordance with modern requirements of information security policies, enhancement of information system security assumes the development of data protection concepts and the implementation of the most advanced encryption methods within the information system. The paper presents the authors' solution for constructing an information system using SSL-based data encryption, SSL standing for the Secure Socket Layer. The characteristic feature of SSL-based encryption is the creation of a public-key cipher. This enables user and server authentication via digital signature technology. In addition, the method produces a session key that can be used to develop a fast symmetric cipher algorithm that allows encrypting of large arrays of information. Based on the proposed concept, the authors develop an information system for monitoring cargo vehicles at production sites that employs SSL-based encryption.

1. INTRODUCTION

Information security in the production process is of major importance for organizations. The measures to counteract illegal interference in an enterprise's information system (IS) proposed by us primarily provide protection against damage to critical information infrastructure. This kind of damage can completely stop an enterprise's operation. Our proposals aim to protect an enterprise's commercial interests in relation to monitoring freight transport and preventing leaks of customer and cargo data. Enhancement of IS security can only be attained through a set of data security measures. The result of the IS's operation should be a clear view of the production process, which allows for making informed management decisions and ensuring the security of transmitted information [1]. The security of transmitted information is constantly exposed to threats from the possibility of an attack on a computer system. An attack on a computer system implies the attacker's search for and/or exploitation of a system vulnerability. In other words, an attack is the implementation of a security threat [2, 3].

Many trucking companies still transmit all commercial information through open communication channels (planning the movement of vehicles, the location of posts, determining the order, possibility, or necessity of stopping, the size and characteristics of goods, customer data, etc.). Overall, this puts drivers and cargo at risk, and trucking companies lose millions of cargo every year due to the illegal dissemination of information.

Software packages designed for monitoring freight transport presented on the software market mainly consider the movement of vehicles. However, there are no software systems on the market that allow one to efficiently and quickly plan the movement of vehicles using data protection. The proposed approach to building an IS for monitoring freight transport has a scientific novelty because, unlike existing concepts, it provides security that meets the modern requirements of companies.

SSL or the Secure Sockets Layer is a cryptographic protocol that provides the most secure connection. It is used to verify the authenticity of the exchange key through asymmetric cryptography [2, 3]. The SSL (Secure Socket Layer) protocol was used in the development of the TLS RFC standard. The protocol also generates a symmetric cipher to provide information confidentiality and data verification codes for message integrity. This protocol has been widely used for instant messaging and for sending voice messages via VoIP in e-mail [3-5].

The SSL protocol secures data exchange by virtue of encryption and authentication. The protocol operates on asymmetric cryptography, which is used to verify the authenticity of the data exchange key. It also provides symmetric encryption to keep the data confidential and generates data authentication codes for message integrity [6]. Thus, the SSL protocol can be considered a secure communication channel characterized by the following properties:

1. This is a private channel. It produces encryption for each message at the end of a dialog, allowing the secret key to be determined.

2. Channel authentication. Each participant in the dialog must be authenticated.

3. Channel reliability. Data is transmitted only after a full integrity check.

Among the advantages of this protocol is its independence from the application layer protocol. HTTP, FTP, and TELNET can be overlaid on top of the protocol in question [7]. In this event, system transparency will be preserved. In other words, the SSL protocol will coordinate the encryption algorithm and the key, authenticating the server before transmitting or receiving the first byte of information [8, 9].

There are two main methods of creating information ciphers [10, 11]. These are symmetric encryption based on a single secret key and asymmetric encryption using several public or private keys. The SSL protocol uses both options. Asymmetric encryption relies on a pair of keys. One of the keys is public and can be found in the owner's certificate. The other is private and not published in the certificate. All keys are used only in pairs. The public key is used to encrypt information, while the private key decrypts the data [9, 12]. This system provides for the following:

1. Each user has the right to obtain a public key and use it to create an information cipher. However, only the person who has access to the private key can decrypt the data.

2. If a user who has a pair of keys creates a data cipher with his own private key, other users will be able to see that this information has been transmitted with a specific private key. In this case, the information could not be altered by a third party. This, in fact, is the essential purpose of creating a digital signature.

Public-key encryption uses two keys, one public and one private, and any of them can be used to encrypt messages [13]. If the message is encrypted via a public key, then the private one is to be used for decryption, and vice versa. In this case, there are two ways the keys can be used. First, the party keeping the private key and publishing the public one can receive public-key encrypted messages from the other side, which no one else can read (as decryption requires the private key known only to this first party) [14].

The goal of data encryption is to prevent damage to the owner, possessor, or user of information as a result of possible information leakage and/or unauthorized and unintentional interference with information [3].

The goal of the present study is to enhance the level of information exchange security in an IS for monitoring cargo vehicles on production sites by introducing modern encryption methods.

2. METHODS

The study aims to find the optimal method for securing information exchange and storage at an enterprise. The studied IS was introduced and tested in the period from 2020 to 2021 at a transport company. The conceptual model of the IS was designed based on the analysis of information tasks solved at the company as part of transporting various cargoes by different vehicles. The information on objects collected for the study contains personal data, financial data, information about vehicles, routes, etc. Relationships between the objects are part of the conceptual model of the IS and should be displayed in the database. Said relationships can extend to any number of objects, and each object can participate in any number of relationships.

We propose our own security policy (SP) (Figure 1), in which information is secured using information object authentication rules, key exchange, records of the results of security events in electronic logs, and records of data security risks in the enterprise. The objects of SP are individual subnets and workstations, which include structural subdivisions of the company.

For the organization of security, we considered an SSL protocol composed of two subprotocols: the handshake protocol and the record protocol. The SSL server and user establish communication through a handshake protocol. In a handshake, the server and user agree on different values used to ensure a secure connection. The record protocol defines the format of information received. The operation of this protocol requires the respective extension on the server.

The SSL protocol allows the use of a communication channel distinguished by three main characteristics:

• Authentication. The server is always checked at the exact moment the user is authenticated, based on the algorithm.

• Integrity. Information exchange is checked for integrity.

• Confidentiality of the established connection. The cipher is created after the connection is set up and applies to all of the following data.

SSL transmits all information in the form of a record of objects that have a header and certain information. Data is always transmitted with a header. It includes no more than three bytes of code length. Note that if the high bit in the original code byte is equal to one, the recording is made without a placeholder. In this case, the size of the header will be up to two bytes. Otherwise, the record will be written with a placeholder and the header will reach three bytes. The record length code is calculated without the number of header bytes. The record size of a two-byte header is as follows:

```
RecLength = ((byte[ 0 ] & 0x7F) << 8) | byte[ 1 ];
```

Herein, byte[0] and byte[1] are initial and subsequent received bytes. The record size of the three-byte header:

```
RecLength = ((byte[ 0 ] & 0x3F) << 8) | byte[ 1 ];
Escape = (byte[ 0 ] & 0x40) != 0;
Padding = byte[ 2 ];
```

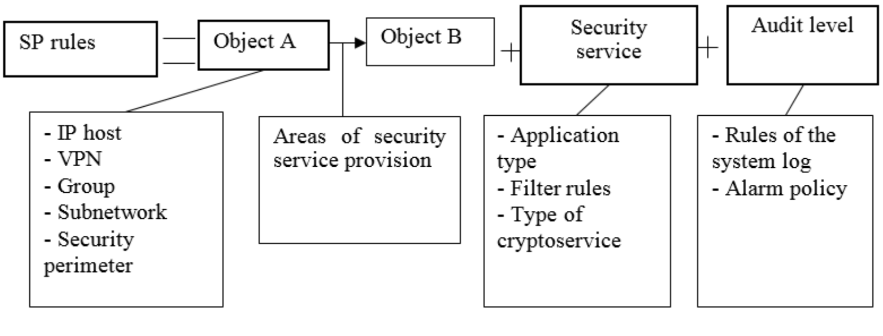

Figure 1. Corporate SP structure

The number of bytes is determined by Padding. They are added to the final content by the user in order to obtain a record size multiple of the encryption block length. The filler is then added by the user and the information is encrypted. The filler text is irrelevant. Given that the size of the transmitted information is known, the header can be formed by Padding. The addressee decrypts each information block and receives the raw data. Then the RecLength parameter is calculated using the Padding parameter. The filler is removed from the information blocks. The record of information includes three elements:

- Actual_Data[N] — factual information
- Padding_Data[Padding] — filler information
- MAC_Data[Mac_Size] – data authentication code

When a record is sent as public content, there is no need to create such encryption. In this case, the MAC_Data and Padding_Data lengths are set to zero. If a cipher is applied, the length of Padding_Data will be affected by the volume of the encrypted data block, and the length of MAC_Data will be affected by the cipher itself. Here is an example of MAC_Data calculation:

MacData = Hash(Secret, Actual_Data, Padding_Data, Sequence_Number)

The Secret parameter is related to the sender or receiver of text information. The Sequence_Number is a counter that increments the variable from the user or server. In our case, the counter is a 32-bit code that comes in the form of a four-byte hash function.

3. RESULTS

The proposed IS incorporates the SSL protocol, which supports the development of ciphers. Information received through the HTTPS protocol is converted into cryptographic data of TLS or SSL protocols. In this way, the safety and confidentiality of information can be provided [15]. Today, this security method provides reliable protection for various Internet applications and secure connections in bank payment systems. The protocol operates with any and all browsers. Unlike HTTP, HTTPS operates on TCP port 443. Virtual private networks (VPNs) using SSL were created as an alternative to IPsec VPN-based remote access. Nevertheless, because of its affordability and high reliability, this technology has become the most attractive for VPNs [16]. SSL is widely used in data exchange in e-mail. Below we give a table comparing the capabilities of IPSec-VPN and SSL-VPN [5].

Based on Table 1, we conclude that SSL VPN has broader characteristics, shows advantages for ensuring secure information transfer, and does not require any additional solutions.

Protocol objectives by priority:

1. Security at the cryptographic level. SSL ensures secure communication between the parties involved in the data exchange process.
2. Compatibility. Programmers create SSL-based applications that can efficiently exchange cryptographic information without having to specifically recognize the encryption of other programs.
3. Extensibility. SSL enables a working environment for the necessary incorporation of public keys and the more labor-intensive processes of creating ciphers.
4. Relative productivity. SSL-based protocols require high CPU speeds. The same applies to the use of public keys. As a result, SSL enters the auxiliary caching phase to reduce the number of connections that require setting up from scratch. Internal network activity is also reduced.

Table 1. Comparison of the capabilities of IPSec VPN and SSL VPN

Characteristic	IPsec VPN	SSL VPN
Business application support	+	+
HTTP application support	+	+
File server access support	+	+
Corporate PC	+	+
Mobile PC	+	+
Working from a third-party network (behind a firewall)	- requires ports to be opened	+ operation through https
Public networks	- requires client installation	+
PDA, communicator	- + requires a VPN client for the device	+
Strict authentication option	+ in most cases	+
Centralized authorization	+	+
Web single sign-on	- requires additional solutions	+
Automatic application of security policies depending on the type of object and user	- requires additional solutions	+
Clientless technology	-	+ a browser is sufficient

The protocol works with three authentication checks [9, 17]:

- Authentication of a server with an unauthenticated user.
- Complete anonymity.
- Authentication of all participants in the data exchange process (server-user).

This protocol handles all errors quite easily. If an error is detected, the relevant information is sent to the other part of the system. An unrecoverable error requires the user or the server to cease communication [18].

SSL is affected by different cryptographic values. Encryption can be performed with different cryptographic algorithms. Thus, if an attack on such an algorithm is implemented with success, the protocol will not be able to provide a secure connection. An attack on a particular communication network is carried out through an in-session entry. It is necessary to distinguish between attacks against SSL. It should be borne in mind that the SSL protocol can resist these attacks if the client only uses a verified server to process the data [5, 19, 20].

The most common is the MitM attack. It involves three parties with the attacker residing between the user and the server. In such circumstances, the offender intercepts the data sent both ways and spoofs it [5, 21]. For the user, the attacker poses as the server, and vice versa. Such attacks are most successful with Diffie-Hellman key exchange due to the integrity of the data and the inability to authenticate it. At the same time, such attacks are not performed within SSL due to the mandatory authentication of the information source.

With this type of attack, some big companies get the data they need by using Forefront TMG. In this scenario, the attacker changes the authentic certificate to their own. Such an attack succeeds because of specifying Forefront TMG as a trusted certificate authority. As a rule, this operation goes unnoticed by the client due to the operation of corporate users within Active Directory. This control tool can be used to obtain data and steal personal information that is transmitted over a secure HTTPS connection.

The issue of adequate awareness of clients about the probable interception of information remains topical [22, 23]. The problem is that when the original certificate is spoofed, the associated security messages are not displayed. The client, therefore, believes that the data transfer is secure. With Forefront TMG, it is possible to perform a second MitM attack on the Internet. In this case, the certificate is not delivered to the client. To defend against this attack, activity with web resources whose certificates contain certain errors needs to be ceased [5, 9, 20, 23-26].

Response attack. The attacker records the communication connection between the user and the server. Next, the attacker connects to the server to reproduce the recorded client data. However, SSL prevents this attack through connection identification. Surely, it is not possible to alert the connection identifier by theory alone, as it involves random events. If the attacker has substantial means, they can keep record of numerous sessions to select the best one based on the nonce cipher. These codes, however, a distinguished by a 128-byte length. This means that the perpetrator has to keep a record of nonce codes to achieve a 50% prediction capability [6, 9].

The algorithms used in SSL include:

• PSK, SRP, ECDH, and RSA used for key exchange and authentication.

• ECDSA, DSA, and RSA for verification of authenticity.

• Camellia, AES, DAS, IDEA, RC4, RC2, and Triple DES for creating symmetric ciphers.

• MD2, MD4, MD5, and SHA for hash functions.

4. DISCUSSION

Recently, the development of technology in the field of information security has evolved a lot. The market has a lot of commercial proposals for the provision of information security in the enterprise. To date, quite a large number of projects on the introduction of remote access in companies based on the SSL VPN technology have already been implemented [5]. Analysis of various sources and recommendations on information security suggests a list of standard rules [3, 5, 20, 23, 25-27]:

- control of logging into the AIS and database loading by means of unique identifiers (login, password, code, etc.);
- regulation of access to objects;
- encryption of file systems;
- secure connections;
- a set of protocols for IPsec data security;
- backups of the most valuable data saved regularly according to the schedule;
- the use of hardware protection; for example, disabling the jumper on the motherboard will protect against ROM erasure;
- protection of software that enables the execution of processes for a particular user from unauthorized entities;
- securing confidential data flows;
- generation of protocols on the destruction and erasure of residual confidential data;
- provision of data integrity by introducing redundant information;

Aside from the above, based on the specifics of the organization and proceeding from the analysis of its information SP, the SSL encryption algorithm, and the software used, changes were introduced to attain the necessary level of IS security. These measures will achieve the desired level of IS security for production sites.

1. Full centralization of the application implies abandoning local databases located on servers in branches, writing instructions for support functions, and transferring application support to Help Desk and infrastructure functions.
2. Publication of the application on the company intranet will allow accounting and filtering of users. In addition, additional group access rights to open this application need to be introduced.
3. Location of the database in the data center will increase the overall availability time of the application. This will ensure proper allocation of hardware resources, fast and high-quality application updates for the entire program at once, and, most importantly, reliable backup because a backup copy of the entire server is taken and, in case of hardware failure or a critical application failure, there will always be an opportunity to deploy a fully working version of the application on different hardware, which can be installed in the data center of the company.
4. Protection of client stations is a must-have part of the concept because they are where the main threat comes from. The antivirus must be network-controlled in order to quickly localize threats. The user must not be able to disable the antivirus or weaken its protection.
5. The main threat to information security comes from users because no matter how perfectly the IS is protected, the user can run a virus on their station. This can result in the loss of information not only on their station, but also on the server, and the spread of the virus over the network.
6. The system may only be accessed from the domain structure. Employees fired or blocked for other reasons must not have access to any IS: files on local stations, e-mail, and other IS of the company. Change of a password after its expiration date and introduction of requirements for password complexity are also needed.
7. Encryption of data transmitted between the server and the client.

5. CONCLUSION

The concept of the designed IS, in contrast to the already existing ones, is marked by the level of security consistent with the current demands of companies. Based on the developed concept, we created an IS for monitoring cargo vehicles on production sites that uses SSL encryption. The system has the capacity to introduce additional monitoring points and is characterized by uniformity. The developed concept for the construction of the IS, unlike other existing concepts, offers security that meets the modern requirements of enterprises.

The practical value of the obtained research results is that based on the developed concept, an IS for monitoring cargo vehicles at production sites using SSL encryption was created.

The system offers an opportunity to introduce additional monitoring points, is unified, and has been successfully implemented at 12 production sites. It is also planned to introduce additional modules of localization and authentication of users in the system by means of certification, which will make it possible to introduce this IS at international production sites and raise the level of system security.

REFERENCES

[1] Fugarov, D.D., Gerasimenko, Y.Y., Nesterchuk, V.V., Gerasimenko, A.N. (2018). Methods for revealing hidden failures of automation system for technological processes in oil and gas sector. Journal of Physics: Conference Series, 1118: 012055. http://dx.doi.org/10.1088/1742-6596/1118/1/012055

[2] Poluyan, A.Y., Fugarov, D.D., Purchina, O.A., Nesterchuk, V.V., Smirnova, O.V., Petrenkova, S.B. (2018). Adaptive algorithm of selecting optimal variant of errors detection system for digital means of automation facility of oil and gas complex. Journal of Physics: Conference Series, 1015: 022013. https://doi.org/10.1088/1742-6596%2F1015%2F2%2F022013

[3] Shangin, V.F. (2010). Zashchita Kompiuternoi Informatsii [Computer Information Security]. DMK Press, Moscow.

[4] Ventsov, N.N., Podkolzina, L.A. (2017). Studying the effect of paralleling settings on the functioning of a barcode recognition app. In: 2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), IEEE, pp. 1-5. https://doi.org/10.1109/ICIEAM.2017.8076476

[5] Tereshchenko, N. (2008). SSL VPN – shag vpered v tekhnologii VPN setei [SSL VPN – a step forward in VPN networking technology]. https://www.anti-malware.ru/node/449, accessed on March 15, 2022.

[6] Chernyshev, Y.O., Purchina, O.A., Poluyan, A.Yu., Fugarov, D.D., Basova, A.V., Smirnova, O.A. (2015). Swarm-intelligence-based algorithm of connections permutation between pins. Journal of Theoretical and Applied Information Technology, 80(1): 13-20.

[7] Purchina, O., Poluyan, A., Fugarov, D. (2021). The algorithm development based on the immune search for solving unclear problems to detect the optical flow with minimal cost. E3S Web of Conferences, 258: 06052. https://doi.org/10.1051/e3sconf/202125806052

[8] Gerasimenko, Y., Gerasimenko, A., Gerasimenko, Y., Fugarov, D., Purchina, O., Poluyan, A. (2021). Mathematical modeling and synthesis of an electrical equivalent circuit of an electrochemical device. In: Murgul, V., Pukhkal, V. (eds) International Scientific Conference Energy Management of Municipal Facilities and Sustainable Energy Technologies EMMFT 2019. EMMFT 2019. Advances in Intelligent Systems and Computing, vol. 1259, Springer, Cham, pp. 471-480. https://doi.org/10.1007/978-3-030-57453-6_45

[9] Iakovlev, A.V., Bezbogov A.A., Rodin V.V., Shamkin V.N. (2016). Kriptograficheskaia Zashchita Informatsii. Uchebnoe posobie [Cryptographic Information Protection. Textbook]. Tambov State Technical University, Tambov.

[10] Solonskaya, O.I. (2021). Sredstva zashchity informatsii [Information security tools]. Siberian State University of Telecommunications and Informatics , Novosibirsk.

[11] Linxuan, X., Jiantao, Z., Lei, Y. (2021). Modeling data, information and knowledge for security protection of tasks scheduling algorithms in cloud computing. IEEE 23rd International Conference on High Performance Computing and Communications, 7th International Conference on Data Science and Systems, 19th International Conference on Smart City and 7th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Applications, HPCC-DSS-SmartCity-DependSys 2021., pp. 2199-2205. Haikou, Hainan: 2021.

[12] Ganzhur, M., Dyachenko, N., Gazizov, A., Otakulov, A., Romanov, D. (2020). Modeling of storage processes using Petri nets. E3S Web of Conferences, 175: 05038. https://doi.org/10.1051/e3sconf/202017505038

[13] Fugarov, D. (2022). Development and mathematical modeling of the AC sensor for refinery automation systems. In: Shamtsyan, M., Pasetti, M., Beskopylny, A. (eds) Robotics, Machinery and Engineering Technology for Precision Agriculture. Smart Innovation, Systems and Technologies, vol. 247, Springer, Singapore, pp. 271-281. https://doi.org/10.1007/978-981-16-3844-2_28

[14] Agibalov, O., Blinovskaya, T., Ventsov, N. (2020). On the issue of using intuitionistic fuzzy sets for describing the expediency of solving optimization problems by genetic algorithms with given parameters. E3S Web of Conferences, 224: 01008. https://doi.org/10.1051/e3sconf/202022401008

[15] Kozinkina, A.I., Fugarov, D.D. (2020). A magneto dielectric AC measuring transducer for refinery automation systems. Journal of Machinery Manufacture and Reliability, 49(11): 963-970. https://doi.org/10.3103/S1052618820110096

[16] Onyshko, D., Fugarov, D., Purchina, O., Poluyan, A., Rasteryaev, N., Skakunova, T. (2020). Synchronization system in wireless sensor networks of oil and gas complex. E3S Web of Conferences, 164: 03030. http://dx.doi.org/10.1051/e3sconf/202016403030

[17] Poluyan, A.Y., Purchina, O.A., Fugarov, D.D., Golovanov, A.A., Smirnova, O.V. (2019). Solution of task on the minimum cost data flow based on bionic algorithm. Journal of Physics: Conference Series, 1333: 032056. http://dx.doi.org/10.1088/1742-6596/1333/3/032056

[18] Gazizov, A., Gazizov, E., Gazizova, S. (2020). Theoretical aspects of the protection of personal data of employees of the enterprise by the method of pseudonymization. E3S Web of Conferences, 210: 11001. http://dx.doi.org/10.1051/e3sconf/202021011001

[19] Poluyan, A.Y., Purchina, O.A., Fugarov, D.D., Gerasimenko, E.Y., Skakunova, T.P. (2019). Application of bionic and immune algorithms for the solution of ambiguous problems of transportation routing. Journal of Physics: Conference Series, 1333: 032057. https://doi.org/10.1088/1742-6596/1333/3/032057

[20] Qualys. (n.d.). SSL Server Test. https://www.ssllabs.com/ssltest/, accessed on October 1, 2021.

[21] Fugarov, D.D., Purchina, O.A., Poluyan, A.Y., Gerasimenko, E.Y., Rasteryaev, N.V. (2019). Magnetodielectric AC measuring transducer for automation systems in oil refineries. Journal of Physics:

Conference Series, 1333(6): 062020. http://dx.doi.org/10.1088/1742-6596/1333/6/062020

[22] Solomentsev, K.Y., Fugarov, D.D., Purchina, O.A., Poluyan, A.Y., Nesterchuk, V.V., Petrenkova, S.B. (2018). Interference elimination in digital controllers of automation systems of oil and gas complex. Journal of Physics: Conference Series, 1015: 032179. https://doi.org/10.1088/1742-6596/1015/3/032179

[23] SearchInform. (n.d.). Metody obespecheniia informatsionnoi bezopasnosti [Information security methods]. https://searchinform.ru/analitika-v-oblasti-ib/Issledovaniya-v-oblasti-ib/metody-obespecheniya-informatsionnoj-bezopasnosti/, accessed on March 15, 2022.

[24] Sukhinov, A.I., Chistyakov, A., Protsenko, E., Sidoryakina, V., Protsenko, S. (2020). Accounting method of filling cells for the solution of hydrodynamics problems with a complex geometry of the computational domain. Mathematical Models and Computer Simulations, 12(2): 232-245. https://doi.org/10.1134/S2070048220020155

[25] Iasenev, V.N., Dorozhkin, A.V., Matveev, V.A., Sochkov, A.L., Yasenev, O.V. (2017). Informatsionnaia Bezopasnost: Uchebnoe posobie [Information Security: Textbook]. National Research Lobachevsky State University of Nizhni Novgorod, Nizhny Novgorod.

[26] ICC Russia. (2016). Obespechenie informatsionnoi bezopasnosti organizatsii [Ensuring information security of the organization]. https://iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/, accessed on March 15, 2022.

[27] Touil, H., El Akkad, N., Satori, K. (2021). Secure and guarantee QoS in a video sequence: A new approach based on TLS protocol to secure data and RTP to ensure real-time exchanges. International Journal of Safety and Security Engineering, 11(1): 59-68. https://doi.org/10.18280/ijsse.110107