IRSTI 81.93.29
UDC 004.056.5

INFORMATION SECURITY TOOLS IN AN AUTOMATED SYSTEM FOR SECURE INFORMATION EXCHANGE

Ye. Begimbayeva[1,2], O. Ussatova[1,2], R. Biyashev[1], Andrzej Smolarz[3], A. Abisheva[1,2]
[1]Institute of Information and Computational Technologies,Almaty, Kazakhstan
[2]al-Farabi Kazakh National University, Almaty, Kazakhstan
[3]Lublin Technical University, Poland.
[1]enlik_89@mail.ru, [2]uoa_olga@mail.ru
[1]ORCID ID: https://orcid.org/0000-0002-4907-3345
[2]ORCID ID: https://orcid.org/0000-0002-5276-6118

Abstract. The article presents tools of information security to ensure the secure exchange of information in an automated system. A model of information security for an automated system of the exchange of information is proposed. Proposed model will increase the level of information security in electronic flow of document in the cross border information space. Any cryptographic system is based on the use of cryptographic keys. Key information is understood as the totality of all keys operating in the information network or system. If a sufficiently reliable management of key information is not ensured, then, having taken possession of it, an attacker gains unlimited access to all information in the network or system. Key management includes the implementation of functions such as generating, storing and distributing keys. The article presents requirements for the key management process. The main methods used to distribute keys between users of a computer network are presented.

Keywords: cross-border information exchange, electronic digital signature, encryption, information security, access control, cryptography, conflict situations, crypto analysis.

Introduction

One of the tasks of the correct functioning of any information data transmission system, namely, in cross-border exchange, is to ensure secure data transmission.

The developed model of an automated system for secure cross-border information exchange (AS SCbIE) was developed taking into account the existence of many subsystems [1-5], including:

cryptographic subsystems confidentiality, data integrity and non-repudiation of authorship, by using encryption algorithms and electronic digital signature;

the access control subsystem provides identification and authentication when logging into the system, access of subjects to various objects and resources using specified policies and procedures;

the registration and accounting subsystem provides registration of: entry (exit) of subjects of access to (from) the system; actions of subjects over objects; object status; conflict situations in the system.

The structural general diagram of the developed model of AS SCbIE is shown in the figure 1.

The developed model of the information system uses an encryption algorithm based on non-positional polynomial notations ModNPSS14. This algorithm is a symmetric block cipher that uses blocks of 128 bits, an 8-cycle Feistel network [6-7].

The basis of the developed model of EDS generation and verification is the developed modified (extended) algorithm for EDS generation and verification based on modular notations. The software implementation of the developed modified algorithm for the formation and verification of EDS on the basis of modular notations has been carried out [5].

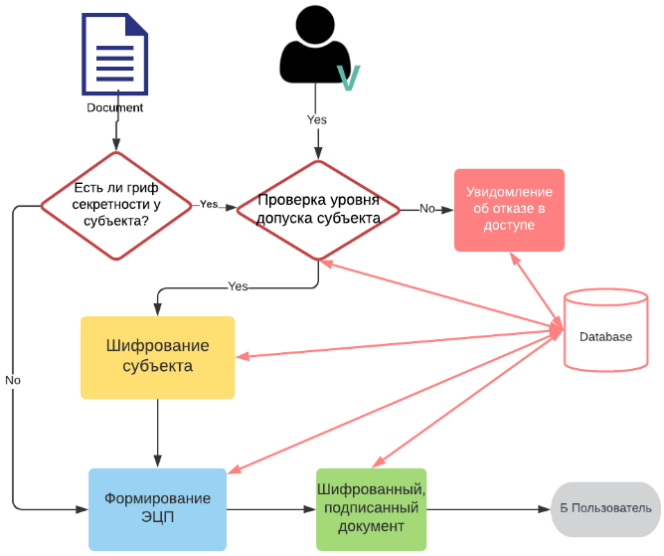

Figure 1 - Structural general diagram of the information security model in AS SCbIE

Any cryptographic system is based on the use of cryptographic keys. Key information is understood as the totality of all keys operating in the information network or system. If a sufficiently reliable management of key information is not ensured, then, having taken possession of it, an attacker gains unlimited access to all information in the network or system. Key management includes the implementation of functions such as generating, storing and distributing keys.

The scope of work to support and maintain keys significantly exceeds the scope of work on their use for encrypting messages. Keys must be securely distributed to authorized users and kept up to date. They must be reliably protected during their transfer and storage on workstations and servers. Keys must be generated, destroyed and recovered in a secure manner. Key management can be organized manually or through an automated process.

It is imperative that the key management process is properly secured. The key management process has the following requirements:

- the key length must be large enough to provide the required level of security.
- keys must be stored and transferred in a secure manner.
- keys must be completely random, and their generation algorithms must make full use of all available key space.
- the key validity period should correspond to the criticality of the data it protects. Less critical data can be protected with a longer validity key, while critical data requires the use of short validity keys.
- the more often the key is used, the shorter its validity period should be.
- a key must be backed up or a duplicate key must be escrowed to an independent third party in case of an emergency.
- keys must be properly destroyed when they expire [8].

The goal of key management is to neutralize threats such as:

- compromising the confidentiality of private keys;
- compromising the authenticity of private or public keys. In this case, authenticity is understood as the knowledge or ability to verify the identity of the correspondent, to ensure confidential communication with which this key is used;
- unauthorized use of private or public keys, for example the use of a key that has expired.

When using a symmetric cryptosystem, two parties entering into an information exchange must first agree on a secret session key, that is, a key for encrypting all messages transmitted during the exchange. This key must be unknown to everyone else and must be periodically updated at the same time at the sender and receiver. The session key negotiation process is also referred to as key exchange, or key distribution.

An asymmetric cryptosystem assumes the use of two keys - public and private (secret). The public key can be disclosed, but the private key must be kept secret. When exchanging messages, only the public key needs to be sent, ensuring the authenticity of the forwarded public key.

Key distribution is one of the fundamental tasks of cryptography and the most critical process in key management. To understand the scale of the problem, we note that when servicing n users who exchange private information with each other, n (n-1)/2 different secret keys are required. As n grows, the problem of managing a huge number of keys arises. There are several ways to solve this problem. The definition of the most suitable one is chosen depending on the current situation [9]:

- physical distribution;
- issuance of a common key to participants in the interaction by the key issuing center - a "subscriber encryption" scheme;
- provision by a certification authority of access keys to public keys of users and issuance of private keys of a user;
- web of trust. Used in asymmetric cryptosystems;
- key exchange protocols.

The following requirements are imposed on the distribution of keys:

- efficiency and accuracy of distribution;
- confidentiality and integrity of distributed keys.

The following basic methods are used to distribute keys between users of a computer network:

1) using one or more key distribution centers;
2) direct exchange of keys between network users.

The problem with the first approach is that the key distribution center knows to whom and what keys are distributed, and this makes it possible to read all messages transmitted over the network. Potential abuse can significantly compromise network security. In the second approach, the problem is to reliably verify the identity of the network subjects.

Let's take a closer look at the second approach - direct key exchange between network users. When using a symmetric secret key cryptosystem for secure information exchange, two users wishing to exchange cryptographically protected information must have a shared secret key. These users must exchange the shared key over the communication channel in a secure manner. If users change keys frequently enough, key delivery becomes a serious problem.

The task of key distribution is reduced to the construction of such a key distribution protocol that provides:

- mutual confirmation of the authenticity of the session participants;
- confirmation of the validity of the session;
- using the minimum number of messages for key exchange.

It is advisable to base the solution to the key distribution problem on the principle of separating the procedure for confirming the authenticity of partners from the procedure for distributing keys itself. The goal of this approach is to provide a method in which, once authenticated, the participants generate the session key themselves, without the involvement of a key distribution center, so that the key distributor cannot identify the content of the messages.

The model and algorithm of the proposed method of protecting information in an automated control system using a combination of two factors: a permanent and temporary password. The user chooses a permanent password (the first factor) and uses it (account) when registering an account. The developed model is based on two types of two-factor authentication: authenticator applications and login verification using mobile applications are implemented [5,10].

One of the constituent components of the conflict resolution system is the Event Log (logging). Event logs are special files in which the system records significant events, such as user logon events or errors that occur while working with the system. When these types of events occur, an entry is created in the event logs. In detailed descriptions of events, users can find information useful for troubleshooting, finding the cause of problems, conflicts with the system

or subsystems. A message in the event log is, first of all, information that can help the administrator and even the user understand what problem or conflict has arisen in the system and how to fix it [11].

Figure 2-3 shows a fragment of the authorization subsystem record and user actions. All user actions in the program are recorded in a separate file.

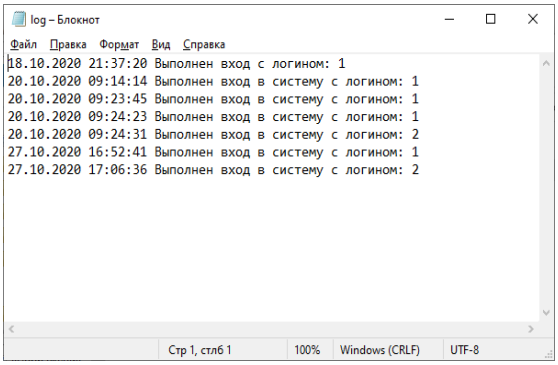

Figure 2 - Fragment of logging into the system

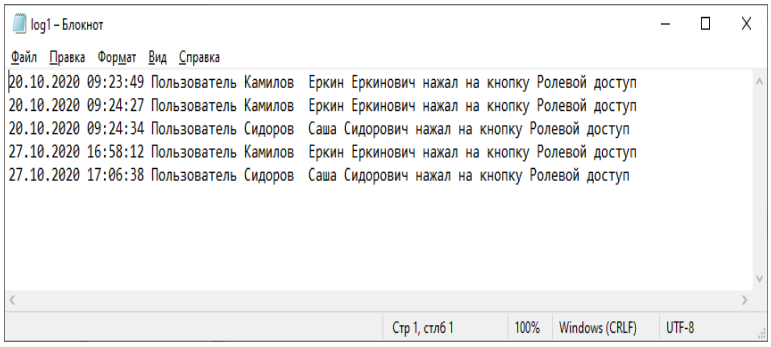

Figure 3 - Fragment of logging user actions

The proposed structure [11-12] can serve as a basis for building a software complex for detecting conflicts in software systems for protecting information and resolving them. The use of conflict resolution systems for software information security systems will increase the efficiency of the system administrator and reduce the time required to identify the presence of conflict interaction in the information system.

When the program starts, an authorization window will open (Figure 4). To enter the system, you need to enter a username and password (if the user is registered in the database). The password field is masked in order to keep the entered password secret, if necessary, you can see the entered password by clicking on the "Show password" field. If all the entered data are correct, the main program window will open, where all information about the user will appear (Figure 5).

The main window of the program contains information about the employee (user) and about his documents. At the bottom of the main window, there are buttons for demonstrating information access models. "Role-based access" opens a new window with information about the user and available functions and documents (Figure 6).

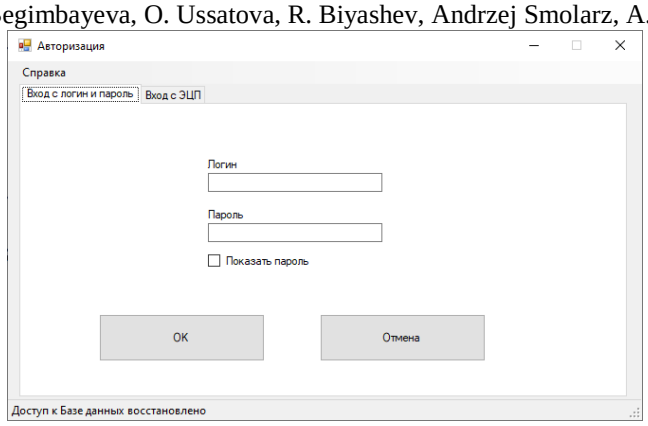

Figure 4 - Program authorization window

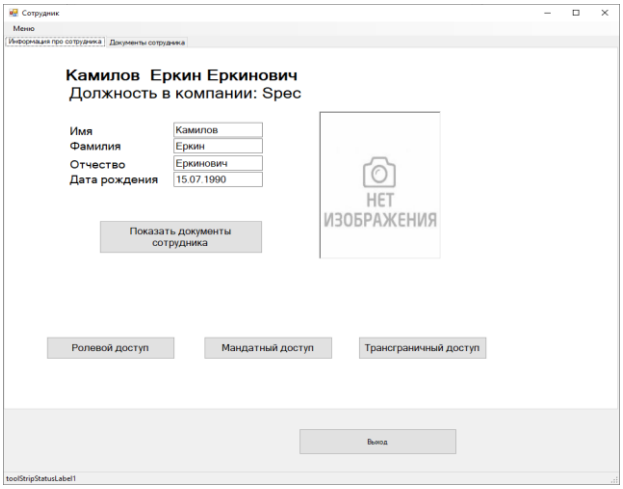

Figure 5 - The main window of the program

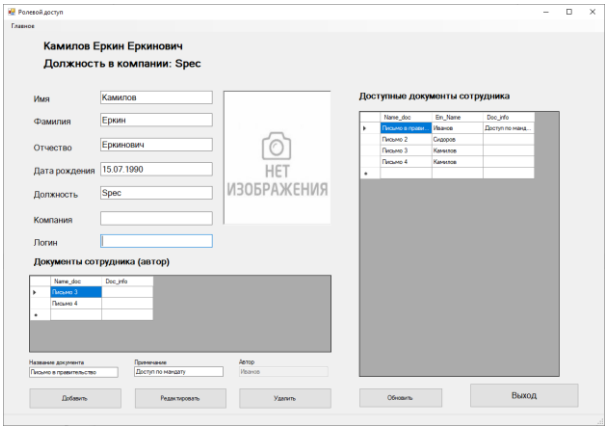

Figure 6 - Role-based access model window

This user has full access to information (all functions for managing information are available). He can add, edit, delete and view information from the database (DB). The table on the right shows all documents available to the user. The name of the document, the creator of the document and brief information about the document. Figure 7 shows a user with read-only access, the user does not have access to the basic functions of editing information in the database.

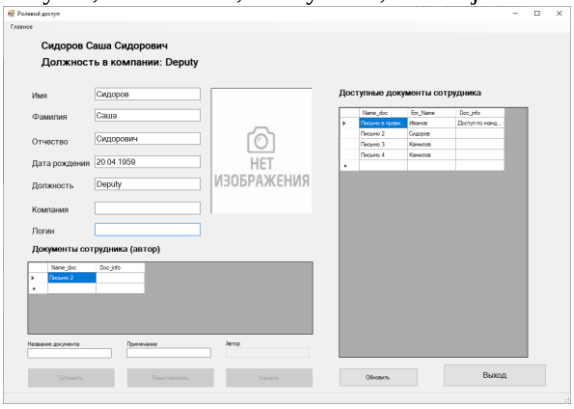

Figure 7 - An example of a role-based access model (read-only)

Conclusion

The assembly, debugging and introduction into the experimental, and then into industrial operation of the system is supposed to be carried out together with the team of the integration gateway, whose functions are determined by the EEU documents to ensure the functioning and subsequent development of the integration gateway. Since only they should know the composition of cross-border exchange subscribers on the territory of Kazakhstan and their secrecy labels. Accordingly, encryption and decryption keys must be jointly generated and distributed. This will reduce possible conflicts and optimally resolve them.

Acknowledgements

Research work was carried out within the framework of the project AP05132584 “Development of Kazakhstan segment of the protected cross border information interaction”, which is being implemented at the Institute of Information and Computer Technologies.

Reference:

[1] R. G. Biyashev, S. E. Nyssanbayeva, and Ye. Y. Begimbayeva Development of the model of protected cross-border information interaction. Open Engineering, 2016. 6. 199–205.

[2] Biyashev R.G., Begimbayeva Ye.Ye., Rog O.A. Development of an automated information protection system in the process of cross-border exchange. Mater. scientific. conf. "Modern problems of informatics and computing technologies". - Almaty: IICT MES RK, (2019). 148-154 (in Russian).

[3] Biyashev R.G., Begimbayeva Ye.Ye., Ussatova O.A., Rog O.A., Dyussenbaev D.S. Development of means for organizing secure information exchange in the Kazakhstani segment during cross-border interaction. Modern problems of informatics and computational technologies: Mat. scientific. conf. - Almaty: IICTT MES RK, (2020). 105-109 (in Russian).

[4] Begimbayeva Ye.Ye., Biyashev R.G. On the development of a system model for the Kazakh segment of secure cross-border information interaction. Mater. V int. scientific-practical conf. Computer science and applied mathematics. Almaty, (2020). 398-401 (in Russian).

[5] Begimbayeva, Y.Y., Ussatova O.A., Nyssanbayeva, S.E., Biyashev, R.G. Development of an automated system model of information protection in the cross-border exchange. Cogent Engineering. 2020. 7, Is. 1 // DOI: 10.1080/23311916.2020.1724597 (SJR 0.272, Q2, percentile 69).

[6] Dyussenbaev D., Sagan Y., Algazy K., Khompysh A. "MODNPSS14" cipher algorithmin cryptography taldau. Khabarshy KazKKA. 2019. 3. 235-243 (in Russian).

[7] Dyussenbaev D., Ostapenko V., Alkazy K., Sagan K. Cryptanalysis of "MODNPSS14" cipher algorithm. Mater. IV int. scientific-practical conf. "Computer Science and Applied Mathematics". Almaty, (2019). 556-561 (in Kazakh).

[8] Fomina I.A. Key management in cryptographic systems. Bulletin of Nizhegorodskogo universiteta im. N.I. Lobachevsky. Ser. inform. 2010. 4(1). 165-169.

[9] Schneier B. Applied Cryptography. Protocols, algorithms, source texts in the C language. M.: Iz-vo "Triumph", 2003. 816 p.

[10] S. Nyssanbayeva, W. Wojcik, O. Ussatova «Algorithm for generating temporary password based on the two- factor authentication model». Przegląd Elektrotechniczny, Poland. 2019. 5. 101 – 106.

[11] Begimbayeva Ye.Ye. On the model for resolving conflict situations in an automated system of secure information interaction. Actual problems of information security in Kazakhstan: Mater. Int. scientific. - practical. conf. Almaty, 2020. 105-107 (in Russian).

[12] Rustem Biyashev, Saule Nyssanbayeva and Yenlik Begimbayeva Development and Analysis of Possible Conflict Situations Resolution Systems in an Automated System. Proceeding of International Conference on Wireless Communication, Network and Multimedia Engineering. Guilin, China, (2019). 89. 182-184.