що у випадку неможливості досягнення глобального екстремуму при заданих обмеженнях доцільно розглянути задачу забезпечення виконання бізнес-процесів точно в строк.

Список літератури: 1. *Vom Brocke J., Rosemann M.* Handbook on Business Process Management 1. Introduction, Methods, and Information Systems. Springer-Verlag Berlin Heidelberg, 2015. 709 p. doi:10.1007/978-3-642-45100-3. 2. *Елиферов В.Г., Репин В.В.* Бизнес-процессы: Регламентация и управление. М.: ИНФРА-М, 2004. 319 с. 3. *Weske M.* Business Process Management: Concepts, Languages, Architectures. Springer-Verlag Berlin Heidelberg, 2012. 403 p. 4. *Van der Aalst W.M.P., Van Hee K.M.* Workflow Management: Models, Methods, and Systems. MIT press. Cambridge, MA. 2002. 361 p. 5. *Richter M.M., Weber R.O.* Case-Based Reasoning. A Textbook. Springer. 2013. 546 p. 6. *Kolodner J.* Case-Based Reasoning. Magazin Kaufmann. San Mateo. 1993. 386 p. 7. *Michalski R.S., Carbonell J.G. & Mitchell T.M. (Eds.).* Learning by analogy: Formulating and generalizing plans from past experience // Machine learning, an artificial intelligence approach. Palo Alto, CA: Tioga Press. 1983. Vol. 1. P. 137 - 162. 8. *Aamodt A., Plaza E.* Case-Based Reasoning: Foundational issues, methodological variations, and system approaches // AI Communications. 1994. IOS Press. Vol.7:1. P. 39- 59. 9. *Николайчук О.А., Юрин А.Ю.* Применение прецедентного подхода для автоматизированной идентификации технического состояния деталей механических систем // Автоматизация и современные технологии. 2009. №5. С.3 - 12.

Надійшла до редколегії 24.01.2018

Чалий Сергій Федорович, д-р техн. наук, професор, професор кафедри ІУС ХНУРЕ. Наукові інтереси: розробка моделей, методів і технологій автоматизованого управління бізнес-процесами (в тому числі із змінною структурою) в умовах неконтрольованих зовнішніх збурень. Адреса: Україна, 61166, Харків, пр. Науки, 14, тел. 70-21-451.

Левикін Ігор Вікторович, канд. техн. наук, доцент, професор кафедри МСТ ХНУРЕ. Наукові інтереси: інформаційні системи і технології; моделі і методи автоматизації процесів управління поліграфічних підприємств. Адреса: Україна, 61166, Харків, пр. Науки, 14, тел. 70-21-378.

Кальницька Анжеліка Юріївна, асистент кафедри ІУС ХНУРЕ. Наукові інтереси: розробка методів і технологій автоматизованого управління бізнес-процесами. Адреса: Україна, 61166, Харків, пр. Науки, 14, тел. 70-21-451.

УДК 004.03:65/.056.55 DOI: 10.30837/0135-1710.2018.175.026

V.I. RUZHENTSEV, O.V. VYSOTSKA, L.M. RYSOVANA, YU.YE. ZINCHENKO, R.V. ALEKSEIENKO

ORGANIZATION OF INFORMATION PROTECTION OF THE INFORMATION SYSTEM DETECTION OF PSYCHOEMOTIONAL AND COGNITIVE DISORDERS

The current problem of modern medicine remains the negative dynamics of the growth of emotional and cognitive disorders against the background of the development of cerebrovascular pathology. In this regard arises the necessity for the development of specialized medical information systems (MIS) that improve the management of medical records, the analysis of clinical information, as well as patient support at all stages of its observation. The purpose of the work is to develop measures to organize information protection for the information system for identifying psychoemotional and cognitive disorders. For provide protection in the developed system, it is proposed to use the symmetric algorithm of block AES encryption. Organization of information protection of the information system for the detection of psychoemotional and cognitive impairments made it possible to eliminate the threat of unauthorized access to information about the patient and his condition, to prevent violation of its integrity and distortion.

1. Introduction

Currently, according to WHO, one of the main medical problems among the developed countries of the world are cerebral vascular disorders, and over the last decade, their substantial rejuvenation is noticeable. An actual problem of modern medicine is the negative dynamics of the growth of emotional and cognitive impairments, which are often accompanied by organic and symptomatic mental disorders on the background of cerebrovascular pathology [1].

The solution of this problem is important and has undoubted medical and social significance, therefore for the timely detection of the disease there is a need to accumulate and analyze a large amount of data obtained by observing patients, and to track their condition over a long period. Consequently, there is a need to develop specialized medical information systems (MIS) that improve the management of medical records, analyze clinical information, and accompany the patient at all stages of his observation [2].

2. Analysis of existing approaches to information protection in medical information systems

Today, any MIS is subject to such mandatory requirements as: functionality, information security and compatibility. Legally medical information about patients refers to information that constitutes a professional secret, access to it is limited and regulated by current legislation, therefore any medical organization and medical personnel must comply with legal regulations for the protection of information constituting medical secrets. Accordingly, a number of measures to ensure the security of both the information and the system as a whole must necessarily be implemented in the MIS, otherwise it will be inappropriate to use it.

After analyzing the classifications of information security threats that may arise from the use of patient data, it can be concluded that most often such threats are theft, destruction and distortion of information, its blocking, and also the denial of the authenticity of information and the imposition of false information [3].

Noting that the use of I MIS led to an increased risk of loss of medical information about the patient, in developing such systems, first of all, security measures should be applied to prevent unauthorized receipt of information, as well as its physical destruction or modification. Such measures include the creation of a security system that takes on functions related to the protection of information in the entire system as a whole and in each of the embedded modules in particular [4].

The security system is integrated and unified, which allows to ensure the confidentiality, integrity and accessibility of data, delineation of access to them [5].

Ensure the protection of information should be a mechanism that includes various security tools: hardware, software, organizational. There are a huge number of different options for building information protection, based on a variety of means of protection. Undoubtedly, in the design of protection, it is necessary to select the most effective means for a particular MIS [6,7].

In the development of MIS in identifying psychoemotional and cognitive disorders, a number of possible threats were identified, namely: the modification and deletion of data stored in the database; violation of confidentiality; theft of data when transferring them to a PC. Even the simplest transformation of information is a very effective means, which makes it possible to hide its essence from the majority of violators, however, cryptography is more often used to protect information, which is able to provide not only the privacy of medical information about the patient, but also its authenticity [4,8,9] .

The use of cryptography, to date, is one of the most common methods of protecting information, consists in changing its components using special algorithms or hardware solutions and key codes, with the same keys used for both encryption and decryption.

There are symmetrical and asymmetric encryption algorithms.

As a rule, long keys (512 bits or more) are used in asymmetric systems. A long key increases the encryption time and key generation is very long. This indicates the undesirable use of asymmetric encryption algorithms in our system, as information about patients accumulates and can increase. Accordingly, symmetric algorithms use shorter keys, so encryption is faster.

Also, asymmetric encryption algorithms use two keys: for encrypting information (public key), and for decrypting (secret key). These keys are different and can not be obtained from one another. Symmetric encryption algorithms are based on using the same key, so this key should be kept secret and transmitted in a way that excludes its loss.

In general, it can be said that asymmetric encryption is more complex in implementation, and the computations performed in this case are much more complicated than in symmetric encryption and the procedure takes longer (10).

Algorithms with symmetric keys have very high performance. Cryptography with symmetric keys is quite persistent, which makes it almost impossible for the decryption process without knowing the key [11].

It is important to note that symmetric ciphers are divided into block and stream ciphers.

In block encryption, plain text is used as the source data, and the alphabet on which this code operates is a set of binary vector blocks of plaintext of equal length. A block cipher is characterized by the ability to encrypt one key or several messages with a total length exceeding the length of the key. The transmission of a smaller key, in comparison with the message, over the encrypted channel is much simpler and requires less time than transferring the message itself or the key of the same length, which makes its practical use possible. Flexibility of block ciphers allows using them for building other cryptographic codes: stream cipher, cryptographic hashes, etc. [12]. A block cipher, as a rule, consists of two pair-forming algorithms: encryption and decryption [12, 13]. From stream ciphers, the block operation is characterized by bit processing by groups, not by flow.

A characteristic feature of stream encryption is its use in encrypting information in communication channels and the absence of the effect of error propagation.

The stream cipher implements a completely different approach to encryption, rather than block cipher. If, in case of block encryption, open text is divided into blocks of equal length, then for streaming, each character of plaintext is converted into an encrypted text symbol, depending not only on the key used, but also on its location in the plaintext stream.

The main difference between these two types of encryption is that block ciphers are used in the case of software implementation, and streaming ciphers are implemented in hardware.

Once again, note that the block cipher is a system of substitution of blocks. Known methods of block ciphers are the TEM cipher (one of the simplest in the implementation), GOST 28147-89 (based on the use of the Feistel network - the method of negotiable text transformations, in which the value calculated from one part of the text is superimposed on other parts), the standard AES et al. [4,9,14].

The most widely used block AES algorithm was approved by the US National Security Agency as suitable for encrypting sensitive information. However, the government decided that AES should be periodically inspected and improved to securely store encrypted data [4].

Information defined as secret must be protected by AES with a key length of 128, 192 and 256 bits. For information defined as highly secret, this length is 192 or 256 bits. The essence of AES is that any "frontal attack" on the protected data - that is, the selection of all possible passwords - in the long run is very much stretched. If we imagine that the burglar has huge resources, that is, a whole collection of supercomputers, then with diligent efforts, access to encrypted data could be obtained in tens of years. If at his disposal there is nothing of this, then AES hacking will take quite a long period (this period can be calculated for years).

It is believed that the 128-bit key used in Advanced Encryption Standard is quite reliable protection against frontal attack, that is, from a purely mathematical point of view, to pick one correct password out of all possible - an impossible task. Despite even some of the shortcomings of AES, it is almost impossible to crack information protected by this algorithm.

The length of the key used in encryption and determines the practical feasibility of doing a complete search, because the information encrypted with longer keys is more difficult to crack than with short ones.

3. Purpose of the article

Analysis of well-known information systems for the detection of psychoemotional and cognitive impairments showed that most of them possess either a weak degree of information protection or, on the contrary, too complicated and cumbersome, and also create a lot of problems in their operation.

The purpose of the work is to develop measures to organize information protection for the information system for identifying psychoemotional and cognitive disorders. For provide protection in the developed system, it is proposed to use a symmetric block encryption algorithm (AES).

4. Exposition of the main material of the study

The proposed MIS of psychoemotional and cognitive disorders has the following structure (look on figure). First of all, it includes the biological and technical subsystems.

Biological subsystem compose is a doctor-psychiatrist (doctor-psychotherapist, medical psychologist), which tests the patient's condition and the patient himself. So the doctor receives information about the patient's condition and his personal data, i.e. the passport data, complaints, the anamnesis of disease, etc. are recorded. Between the doctor and the patient, through communication during the consultation, there is interaction.

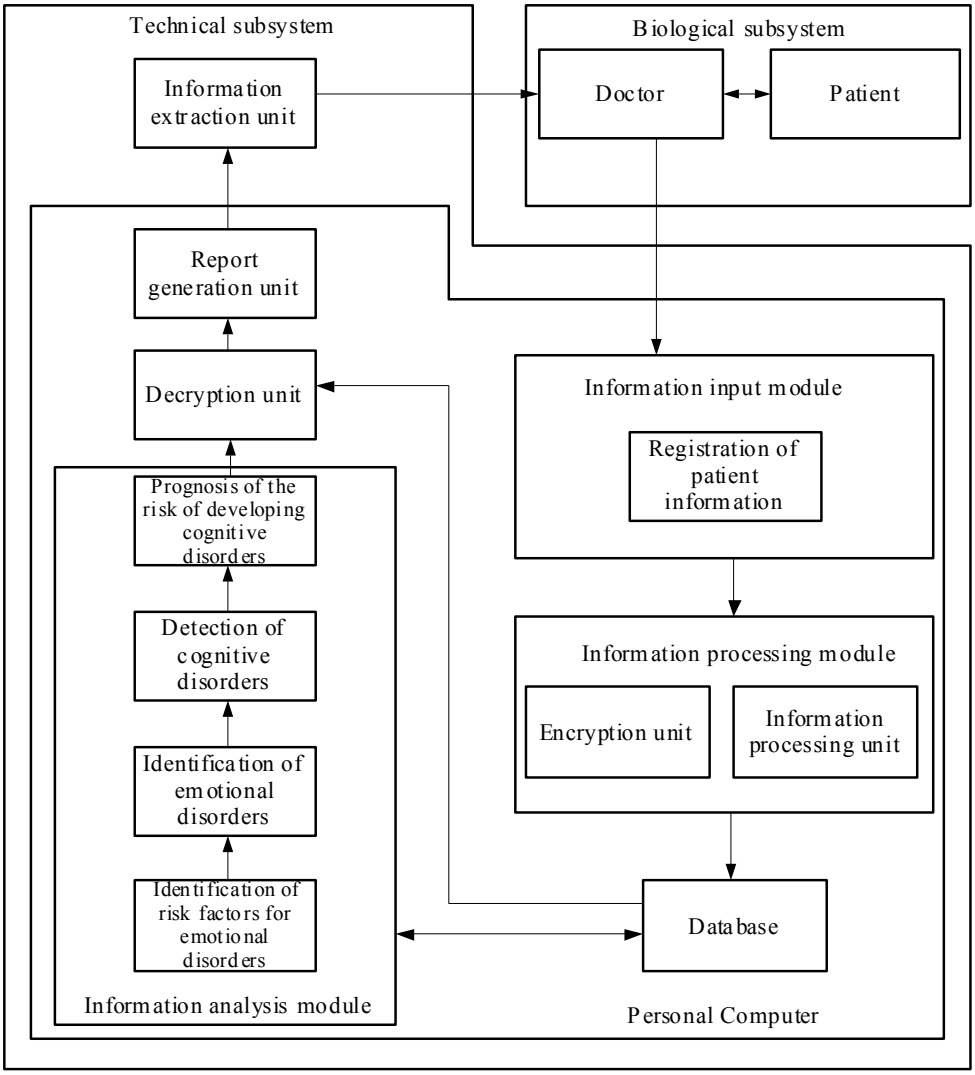

Fig. Structural diagram of the medical information system for the detection of psychoemotional and cognitive disorders

Then the data goes to the technical subsystem, which consists of a number of elements: an information input unit, an information processing unit, a database, an information analysis unit, and an information extraction unit.

The module for introducing information is intended for recording such patient data obtained during communication, as well as the results of its psychodiagnostic, clinical and laboratory and instrumental studies, the conclusions of other specialists (neurologist, cardiologist, ophthalmologist, etc.).

The processing of the registered patient data and the coding of the stage of the disease are carried out in the information processing unit, after which the patient data is transferred to the database (DB) or to the information analysis unit.

In the information analysis module, consisting of four blocks, using statistical and mathematical methods of analyzing the data obtained, a process of identifying psychoemotional and cognitive disorders, the degree of severity and predicting their further development are carried out.

The information received in the analysis block is sent to the database, and then to the report generation unit. The conclusion about the psychoemotional and / or cognitive state of the patient can be viewed in the information output block. Based on the findings, the doctor prescribes appropriate treatment or psychocorrection.

Having described the work of the MIS in identifying psychoemotional and cognitive disorders, it becomes evident that the most vulnerable information about the patient becomes during storage in the database. It is when storing information in a database that it is subject to a number of threats, namely: violation of data confidentiality, i.e. copying or unauthorized distribution; The harmful

effect on the content of information, i.e. changing the patient's personal data or destroying it; unauthorized influence on the program elements of MIS, etc.

Thus, after analyzing the work of MIS on the detection of psychoemotional and cognitive disorders, it was found that it is most rational to carry out encryption of patient information in the information processing module. Decryption is advisable to implement at the stage of report formation. The figure shows the structure of the MIS.

To protect against unauthorized access to the database from other software products, a symmetric block cipher AES algorithm was used.

AES is based on the Rijndael algorithm. For AES, the length of the input data block and the state is constant and equal to 128 bits, and the length of the encryption key K is 128, 192 or 256 bits. In this case, the output Rijndael algorithm allows the key length and block size from 128 to 256 bits in 32-bit increments. To denote selected input, State and Cipher Key lengths in 32-bit words, Nb = 4 for input and State, Nk = 4, 6, 8 for Cipher Key, respectively, for different key lengths is used [4].

At the initial stage of encryption, the input is copied to the State array by the rule:

state [r, c] = input [r + 4c],

for $0 \le r \le 4$ and $0 \le c \le Nb$.

After this, the AddRoundKey () procedure is applied to the State and then the State passes through the transformation procedure (round), depending on the length of the key 10, 12, or 14 times, with the last transformation being different from the previous ones. As a result, after the last round of transformation is completed, State is copied to the output according to the rule:

output [r + 4c] = state [r, c],

for $0 \le r \le 4$ and $0 \le c \le Nb$.

Separate transformations SubBytes () ShiftRows () MixColumns () and AddRoundKey () - handle the State.

The procedure SubBytes () processes each byte of the state, independently by making a nonlinear substitution of bytes using the replacement table (S-box). In the SubBytes procedure, each byte in state is replaced by the corresponding element in a fixed 8-bit lookup table, S; bij = S (aij). The construction of the S-box consists of two steps: in the first step, each byte is replaced by a multiplicative inverse to it in the Galois field GF (28), on the second - to each byte b, from which the S-box is created, the corresponding operation is used polynomial. This operation ensures the nonlinearity of the encryption algorithm [4].

ShiftRows works with State strings. With this transformation, the status bars are cyclically shifted by r bytes horizontally, depending on the line number. For zero line r = 0, for the first row r = 1 byte, etc. When this step of encryption is performed by the ShiftRows procedure, the bytes in each State line are cyclically shifted to the left. The size of the byte offset of each line depends on its number. Thus, each column of the output state after applying the ShiftRows procedure consists of the bytes of each column of the initial state.

In the MixColumns procedure, the four bytes of each State column are mixed using a reversible linear transformation. Each state column is multiplied with a fixed polynomial c (x).

MixColumns processes states on columns, interpreting each of them as a fourth-degree polynomial. Together with ShiftRows, MixColumns introduces diffusion into the cipher.

In the AddRoundKey procedure, RoundKey of each round is combined with the State. For each round, Roundkey is obtained from CipherKey using the KeyExpansion procedure; each RoundKey is the same size as the State. The procedure produces a bitwise XOR of each State byte with each RoundKey byte, i.e. In the AddRoundKey procedure, each state byte is combined with RoundKey using the XOR operation.

To verify the operation of the presented encryption algorithm, two patient data blocks were selected, differing by 1 bit. Comparing the same blocks after encryption, their significant differences were noticed (differences in ciphertext were 65 bits of information).

5. Conclusions

Thus, the analysis of current trends in the organization of information protection of the information system for the detection of psychoemotional and cognitive disorders has shown that they can be confirmed by various types of threats, for example, unauthorized access to information stored in the database, data exchange attacks etc.

As the most effective algorithm for protecting information, a symmetric block cipher AES algorithm was chosen. The application of this algorithm allowed, due to its byte-oriented structure, to

achieve the necessary and sufficient performance of encryption operations on various software platforms with a sufficiently large amount of heterogeneous information and to ensure the confidentiality of important medical information at all stages of identifying psychoemotional and cognitive impairments.

Note that due to the implementation of additional operations related to encryption and decryption processes, the processing time of patient data has increased, but this time increase is insignificant. Also, the lack of the encryption algorithm used should be attributed to the ease of manipulating blocks (deletion, repetition or permutation), but the main advantage is the implementation of data conversion in two dimensions, i.e. by rows and columns, which guarantees complete dispersion and mixing of information in two iterations. So, when encrypting two practically identical blocks of data on the results of psychological, clinical and laboratory and instrumental research, absolutely different blocks of ciphertext were obtained.

Organization of information protection of the information system for the detection of psychoemotional and cognitive disorders made it possible to eliminate the threat of unauthorized access to information about the patient and his condition, to prevent violation of its integrity and distortion.

References: 1. *Vysotskaya O.V., Kozhina A.M., Risovanaya L.M., Seagull E.E.* The use of discriminant analysis for the classification of cognitive disorders in patients with discirculatory encephalopathy // Sistemi obrobki informatsii. 2013. Issue 9 (116). P.189-193. 2. *Vysotskaya O.V., Panferova I.Yu., Rysovana L.M.* Development of a database of the information system for diagnosing the degree of cognitive disorders in patients with discirculatory encephalopathy // East-European Journal of Advanced Technologies. 2014. Information Technologies Series 3 /2 (69). P.9-14. 3. *Khoroshko V.A., Chekatkov A.A.* Methods and means of information protection. L.: Junior, 2000. 504p. 4. *Rouzhentsev V.I., Porvan A.P., Pashchenko M.A.* Organization of information security in the information system for determining the cells of toxicity of bioobjects // News of NTU "KhPI". 2015. No. 52 (1161). P.152-156. 5. *Security* Code. Products. Access mode: www / URL: http:// www.security code.ru/products/ zagl. from the screen. 6. *Katsupeev A.A., Shcherbakova E.A., Vorobiev S.P.* Statement and formalization of the task of forming information protection of distributed systems // Electronic scientific journal "Engineering Bulletin of the Don". 2015. №1. P.128-137. 7. *Alushkevich V.B., Dmitriev V.A., Lapitsky V.A., Sacek M.M.* Issues of Information Security in Healthcare // Issues of Health Organization and Informatization. 2016. №3. P. 9-11. 8. *Simmons G.D.* Overview of authentication methods // TIIER. 2008. №5. P. 156-174. 9. *Babichev S.G., Goncharov V.V., Serov R.E.* Fundamentals of modern cryptography. M.: Ozon.ru, 2011. 176p. 10. *Goncharov N.O.* Symmetric and asymmetric encryption // Youth Scientific and Technical Herald. 2013. № 1. Access mode: www / URL: http://sntbul.bmstu.ru/doc/532002.html 11. *Zhukov A.E.* Lightweight cryptography // Questions of cybersecurity. 2015. № 1 (9). P. 26-43. 12. *Sidorenko A.V., Zhukovets D.A.* Block algorithm of encryption based on dynamic chaos // Bulletin of BSU. Ser. 1. 2015. No 3. P. 34-39. 13. *Zhang X., Fan X., Wang J., Zhao Z.* A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution. Berlin, 2014. P. 158-159. 14. *Block* ciphers. Access mode: www / URL: http://citforum.ru/internet/ infsecure / its2000_16.shtml - zagl. from the screen.

Надійшла до редколегії 12.02.2018

Ruzhentsev Victor, Doctor of Technical Sciences, Associate Professor, Professor of Department of Information Technology Security, NURE. Scientific interests: methods of cryptographic analysis and information security. Address: Nauky Ave., 14, Kharkiv, Ukraine, 61166; e-mail: viktor.ruzhentsev@nure.ua.

Vysotska Olena, Doctor of Technical Sciences, Professor, Professor of Department of Information Control Systems, NURE. Scientific interests: medical cybernetics, decision-making in medicine, medical statistics, medical information technologies and systems. Address: Nauky Ave., 14, Kharkiv, Ukraine, 61166; e-mail: olena.vysotska@nure.ua.

Rysovana Lyubov, assistant of Department of Medical and Biological Physics and Medical Informatics, KhNMU. Scientific interests: medical informatics, medical statistics. Address: Nauky Ave., 4, Kharkiv, Ukraine, 61022; tel.: 067-388-75-97; e-mail: rluba_24@ukr.net.

Zinchenko Yuliia, student of Department of Biomedical Engineering, NURE. Scientific interests: medical statistics. Address: Nauky Ave., 14, Kharkiv, Ukraine, 61166; e-mail: pharjul@ukr.net.

Alekseienko Roman, Candidate of Medical Sciences, Associate Professor of Physiology Department , KhNMU. Scientific interests: medical cybernetics. Address: Nauky Ave., 4, Kharkiv, Ukraine, 61022, e-mail: alekseenko-roman@ukr.net.